



DmSwitch Command Reference

Revision History

Revision 15.2.18 2021/06/18

204.4096.16

Contact Information

In order to contact the DATACOM technical support, or sales department:

- Support:

- E-mail: suporte@datacom.ind.br
- Phone: +55 51 3933-3122

- Sales:

- E-mail: sales@datacom.ind.br
- Phone: +55 51 3933-3000

- Internet:

- www.datacom.ind.br

- Address:

- DATACOM - Telemática
- R. America, 1000 - Eldorado do Sul, RS - Brasil
- CEP: 92990-000

Conventions

This guide uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in screen font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Table of Contents

1. Introduction.....	1
The Command Line Interface	1
2. Root Commands.....	2
bpdu-protect manual-unblock	2
cfm delay-measurement	4
cfm linktrace	6
cfm loopback	8
clear capture	10
clear core-dump.....	12
clear counter	14
clear cpu arp-table	15
clear cpu counters queues	17
clear cpu packets	18
clear elmi.....	19
clear interface counters	21
clear interface queue-counters.....	24
clear interface test	26
clear dump.....	28
clear ip arp.....	30
clear ip bgp.....	32
clear ip dhcp server	34
clear ip dhcp snooping	36
clear ip ospf.....	38
clear ip path-mtu-discovery cache.....	40
clear ip rip	42
clear ipv6 bgp.....	44
clear ipv6 ospfv3.....	46
clear ipv6 path-mtu-discovery cache.....	48
clear ipv6 ripng	50
clear logging.....	52
clear lldp.....	54
clear mac-address-table	56
clear meter.....	58
clear mpls ^{[1] [3] [6]}	59
clear mpls l2vpn ^{[1] [3] [5]}	61
clear mpls ldp ^{[1] [3] [6]}	63
clear mpls-oam ^{[1] [3] [6]}	65
clear spanning-tree counters.....	67
clear spanning-tree detected-protocols.....	69
clear snmp counters.....	71
clear stacking saved-topology	73
clock set.....	75
configure.....	77
copy	78
debug	83

debug cfm.....	88
debug ip-tunnel.....	90
debug lldp.....	92
debug port-security.....	94
debug oam	96
debug openflow	98
diff.....	100
dot1x initialize ethernet.....	102
dot1x reauthenticate ethernet	104
erase	106
exit.....	108
help.....	109
dump.....	111
light unit	112
memory unit <i>unit</i> external ^{[5][7]}	113
Output modifiers	115
ping.....	117
ping6.....	119
ping mpls ^{[1][3][6]}	121
ping vrf.....	125
process.....	127
reboot	129
redundancy ^[5]	131
remote-devices force ethernet	133
select.....	135
show arp aging-time	137
show authentication.....	138
show backup-link	140
show batch.....	142
show bridge-ext	144
show bpdu-protect.....	145
show cable-diagnostics.....	147
show capture file	149
show capture files.....	152
show capture realtime	153
show cesop	156
show cfm	158
show cfm mep	159
show cfm delay-statistics	161
show cfm error	163
show cfm linktrace	165
show cfm md	167
show cfm probe delay-measurement.....	169
show clock.....	171
show core-dump	172
show counter	174
show cpu.....	177
show cpu egress-block	181

show cpu-dos-protect	183
show cpu arp-table	186
show cpu counters queues	188
show debug-counters rx	190
show debugging	192
show debugging cfm	193
show debugging dot1x	195
show debugging elmi	197
show debugging oam	199
show dot1x	201
show dscp-table	204
show eaps	206
show elmi	208
show erps	210
show filter	212
show firmware	214
show flash	216
show flash-config	218
show garp	220
show gvrp	222
show hardware-status	224
show hardware-status fans fuses	226
show hardware-status transceivers detail	228
show hardware-status transceivers presence	230
show history	232
show hqos	233
show interfaces bundle	235
show interfaces counters	238
show interfaces description	241
show interfaces e1c	243
show interfaces e1c mappings	245
show interfaces g704	247
show interfaces g704 mappings	249
show interfaces link	251
show interfaces local-tunnel ^[1] ^[3] ^[5]	253
show interfaces loopback	254
show interfaces ptp	256
show interfaces sdh	258
show interfaces status	260
show interfaces switchport	263
show interfaces table bundle	265
show interfaces table configuration	267
show interfaces table counter	269
show interfaces table queue-l2	271
show interfaces table utilization	273
show interfaces test bundle	275
show interfaces test sdh	277
show dump	279

show ip	281
show ip bfd neighbors	283
show ipv6 bfd neighbors	285
show ip bgp	287
show ip bgp community	292
show ipv6 bgp	294
show ip prefix-list.....	298
show ip default-gateway.....	300
show ipv6 default-gateway.....	301
show ip dhcp relay	302
show ip dhcp server.....	304
show ip dhcp pool	306
show ipv6 dhcp relay	308
show ipv6 dhcp server.....	310
show ipv6 dhcp pool	312
show ip dhcp snooping.....	314
show ip dhcp snooping database.....	316
show ip dhcp snooping statistics	318
show ip dns-servers	321
show ip domain-name	322
show ip hardware ecmp-table.....	324
show ip hardware egr-table	326
show ip hardware egr-info.....	328
show ip hardware host-table.....	331
show ipv6 hardware host-table.....	333
show ip hardware intf-table.....	335
show ip hardware lpm-table	337
show ipv6 hardware lpm-table	339
show ip http	341
show ip igmp snooping	343
show ipv6 mld snooping	345
show ip igmp snooping mroute	347
show ipv6 mld snooping mroute	349
show ip interface	350
show ipv6 interface	351
show ip multicast-routing.....	353
show ipv6 multicast-routing.....	355
show ip ospf	357
show ipv6 ospfv3	360
show ip path-mtu-discovery cache.....	363
show ipv6 path-mtu-discovery cache.....	365
show ip pim bsr-candidate.....	367
show ipv6 pim bsr-candidate.....	369
show ip pim config	371
show ipv6 pim config	373
show ip pim interfaces.....	375
show ipv6 pim interfaces.....	377
show ip pim join.....	379

show ipv6 pim join	381
show ip pim mfc	383
show ipv6 pim mfc	385
show ip pim neighbors	387
show ipv6 pim neighbors	389
show ip pim rp-candidate	391
show ipv6 pim rp-candidate	393
show ip pim rps	395
show ipv6 pim rps	397
show ip rip	399
show ip rip neighbor	401
show ipv6 ripng	403
show ipv6 ripng neighbors	405
show ipv6 ripng database	407
show ip route	409
show ip route pbr	411
show ipv6 route	413
show ip route vrf	415
show ip routing	417
show ip snmp-server	419
show ip snmp-server traps	421
show ip ssh	423
show ip telnet	425
show ip tftp	426
show ip vrf	427
show ip-tunnel	429
show isis	431
show ipfix	435
show l2protocol-tunnel	437
show lacp counters	439
show lacp <i>port-channel</i>	441
show lacp internal	443
show lacp neighbors	445
show lacp sysid	447
show link-flap	449
show link-state-tracking	451
show lldp	453
show lldp counters	456
show lldp neighbor	458
show log	460
show logging	462
show loopback-detection	464
show mac-address-table	466
show mac-address-table aging-time	469
show mac-address-table sort	471
show mac-address-table summary	473
show mac-address-table usage	475
show management	477

show managers	479
show memory	480
show meter	482
show monitor	484
show mpls forwarding-table ^{[1] [3] [6]}	486
show mpls exp-map egress ^{[1] [3] [6]}	490
show mpls exp-map ingress ^{[1] [3] [6]}	492
show mpls ftn ^{[1] [3] [6]}	494
show mpls l2vpn ^{[1] [3] [6]}	496
show mpls l2vpn hardware	500
show mpls audit l2vpn ^{[1] [3] [6]}	505
show mpls vpls mac-address-limit ^{[1] [3] [6]}	507
show mpls ldp database ^{[1] [3] [6]}	509
show mpls ldp discovery ^{[1] [3] [6]}	513
show mpls ldp graceful-restart ^{[1] [3] [6]}	515
show mpls ldp igp sync ^{[1] [3] [6]}	517
show mpls ldp neighbor ^{[1] [3] [6]}	519
show mpls ldp parameters ^{[1] [3] [6]}	521
show mpls oam ^{[1] [3] [6]}	523
show mpls rsvp ^{[1] [3] [6]}	525
show mpls te traffic-eng tunnels ^{[1] [3] [6]}	527
show network-policy	529
show network-policy mac-list	531
show oam	533
show openflow	535
show poe	537
show port-security	540
show privilege	542
show processes	543
show profile-config	545
show ptp	547
show public-key	549
show queue config	551
show queue cos-map	553
show radius-server	555
show redundancy-status ^[5]	557
show remote-devices	559
show rmon alarm	562
show rmon event	564
show rmon history	566
show rmon statistics	568
show running-config	570
show running-config cfm	572
show running-config interface	574
show running-config private-vlan	577
show running-config sdh-map	579
show running-config vlan	581
show sdh-map	583

show sdh-map table.....	585
show sflow config.....	587
show sflow counters	589
show sflow interfaces	591
show snmp.....	593
show spanning-tree.....	595
show stacking	598
show stacking priority	600
show stacking saved-topology.....	602
show stacking synced-status	604
show startup-config	606
show sync-source	608
show sync-source bits-clock-mode	610
show sync-source hierarchy	612
show sync-source status	614
show system	616
show tacacs-server.....	618
show tech-support	620
show terminal	622
show terminal encrypted-data	624
show units.....	625
show chassis-load-balance ^{[1] [5] [6] [8] [9]}	627
show uptime	629
show users	631
show vlan	632
show vlan-group.....	636
show vlan-mac-table ^[1]	638
show vrrp.....	640
show warnings.....	643
show wred	645
ssh.....	647
stacking	649
telnet.....	652
terminal aux.....	654
terminal encrypted-data.....	655
trace mpls	657
traceroute.....	660
traceroute vrf	662
traceroute6.....	664
transceiver identification-restart.....	666
unit	668
3. Configure Commands.....	669
arp aging-time	669
arp static	671
authentication login.....	673
banner login.....	675
batch <i>index</i> date.....	677

batch <i>index</i> disable	679
batch <i>index</i> enable	681
batch <i>index</i> remark	683
batch <i>index</i> start-session	685
batch new	687
batch term-session	689
bridge-ext gvrp	691
cesop idle-byte	693
cfm	695
clock timezone	697
counter	699
cpu-dos-protect	701
cpu egress-block	705
cpu protocol-priority default	707
cpu protocol-priority enable	709
cpu protocol-priority l2-protocol	711
cpu protocol-priority hardware	713
cpu protocol-priority management	715
cpu protocol-priority tunnel	717
cpu protocol-priority unknown	719
cpu protocol bpd-protect	721
dot1x accounting	723
dot1x captive-portal	725
dot1x default	727
dot1x max-users	729
dot1x sytem-auth_control	731
dscp-table	733
eaps <i>domain</i>	735
eaps <i>domain</i> control-vlan	737
eaps <i>domain</i> failtime	739
eaps <i>domain</i> hellotime	741
eaps <i>domain</i> mode	743
eaps <i>domain</i> packet-mode	745
eaps <i>domain</i> name	747
eaps <i>domain</i> port	749
eaps <i>domain</i> port-block-aware	751
eaps <i>domain</i> protected-vlans	752
eaps hw-forwarding	754
elmi	755
erps <i>domain</i>	757
erps <i>domain</i> accept	759
erps <i>domain</i> control-vlan	761
erps <i>domain</i> guard-time	763
erps <i>domain</i> holdoff-time	765
erps <i>domain</i> name	767
erps <i>domain</i> port0	769
erps <i>domain</i> port1	771
erps <i>domain</i> protected-vlans	773

erps domain restore-time.....	775
evc	777
external-alarm	779
debug-counters rx.....	781
fetch tftp	784
filter	786
hostname	793
hqos	794
interface bundle.....	796
interface ethernet.....	798
interface g704.....	800
interface e1c	802
interface ip-tunnel	804
interface local-tunnel ^{[5][7]}	805
interface loopback	806
interface port-channel.....	808
interface private-vlan.....	810
interface ptp.....	812
interface sdh	814
interface vlan.....	816
ip default-gateway	818
ipv6 default-gateway	820
ip dhcp relay	822
ipv6 dhcp relay	824
ip dhcp relay information option.....	826
ip dhcp relay information trusted	828
ip dhcp relay vlan.....	830
ip dhcp pool.....	832
ipv6 dhcp server	834
ipv6 dhcp pool.....	835
ip dhcp server	836
ip dhcp snooping	838
ip dhcp snooping cyclic save timer	840
ip dhcp snooping verify mac-address.....	842
ip dhcp snooping vlan	844
ip dns server	846
ip domain-name.....	848
ip helper-address	850
ipv6 helper-address	852
ip http	854
ip igmp	856
ipv6 mld	859
ip igmp snooping vlan.....	862
ipv6 mld snooping vlan.....	864
ip path-mtu-discovery	866
ip pim	868
ipv6 pim	870
ip pim bootstrap	872

ipv6 pim bootstrap	874
ip pim bootstrap bsr-candidate	876
ipv6 pim bootstrap bsr-candidate	878
ip pim bootstrap rp-candidate	880
ipv6 pim bootstrap rp-candidate	882
ip pim rp-address.....	884
ipv6 pim rp-address.....	886
ip pim spt-switch.....	888
ipv6 pim spt-switch	890
ipv6 nd ra	892
ip prefix-list	894
ip route	896
ip route pbr	899
ipv6 route	901
ip routing	904
ip snmp-server	906
ip snmp-server traps	909
ip ssh	914
ipv6 ssh	917
ip telnet.....	919
ip tftp	921
ipv6 telnet.....	923
ip vrf.....	925
key chain	927
l2protocol-tunnel.....	929
lacp mode	931
lacp rate	933
lacp system-priority	935
link-state-tracking	937
lldp	939
lldp notification-interval.....	941
lldp reinitialize-delay	943
lldp transmit-delay	945
lldp transmit-hold.....	947
lldp transmit-interval	949
lldp med location-identification coordinate altitude	951
lldp med location-identification coordinate altitude-resolution	953
lldp med location-identification coordinate altitude-type	955
lldp med location-identification coordinate datum	957
lldp med location-identification coordinate latitude	959
lldp med location-identification coordinate latitude-resolution	961
lldp med location-identification coordinate longitude	963
lldp med location-identification coordinate longitude-resolution.....	965
lldp med location-identification ecs-elin.....	967
logging commands	969
logging debug.....	971
logging facility	976
logging history	978

logging host.....	980
logging host destination-ipv6.....	982
logging on	984
logging sendmail	986
logging trap	988
loopback-detection action	990
loopback-detection destination-address	992
mac-address-table aging-time	994
mac-address-table duplication-monitoring	996
mac-address-table move-monitoring.....	998
mac-address-table static	1000
management	1002
memory-external resource ^[5]	1004
chassis load-balance ^{[1] [5] [6] [8] [9]}	1006
meter.....	1009
monitor	1011
mpls exp-map egress ^{[1] [3] [6]}	1013
mpls exp-map ingress ^{[1] [3] [6]}	1015
mpls expl-path ^{[1] [3] [6]}	1017
mpls ldp control-mode ^{[1] [3] [5]}	1019
mpls ldp discovery ^{[1] [3] [6]}	1021
mpls ldp holdtime ^{[1] [3] [6]}	1023
mpls ldp neighbor ^{[1] [3] [6]}	1025
mpls ldp logging.....	1028
mpls ldp igp sync holddown ^{[1] [3] [6]}	1030
mpls ldp graceful-restart ^{[1] [3] [6]}	1032
mpls l2vpn logging.....	1035
mpls rsvp ^{[1] [3] [6]}	1037
mpls rsvp logging.....	1039
mpls te ^{[1] [3] [6]}	1041
mpls vpws ^{[1] [3] [6]}	1043
mpls vpls ^{[1] [3] [6]}	1044
mpls vpls mac-address limit global ^{[1] [3] [6]}	1045
mpls audit l2vpn ^{[1] [3] [6]}	1047
mvr	1049
network-policy	1051
network-policy mac-list	1053
openflow	1055
port-channel nuc-load-balance ^[1]	1057
ptp unit domain	1059
ptp unit enable	1061
ptp unit mode	1063
queue cos-map.....	1065
radius-server acct-port.....	1067
radius-server auth-port	1069
radius-server host	1071
radius-server key	1073
radius-server retries	1075

radius-server timeout.....	1077
remote-devices devices-vlan	1079
remote-devices enable	1081
remote-devices force	1083
remote-devices rate-limit	1085
remote-devices service	1087
rmon	1089
rmon alarm	1091
rmon event.....	1093
route-map	1095
router bgp	1097
router isis.....	1099
router ospf	1101
router ospfv3	1103
router rip.....	1105
router ripng.....	1107
sdh-map	1109
rpu power-sharing	1111
sniffer	1113
sntp	1115
spanning-tree	1117
spanning-tree bpdupfilter	1119
spanning-tree bpduguard.....	1121
spanning-tree <i>instance</i>	1123
spanning-tree <i>instance</i> forward-delay	1126
spanning-tree <i>instance</i> hello-time	1128
spanning-tree <i>instance</i> max-age.....	1130
spanning-tree <i>instance</i> max-hops.....	1132
spanning-tree <i>instance</i> priority.....	1134
spanning-tree <i>instance</i> root	1136
spanning-tree <i>instance</i> vlan-group	1138
spanning-tree <i>instance</i> bpdu-tag	1140
spanning-tree mode	1142
spanning-tree mst	1144
storm-control	1146
sync-source bits-clock-mode.....	1147
sync-source hierarchy ack-out-of-limits	1149
sync-source hierarchy enable	1151
sync-source hierarchy transmit-clock-source bits.....	1153
sync-source hierarchy transmit-clock-source g704.....	1155
sync-source hierarchy transmit-clock-source internal	1157
sync-source hierarchy transmit-clock-source ptp.....	1159
sync-source hierarchy transmit-clock-source sdh	1161
sync-source hierarchy wtr	1163
sync-source revertive.....	1165
sync-source switch-enable	1167
tacacs-server acct-port.....	1169
tacacs-server acct-timeout.....	1171

tacacs-server acct-type	1173
tacacs-server authe-port	1175
tacacs-server authe-timeout.....	1177
tacacs-server authe-type	1179
tacacs-server autho-port	1181
tacacs-server autho-timeout	1183
tacacs-server host	1185
tacacs-server key	1187
terminal login-timeout.....	1189
terminal paging	1191
terminal timeout	1193
username	1195
vlan-group	1197
vlan link-detect.....	1199
vlan-mac-table source-mac ^[1]	1201
vlan qinq.....	1203
vlan-translate	1205
wred.....	1207
4. CFM MA Commands	1209
ais alarm-suppression.....	1209
ais enable.....	1211
ais level.....	1213
ais period	1215
ais priority	1217
ais recovery-limit	1219
ais vlan-notify	1221
ccm-interval.....	1223
fault-alarm-address.....	1224
mep.....	1226
mep-list.....	1228
mip	1230
sender-id-tlv	1232
5. CFM MD Commands	1234
fault-alarm-address.....	1234
ma	1236
sender-id-tlv	1238
6. CFM MEP Commands.....	1240
action shutdown event	1240
enable	1242
fault-alarm-address.....	1244
fault-alarm-priority.....	1246
fault-alarm-time.....	1248
generate-ccm	1250
primary-vid.....	1252
priority.....	1254

7. CFM Probe Commands	1256
delay-measurement	1256
8. CFM Probe DM Commands.....	1258
interval.....	1258
ma.....	1260
9. CFM Test Commands.....	1262
cfm-test-tst	1262
10. E-LMI Commands.....	1264
uni-c	1264
uni-n	1266
11. E-LMI UNI-C Commands	1268
polling-counter	1268
polling-timer.....	1270
status-counter	1272
12. E-LMI UNI-N Commands	1274
evc	1274
evc-map-type.....	1276
polling-verification-timer	1278
status-counter	1280
id.....	1282
13. HQoS Commands	1284
service	1284
14. Interface Bundle Commands.....	1287
bundle circuit-name.....	1287
bundle destination-bundle	1289
bundle destination-ip-address.....	1291
bundle destination-mac	1293
bundle dscp.....	1295
bundle ecid	1297
bundle ip-next-hop	1299
bundle jitter-buffer	1301
bundle jitter-buffer-history	1303
bundle jitter-buffer-history interval	1304
bundle lost-pkt-fill.....	1306
bundle lops-limits.....	1308
bundle r-bit-send-rai	1310
bundle packet-delay	1311
bundle packet-loss-threshold.....	1313
bundle psn-type	1315
bundle qinq.....	1317
bundle shutdown	1319
bundle source-ip-address.....	1320
bundle tdm-channel	1322
bundle test	1324
bundle timeslots	1326

bundle vlan	1328
15. Interface Ethernet/Port-channel Commands.....	1330
capabilities	1330
description.....	1332
dot1x captive-portal.....	1334
dot1x guest-vlan	1336
dot1x mac-authentication	1338
dot1x max-req	1340
dot1x max-users	1342
dot1x port-control	1344
dot1x host-mode.....	1346
dot1x quiet-period	1348
dot1x re-auth-enable	1350
dot1x re-authentication	1352
dot1x re-auth-max	1354
dot1x re-auth-period.....	1356
dot1x restricted-vlan	1358
dot1x server-timeout	1360
dot1x timeout	1362
dscp-mapping	1364
flowcontrol	1366
garp timer	1368
ip arp-protection trust.....	1370
ip dhcp snooping trust	1372
ipfix	1374
l2protocol-tunnel.....	1375
lacp	1377
lacp actor port-priority	1378
link-flap	1380
lldp admin-status.....	1382
lldp notification	1384
lldp tlvs-tx-enable	1386
lldp med enable	1388
lldp med fast-start-repeat-count	1390
lldp med notification	1392
lldp med tlvs-tx-enable.....	1394
loopback-detection	1396
loopback-internal	1398
mac-address-table move-monitoring.....	1400
mac-learn.....	1402
mdix	1404
monitor source.....	1406
negotiation.....	1408
network-policy	1410
oam.....	1412
openflow enable	1414
poe.....	1416

queue max-bw	1419
queue sched-mode sp	1421
queue sched-mode wfq.....	1423
queue sched-mode wrr	1425
queue sched-mode wdr	1427
rate-limit.....	1429
rmon collection history	1431
rmon collection stats	1433
sflow counter-interval.....	1435
sflow max-header-size.....	1437
sflow receiver	1439
sflow sample-rate	1441
sflow	1443
shutdown	1445
slow-protocols	1447
spanning-tree	1449
spanning-tree bpdupfilter	1451
spanning-tree bpduguard.....	1453
spanning-tree edge-port.....	1455
spanning-tree <i>instance</i>	1457
spanning-tree link-type	1459
spanning-tree restricted-role	1461
spanning-tree restricted-tcn.....	1463
speed-duplex	1465
switchport acceptable-frame-types	1467
switchport backup-link.....	1469
switchport block broadcast ethernet.....	1471
switchport block multicast ethernet	1473
switchport block unicast ethernet.....	1475
switchport bpdu-protect	1477
switchport egress-block ethernet.....	1479
switchport gvrp	1481
switchport ingress-filtering	1483
switchport multicast-flood.....	1485
switchport mtu.....	1487
switchport native vlan	1489
switchport port-security maximum ^[3]	1491
switchport port-security mac-address ^[3]	1493
switchport port-security violation ^[3]	1495
switchport priority default.....	1497
switchport protocol	1499
switchport qinq.....	1501
switchport storm-control	1503
switchport tpid.....	1506
vlan-translate	1508
trap-enable.....	1510
wred averaging-time.....	1512
wred cng-drop-start-point	1514

wred cng-slope	1516
wred drop-start-point.....	1518
wred slope	1520
16. Interface IP Tunnel Commands	1522
description	1522
ipv6 address.....	1524
tunnel destination ip-address.....	1526
tunnel source interface	1528
tunnel type.....	1530
17. Interface Local Tunnel Commands ^{[5][7]}	1532
ltn-endpoint ^{[1] [3] [5]}	1532
18. Interface G704 Commands	1534
g704 line-type	1534
g704 shutdown	1536
g704 sync-source.....	1537
g704 test	1539
19. Interface E1C Commands.....	1541
e1c line-type	1541
e1c shutdown.....	1543
e1c sync-source	1545
20. Interface Loopback Commands	1547
ip address.....	1547
ipv6 <i>enable</i>	1549
ipv6 address.....	1551
ipv6 ripng	1553
isis authentication direction recv-only	1555
isis authentication direction send-only.....	1557
isis authentication key-chain	1559
isis authentication mode clear-text	1561
isis authentication mode hmac-md5.....	1563
isis circuit-type.....	1565
isis hello-interval.....	1567
isis metric	1569
isis metric-wide	1571
isis passive-interface	1573
mpls enable ^{[1] [3] [6]}	1575
shutdown	1577
21. Interface Port-channel Commands	1579
load-balance	1579
set-member ethernet.....	1581
lacp	1583

22. Interface PTP Commands.....	1585
ptp announce-rate	1585
ptp delay-req-rate	1587
ptp destination-ip-address	1589
ptp ip-next-hop	1591
ptp name	1593
ptp role	1595
ptp shutdown	1597
ptp source-ip-address	1598
ptp sync-rate	1600
ptp transport-mode	1602
ptp vlan.....	1604
23. Interface SDH Commands.....	1606
sdh path-trace	1606
sdh shutdown.....	1608
sdh test.....	1609
sdh vc4	1611
24. Interface SDH VC4 Commands	1613
sdh vc4 h4-multiframe	1613
sdh vc4 path-label	1615
sdh vc4 path-trace	1617
sdh vc4 tug-structure	1619
sdh vc4 vc4-structure	1621
sdh vc4 vc12.....	1623
25. Interface SDH VC4 VC12 Commands	1624
sdh vc12 path-label	1624
sdh vc12 path-trace	1626
26. Interface Private VLAN Commands.....	1628
community-vlan	1628
isolated-vlan	1630
mac-address-table learn.....	1632
mac-address-table maximum	1634
name	1636
set-member interswitch	1638
set-member promiscuous	1640
shutdown	1642
27. Community VLAN Commands	1644
mac-address-table learn.....	1644
name	1646
set-member	1648
shutdown	1650

28. Isolated VLAN Commands	1652
mac-address-table learn	1652
name	1654
set-member	1656
shutdown	1658
29. Interface VLAN Commands	1660
bfd interval	1660
gratuitous-arp-handling	1662
ip address	1664
ip arp-protection	1666
ip dhcp relay	1668
ip dhcp relay information trusted	1670
ipv6 dhcp relay	1672
ip helper-address	1674
ipv6 enable	1676
ipv6 address	1678
ip dhcp snooping	1680
ip directed-broadcast	1682
ip local-proxy-arp	1684
ip ospf authentication	1686
ip ospf authentication-key	1688
ip ospf bfd	1690
ip ospf cost	1692
ip ospf dead-interval	1694
ip ospf hello-interval	1696
ip ospf message-digest-key	1698
ip ospf mtu-ignore	1700
ip ospf network	1702
ip ospf priority	1704
ip ospf retransmit-interval	1706
ip ospf transmit-delay	1708
ipv6 nd ra	1710
ipv6 ospfv3 authentication	1712
ipv6 ospfv3 bfd	1714
ipv6 ospfv3 cost	1716
ipv6 ospfv3 dead-interval	1718
ipv6 ospfv3 hello-interval	1720
ipv6 ospfv3 instance-id	1722
ipv6 ospfv3 mtu-ignore	1724
ipv6 ospfv3 neighbor	1726
ipv6 ospfv3 network	1728
ipv6 ospfv3 priority	1730
ipv6 ospfv3 retransmit-interval	1732
ipv6 ospfv3 transmit-delay	1734
ip igmp snooping flood-unknown	1736
ip pim	1738
ipv6 pim	1740

ip proxy-arp	1742
ipv6 ripng	1744
ip vrf forwarding	1746
ip router isis	1748
isis authentication direction recv-only	1750
isis authentication direction send-only	1752
isis authentication key-chain	1754
isis authentication mode clear-text	1756
isis authentication mode hmac-md5	1758
isis circuit-type	1760
isis hello-interval	1762
isis metric	1764
isis metric-wide	1766
isis network point-to-point	1768
isis passive-interface	1770
isis priority	1772
ldp enable ^{[1] [3] [6]}	1774
link-detect	1776
mac-address-table learn	1778
mac-address-table maximum ^{[1] [3]}	1780
management-mtu	1782
mpls bgp forwarding ^{[1] [3] [5]}	1784
mpls ldp igp sync ^{[1] [3] [6]}	1786
mpls traffic-eng bandwidth ^{[1] [3] [6]}	1788
mtu	1790
mvr receiver	1792
name	1794
openflow enable	1796
rsvp enable ^{[1] [3] [6]}	1798
rsvp signalling hello refresh interval ^{[1] [3] [6]}	1800
rsvp signalling hello refresh misses ^{[1] [3] [6]}	1802
rsvp signalling link attributes ^{[1] [3] [6]}	1804
rsvp signalling refresh interval ^{[1] [3] [6]}	1806
rsvp signalling refresh misses ^{[1] [3] [6]}	1808
rsvp signalling refresh reduction ^{[1] [3] [6]}	1810
set-member forbidden	1812
set-member tagged	1814
set-member untagged	1816
shutdown	1818
vrrp group authentication	1820
vrrp group ip	1822
vrrp group ipv6	1824
vrrp group preempt	1826
vrrp group priority	1828
vrrp group shutdown	1830

30. Interface Management Commands.....	1832
ipv6 enable	1832
ipv6 address	1834
31. IP Route PBR Commands.....	1836
action	1836
description	1838
match dest-ip	1840
match src-interface	1842
match src-ip	1844
32. IPFIX Commands.....	1846
ipfix host.....	1846
ipfix flow-trigger	1848
33. IP VRF Commands.....	1850
import-map	1850
maximum routes.....	1852
rd ^{[1] [3] [5]}	1854
route-target ^{[1] [3] [5]}	1856
34. IP DHCP Server Commands	1858
enable	1858
excluded-address	1860
fixed-address	1862
35. IP DHCP Pool Commands	1864
network.....	1864
default-router	1866
dns-server	1868
netbios-name-server	1870
netbios-node-type	1872
domain-name	1874
lease	1876
deny-unknown-clients	1878
36. IPv6 DHCPv6 Server Commands	1880
enable	1880
37. IPv6 DHCPv6 Pool Commands	1882
network.....	1882
sip-address.....	1884
sip-domain.....	1886
dns-server	1888
domain-name	1890
38. Key Commands	1892
key-string.....	1892
39. Keychain Commands.....	1894
key id.....	1894

40. Link-state Tracking	1896
enable	1896
set-member	1898
41. Monitor Commands.....	1900
destination	1900
rspan	1902
source	1904
42. MPLS EXPL-PATH Commands	1906
explicit-path identifier ^{[1] [3] [6]}	1906
description ^{[1] [3] [6]}	1908
tsp-hop ^{[1] [3] [6]}	1910
43. MPLS RSVP Commands	1912
mpls traffic-eng fast-reroute revertive global ^{[1] [3] [6]}	1912
signalling refresh interval ^{[1] [3] [6]}	1914
signalling refresh misses ^{[1] [3] [6]}	1916
44. MPLS TE Commands	1918
interface te-tunnel ^{[1] [3] [6]}	1918
tunnel mpls destination ^{[1] [3] [6]}	1920
tunnel mpls traffic-eng affinity ^{[1] [3] [6]}	1922
tunnel mpls traffic-eng autoroute announce ^{[1] [3] [6]}	1924
tunnel mpls traffic-eng autoroute metric ^{[1] [3] [6]}	1926
tunnel mpls traffic-eng bandwidth ^{[1] [3] [6]}	1928
tunnel mpls traffic-eng igp ospf area.....	1930
tunnel mpls traffic-eng fast-reroute ^{[1] [3] [6]}	1932
tunnel mpls traffic-eng path-option ^{[1] [3] [6]}	1935
tunnel mpls traffic-eng priority ^{[1] [3] [6]}	1937
tunnel mpls traffic-eng record-route ^{[1] [3] [6]}	1939
tunnel name ^{[1] [3] [6]}	1941
shutdown ^{[1] [3] [6]}	1943
45. MPLS VPWS Commands	1945
vpn ^{[1] [3] [6]}	1945
name ^{[1] [3] [6]}	1947
xconnect vlan ^{[1] [3] [6]}	1949
neighbor ^{[1] [3] [6]}	1951
mplstype ^{[1] [3] [6]}	1953
backup-peer ^{[1] [3] [6]}	1955
backup-delay ^{[1] [3] [6]}	1957
vlanmode ^{[1] [3] [6]}	1959
statistics ^{[1] [2] [3] [4] [5] [6] [7]}	1961
exp-ingress-mapping ^{[1] [3] [6]}	1963
46. MPLS VPLS Commands	1965
vpn ^{[1] [3] [6]}	1965
name ^{[1] [3] [6]}	1967
mac-address limit ^{[1] [3] [6]}	1969
xconnect vlan ^{[1] [3] [6]}	1971

neighbor ^{[1] [3] [6]}	1973
transparent-lan-service ^{[1] [3] [6]}	1975
mplstype ^{[1] [3] [6]}	1977
split-horizon ^{[1] [3] [6]}	1979
vlanmode ^{[1] [3] [6]}	1981
statistics ^{[1] [2] [3] [4] [5] [6] [7]}	1983
exp-ingress-mapping ^{[1] [3] [6]}	1985
47. Network Policy Commands.....	1987
voice vlan	1987
voice-signaling vlan	1989
48. OpenFlow.....	1991
clear-flows	1991
controller	1993
filter-group-prio	1995
mode	1997
native-vlan	1999
rem-ssl-file	2001
shutdown	2002
strip-fcs.....	2004
49. Route-map Commands.....	2006
continue	2006
match as-path	2008
match community	2011
match extcommunity	2014
match ip address	2017
match ip next-hop.....	2019
match ip route-source	2021
match metric	2023
set as-path.....	2025
set as-path-limit	2027
set community	2029
set extcommunity	2031
set local-preference	2033
set metric	2035
set next-hop	2037
set origin.....	2039
set weight	2041
50. Router BGP Commands.....	2043
address-family	2043
aggregate-address	2045
bgp always-compare-med	2048
bgp client-to-client reflection	2050
bgp cluster-id.....	2052
bgp confederation identifier	2054
bgp confederation peers	2056
bgp dampening.....	2058

bgp dampening half-life	2060
bgp dampening max-suppress-time	2062
bgp dampening reuse	2064
bgp dampening route-map	2066
bgp dampening suppress	2068
bgp default local-preference	2070
bgp deterministic-med	2072
bgp_enforce_first_as	2074
bgp graceful-restart	2075
bgp log-neighbor-changes	2077
bgp router-id	2079
default-metric	2081
distance	2083
neighbor activate	2085
neighbor advertisement-interval	2087
neighbor bfd enable	2089
neighbor bfd interval	2091
neighbor description	2093
neighbor enforce first as	2095
neighbor ebgp-multihop	2097
neighbor local-address	2099
neighbor local-port	2101
neighbor maximum-prefix	2103
neighbor next-hop-self	2105
neighbor passive	2107
neighbor password	2109
neighbor port	2111
neighbor prefix-list	2113
neighbor peer-group	2115
neighbor remote-as	2118
neighbor remove-private-as	2120
neighbor route-map	2122
neighbor route-reflector-client	2124
neighbor send-label ^{[1] [3] [5]}	2126
neighbor shutdown	2128
neighbor soft-reconfiguration inbound	2130
neighbor timers	2132
network	2134
peer-group	2136
peer-group activate	2138
peer-group advertisement-interval	2140
peer-group description	2142
peer-group ebgp-multihop	2144
peer-group local-address	2146
peer-group local-port	2148
peer-group maximum-prefix	2150
peer-group next-hop-self	2152
peer-group passive	2154

peer-group port.....	2156
peer-group prefix-list.....	2158
peer-group password	2160
peer-group remote-as	2162
peer-group remove-private-as	2165
peer-group route-map.....	2167
peer-group route-reflector-client	2169
peer-group shutdown.....	2171
peer-group soft-reconfiguration inbound	2173
peer-group timers	2175
redistribute.....	2177
timers bgp.....	2179
51. Router ISIS Commands	2181
authentication direction recv-only	2181
authentication direction send-only	2183
authentication key-chain	2185
authentication mode clear-text	2187
authentication mode hmac-md5	2189
distance.....	2191
graceful-restart	2193
is-type.....	2195
lsp-gen-interval max-lsp-int	2197
lsp-gen-interval min-lsp-int.....	2199
max-age	2201
metric-style.....	2203
net.....	2205
redistribute.....	2207
set-attached.....	2209
summary-address	2211
vrf	2213
52. Router OSPF Commands.....	2215
abr-type	2215
area <i>id/ip-address_id</i> authentication	2217
area <i>id/ip-address_id</i> default-cost.....	2219
area <i>id/ip-address_id</i> nssa	2221
area <i>id/ip-address_id</i> range	2223
area <i>id/ip-address_id</i> stub	2225
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i>	2227
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> authentication	2229
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> authentication-key	2231
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> dead-interval	2233
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> hello-interval.....	2235
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> message-digest-key	2237
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> retransmit-interval	2239
area <i>id/ip-address_id</i> virtual-link <i>ip-address</i> transmit-delay	2241
auto-cost reference-bandwidth.....	2243
compatible rfc1583	2245

default-information-originate	2247
default-metric	2249
distance	2251
log-adjacency-changes	2253
max-metric router-lsa	2255
mpls ldp sync ^{[1] [3] [6]}	2257
mpls traffic-eng ^{[1] [3] [6]}	2259
neighbor	2261
network	2263
nsf	2265
passive-interface	2267
redistribute	2269
refresh timer	2271
router-id	2273
timers spf	2275
timers throttle spf	2277
53. Router OSPFv3 Commands.....	2279
area <i>id</i> / <i>ipv4-address_id</i> default-cost	2279
area <i>id</i> / <i>ipv4-address_id</i> nssa	2281
area <i>id</i> / <i>ipv4-address_id</i> stub	2283
area <i>id</i> / <i>ip-address_id</i> virtual-link <i>ip-address</i>	2285
area <i>id</i> / <i>ip-address_id</i> virtual-link <i>ip-address</i> dead-interval	2287
area <i>id</i> / <i>ip-address_id</i> virtual-link <i>ip-address</i> hello-interval	2289
area <i>id</i> / <i>ip-address_id</i> virtual-link <i>ip-address</i> instance-id	2291
area <i>id</i> / <i>ip-address_id</i> virtual-link <i>ip-address</i> retransmit-interval	2293
area <i>id</i> / <i>ip-address_id</i> virtual-link <i>ip-address</i> transmit-delay	2295
auto-cost reference-bandwidth	2297
default-information-originate	2299
default-metric	2301
distance	2303
log-adjacency-changes	2305
max-metric router-lsa	2307
nsf	2309
passive-interface	2311
redistribute	2313
refresh timer	2315
router-id	2317
timers throttle spf	2319
54. Router RIP Commands.....	2321
default-metric	2321
distance	2323
network	2325
passive-interface	2327
redistribute	2329
timers basic	2331

55. Router RIPng Commands.....	2333
default-metric	2333
distance.....	2335
passive-interface.....	2337
redistribute.....	2339
timers basic	2341
56. SFLOW Commands	2343
sflow agent-ip	2343
sflow enable.....	2345
receiver enable.....	2347
sflow receiver	2349
receiver ip-address.....	2351
receiver max-datagram-size	2353
receiver port.....	2355
57. Sniffer Commands	2357
accepted.....	2357
direction	2359
enable	2361
interface-ethernet.....	2363
max-packets.....	2365
protocol	2367
show-config	2371
vlan	2373
58. Obsolete Commands.....	2375
Root Commands.....	2375
Configure Commands	2400
MPLS RSVP Commands	2428
MPLS TE Commands	2432
Router BGP Commands.....	2434
Route-Map Commands	2440
Router OSPF Commands	2442
59. Notes.....	2444

Chapter 1. Introduction

The Command Line Interface

The DmSwitch Command Reference Guide was built to help network managers in their daily tasks. This guide shows the commands that can be entered in the input prompt of the command line interface.

The commands are described with all the available parameters. Moreover, the guide also has command usage examples, related commands, usage guidelines, default values and other descriptions that will help you understand how to operate the DmSwitch.

Chapter 2. Root Commands

bpdu-protect manual-unblock

bpdu-protect manual-unblock { **ethernet** *unit-port* | **port-channel** | *portchannel* }

Description

Allows to unblock BPDU protect manually for an interface.

Syntax

Parameter	Description
ethernet <i>unit/port</i>	Specifies the Unit number/ Ethernet interface number.
port-channel <i>portchannel</i>	Specifies the Port-channel interface number

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.6	This command was introduced.

Usage Guidelines

When a port is in fail state, entering this command will manually unblock the port specified.

Example

This example shows how to manually unblock BPDU protect for interface ethernet 1.

```
DmSwitch#bpdu-protect manual-unblock ethernet 1
DmSwitch#
```

You can verify that the information was deleted by entering the **show interface counters** privileged EXEC command.

Related Commands

Command	Description
<code>cpu protocol bpdu-protect</code>	Control BPDU packets per second.
<code>switchport bpdu-protect</code>	Protect BPDUs configuration for an interface.

cfm delay-measurement

```
cfm delay-measurement { one-way | two-way } ma ma-name mep id mep-id remote-mep  
{ mac mac-address | id mep-id } [ count number [ interval { 1s | 10s | 1min | 10min } [   
wait-reply ] | wait-reply ]
```

Description

Send Ethernet frame delay measurement.

Syntax

Parameter	Description
one-way	Specifies mode One-way Ethernet frame delay measurement.
two-way	Specifies mode Two-way Ethernet frame delay measurement.
ma <i>ma-name</i>	Specifies Maintenance Association (MA) name.
mep id <i>mep-id</i>	Insert a source MEP ID value. (Range: 1-8191)
remote mep id <i>mep-id</i>	Insert a destination MEP ID. (Range: 1-8191)
remote mep mac <i>mac-address</i>	Insert a destination MEP MAC address. (Range: 1-8191)
count <i>number</i>	(Optional) Insert a frame count number. (Range: 1-65535)
interval	(Optional) Specifies a time between frames transmission. (1s 10s 1min 10min)
wait-reply	(Optional) Print reply information if two-way mode was chosen.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to measure a delay between mep id 1 and remote id 2

```
DmSwitch#cfm delay-measurement two-way ma 11 mep id 1 remote-mep id 2 wait-reply
Delay Measurement to remote MEP ID 2 waiting for reply message...
delay from 00:05:00:19:25:e9: 1714 us

Delay Measurement statistics:
1 packet(s) sent, 1 received, 0% packet loss
Average delay: 1714 (microsecond)
Average delay variation: 0 (microsecond)
```

Related Commands

Command	Description
cfm linktrace	Send Linktrace Messages.
cfm loopback	Send Loopback Messages.

cfm linktrace

```
cfm linktrace ma ma-name mep id mep-id remote-mep { mac mac-address | id mep-id } [
ttl value ]
```

Description

Send Linktrace Messages.

Syntax

Parameter	Description
ma <i>ma-name</i>	Specifies Maintenance Association (MA) name.
mep id <i>mep-id</i>	Insert a source MEP ID value. (Range: 1-8191)
remote mep id <i>mep-id</i>	Insert a destination MEP ID. (Range: 1-8191)
remote mep mac <i>mac-address</i>	Insert a destination MEP MAC address. (Range: 1-8191)
ttl <i>value</i>	(Optional) Insert a TTL value for link trace command. (Range: 2-255)

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to send linktrace messages.

```
DmSwitch#cfm linktrace ma MA_1 mep id 11 remote-mep id 12
```

```
Linktrace to remote MEP ID 12 waiting for reply message...
Sent to 00:04:DF:17:31:3A, Transaction ID 0
```

Seq.	TTL	From	Relay	Egress Data	Ingress Data	Forwarding	
		OUI/ID	Action			Last	Next
1	63	00:04:DF	RlyHit	00:00:00 None	17:31:3A Ok	19:54:14	17:31:2E
		MEP at 00:04:DF:17:31:3A					

DmSwitch#

Related Commands

Command	Description
cfm delay-measurement	Send Ethernet frame delay measurement.
cfm loopback	Send Loopback Messages.

cfm loopback

```
cfm loopback ma ma-name mep id mep-id remote-mep { mac mac-address | id mep-id } [
count number ]
```

Description

Send Loopback Messages.

Syntax

Parameter	Description
ma <i>text</i>	Specifies Maintenance Association (MA) name.
mep id <i>mep-id</i>	Insert a source MEP ID value. (Range: 1-8191)
remote mep id <i>mep-id</i>	Insert a destination MEP ID. (Range: 1-8191)
remote mep mac <i>mac-address</i>	Insert a destination MEP MAC address.
count <i>number</i>	(Optional) Insert a number of Loopback Messages to be sent. (Range: 1-10)

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how send loopback messages.

```
cfm loopback ma MA_1 mep id 12 remote-mep id 11 count 5
```

```
Loopback to remote MEP ID 11 waiting for reply message
Received from 00:05:00:19:25:e9, transaction ID 0
Received from 00:05:00:19:25:e9, transaction ID 1
Received from 00:05:00:19:25:e9, transaction ID 2
Received from 00:05:00:19:25:e9, transaction ID 3
Received from 00:05:00:19:25:e9, transaction ID 4
```

```
DmSwitch#
```

Related Commands

Command	Description
<code>cfm delay-measurement</code>	Send Ethernet frame delay measurement.
<code>cfm linktrace</code>	Send Linktrace Messages.

clear capture

```
clear capture { filename | all }
```

Description

Clears packet capture files stored in the DmSwitch.

Syntax

Parameter	Description
<i>filename</i>	Name of the file to be deleted.
all	Clear all files.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear all packet capture files.

```
DmSwitch#clear capture all
DmSwitch#
```

Related Commands

Command	Description
copy	Copies configuration and firmware.

Command

`show capture file`
`show capture files`

Description

Show packets captured contained in a file.
Shows a list of files containing packet captures.

clear core-dump

```
clear core-dump [ standby-mpu | unit unit-number ] { filename | all }
```

Description

Clears applications core dump files.

Syntax

Parameter	Description
<i>filename</i>	File name.
all	Clear all core files.
standby-mpu	(Optional) Indicates that the core files will be cleaned from the standby MPU.
unit <i>unit-number</i>	(Optional) Indicates the unit for which the core files will be cleaned. (Range: 1-8)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.
14.0	Added standby-mpu option for cleaning coredumps.

Usage Guidelines

Not available.

Example

This example shows how to clear core dump file.

```
DmSwitch#clear core-dump strace.15227.2752.7011e6c1.core.gz
DmSwitch#
```

Related Commands

Command	Description
<code>show core-dump</code>	Shows the files stored in a core files directories.
<code>copy</code>	Copies configuration and firmware.

clear counter

```
clear counter { ingress | egress } [ filter-counter-id ]
```

Description

Clears filter counters.

Syntax

Parameter	Description
<i>ingress</i>	Selects ingress mode filters.
<i>egress</i>	Selects egress mode filters.
<i>filter-counter-id</i>	(Optional) Clears only the counter with the specified ID. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced. It replaces the command clear ffpcounters .

Usage Guidelines

Entering this command without parameters, all filter counters will be cleared.

Example

This example shows how to clear all filter counters.

```
DmSwitch#clear counter ingress
DmSwitch#
```

You can verify that the information was deleted by entering the **show counter** privileged EXEC command.

Related Commands

No related command.

clear cpu arp-table

clear cpu arp-table [*ip-address*]

Description

Deletes entries from the CPU ARP table.

Syntax

Parameter	Description
<i>ip-address</i>	(Optional) Clears only the entry that contains the specified IP address.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.1	This command was introduced. Before this was called clear cpu-arp-table .

Usage Guidelines

Not available.

Example

This example shows how to delete the entry that contains the specified IP address.

```
DmSwitch#clear cpu arp-table 192.168.0.1
DmSwitch#
```

You can verify that the information was deleted by entering the **show cpu arp-table** privileged EXEC command.

Related Commands

Command	Description
show cpu	Shows CPU information.

clear cpu counters queues

clear cpu counters queues [**unit** *unit-number*]

Description

Clear counters for CPU interface queues.

Syntax

Parameter	Description
unit <i>unit-number</i>	(Optional) Shows counters for specific unit.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.0	Command is appended to clear cpu options.

Usage Guidelines

If you enter this command without specifying an unit, counters for all units will be cleared.

Example

This example illustrates how to show the CPU counters queues.

```
DmSwitch#clear cpu counters queues unit 1
DmSwitch#
```

You can verify that the counters were cleared by entering the **show cpu counters queues**

Related Commands

Command	Description
show cpu counters queues	Shows counters of CPU interface queues.

clear cpu packets

`clear cpu packets`

Description

Clear all cpu packet counters.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
6.0	No modifications yet.

Usage Guidelines

Not available.

Example

This example shows how to clear the cpu packet counters.

```
DmSwitch#clear cpu packets
```

You can verify that the information was deleted by entering the **show cpu packets** privileged EXEC command.

Related Commands

Command	Description
show cpu	Shows CPU information.

clear elmi

clear elmi interface ethernet [*unit-number/*] *port-number* **error-counters**

Description

Clears Ethernet Local Management Interface counters.

Syntax

Parameter	Description
interface ethernet [<i>unit-number/</i>] <i>port-number</i>	Clears the counters from the specified unit and port.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear UNI error counters.

```
DmSwitch#clear elmi interface ethernet 5 error-counters
DmSwitch#
```

You can verify that the information was deleted by entering the **show elmi interface ethernet 5 detail** privileged EXEC command.

Related Commands

Command	Description
show elmi	Shows Ethernet Local Management Interface settings.

Command

`show running-config`
`elmi`

Description

Shows the current operating configuration.
Enters on Ethernet Local Management Interface
protocol configuration mode.

clear interface counters

```
clear interface counters [ ethernet { all | [unit-number/ ]port-number| range
[ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } | port-channel {
port-number | all | range { [ first-port-number ] [ last-port-number ] } | stacking { all
| [ unit-number/ ] stack-port } } | bundle { all | [ unit-number/ ] bundle-id | range [ first-
unit-number/ ] first-bundle-id [ last-unit-number/ ] last-bundle-id } | { [ jitter-buffer-history
] } | ptp { all | [ unit-number/ ] ptp-id | range [ first-unit-number/ ] first-ptp-id [ last-unit-
number/ ] last-ptp-id } | { pwe3-chipset unit unit-number } | { ptp-chipset unit
unit-number } ]
```

Description

Clear counters on an ethernet interface, a port-channel or all ports.

Syntax

Parameter	Description
ethernet all	(Optional) Clears counters on all ethernet ports.
ethernet [unit-number/] port-number	(Optional) Clears counters on a specified unit and port. (Range: 1-1/1-28)
ethernet range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	(Optional) Clears counters for a specific range of units and ports. (Range: 1-1/1-28)
bundle { all range { [first-unit-number/] first-bundle-id [last-unit-number/] last-bundle-id }	(Optional) Clears counters for a specific range of bundles. (Range: 1-1/1-256)
port-channel port-number	(Optional) Clears counters on a specified port. (Range: 1-128)
port-channel all	(Optional) Clears counters on all port-channels ports.
port-channel range { [first-port-number] [last-port-number] }	(Optional) Clears counters for a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
stacking all	(Optional) Clears counters on all stacking ports in the stack.
stacking [unit-number/] stack-port	(Optional) Clears counters for a specific stacking port. (Range: depends on the switch model and can be viewed with CLI's built-in help -- press "?").
ptp { all range { [first-unit-number/] first-ptp-id [last-unit-number/] last-ptp-id }	(Optional) Clears counters for a specific range of ptp interfaces. (Range: 1-1/1-16)
ptp-chipset unit unit-number	(Optional) Clears ptp-chipset counters for a specific unit.
pwe3-chipset unit unit-number	(Optional) Clears pwe3-chipset counters for a specific unit.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
6.2	This command was introduced. It replaces the command clear counters .
11.2	The options range and all in the command port-channel were introduced.
13.2	The commands bundle, ptp and chipset-pwe3 were introduced.
13.2	The commands bundle, ptp, ptp-chipset and pwe3-chipset were introduced.

Usage Guidelines

If you enter **clear interface counters** without parameters, the counters on all ports will be cleared.

Example

This example shows how to delete counters on interface ethernet port 1.

```
DmSwitch#clear
interface counters ethernet 1
DmSwitch#
```

The example below shows how to delete counters on the port-channels ranging from 1 to 2.

```
DmSwitch#clear
interface counters port-channel range 1 2
DmSwitch#
```

For both examples above, you can verify that the information was deleted by entering the **show interface counters** privileged EXEC command.

Stacking port example: for clearing counters on stacking port S1 of unit 2, you can enter the command below.

```
DmSwitch#clear
interface counters stacking 2/S1 DmSwitch#
```

Related Commands

Command	Description
show interfaces counters	Shows the interface counters information.

clear interface queue-counters

```
clear interface queue-counters [ ethernet { all | [ unit-number / ] port-number | range [ first-unit-number / ] first-port-number [ last-unit-number / ] last-port-number } | port-channel { port-number }
```

Description

Clear counters on an ethernet interface, a port-channel or all ports.

Syntax

Parameter	Description
ethernet all	(Optional) Clears counters on all ethernet ports.
ethernet [<i>unit-number</i> /] <i>port-number</i>	(Optional) Clears counters on a specified unit and port.
ethernet range { [<i>first-unit-number</i> /] <i>first-port-number</i> [<i>last-unit-number</i> /] <i>last-port-number</i> }	(Optional) Clears counters for a specific range of units and ports.
port-channel <i>port-number</i>	(Optional) Clears counters on a specified port.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, the queue counters on all ports will be cleared.

Example

This example shows how to delete queue counters on interface ethernet port 1.

```
DmSwitch#clear interface queue-counters ethernet 1
DmSwitch#
```

Other example shows how to delete queue counters on interface portchannel 2.

```
DmSwitch#clear interface queue-counters port-channel 2
DmSwitch#
```

For both examples, you can verify that the information was deleted by entering the **show interfaces table queue** privileged EXEC command.

Related Commands

Command	Description
show interfaces table queue-12	Shows counters of all queues of a specific interface.

clear interface test

```
clear interface test [ bundle { all | [ unit-number/ ] port-number | range [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } | port-channel { port-number | all | range { [ first-port-number ] [ last-port-number ] } | }
```

Description

Clear test counters on a bundle interface, or all bundles.

Syntax

Parameter	Description
bundle all	(Optional) Clears test counters on all bundle interfaces.
ethernet [unit-number/] port-number	(Optional) Clears test counters on a specified bundle. (Range: 1-1/1-256)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Entering this command without parameters, the test counters on all bundles will be cleared.

Example

This example shows how to delete counters on interface bundle 1.

```
DmSwitch#clear interface test bundle 1
DmSwitch#
```

You can verify that the information was deleted by entering the **show interfaces test** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces test</code>	the Section called <i>show interfaces test bundle</i>

clear dump

```
clear dump { filename | all }
```

Description

This command remove the dump files.

Syntax

Parameter	Description
<i>filename</i>	File name.
<i>all</i>	Clear all dump files.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear all dump files.

```
DmSwitch#clear dump all
DmSwitch#
```

Related Commands

Command	Description
dump	Generate an dump file.

Command

show dump

copy

Description

Shows the files stored in the dumps directory.

Copies configuration and firmware.

clear ip arp

```
clear ip arp [ interface { ethernet [ unit-number/ ] port-number | port-channel  
channel-group-number | vlan vlan-number } ]
```

Description

Deletes the ARP cache entries.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Clears the entries from the specified unit and port.
port-channel <i>channel-group-number</i>	(Optional) Clears the entries from the specified port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
vlan <i>vlan-number</i>	(Optional) Clears the entries from the specified VLAN. The VLAN must be specified in accordance with the VLAN configured in the switch. (Range: 1-4094)

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If no **interface** parameter is specified, the entire ARP cache will be cleared.

Example

This example shows how to clear the entire ARP cache on the specified VLAN interface.

```
DmSwitch#clear ip arp interface vlan 1
DmSwitch#
```

Related Commands

Command	Description
<code>show ip hardware</code> <code>host-table</code>	Shows the hardware host table.

clear ip bgp

```
clear ip bgp [ { dampening ipaddress/mask | flap-statistic ipaddress/mask | process |  
* {soft-in} | ipaddress {soft-in} } ]
```

Description

Clear BGP connections.

Syntax

Parameter	Description
dampening	Clear dampening information and unsuppress route.
flap-statistics	Clear route flap statistics.
process	Resets the BGP process.
* soft-in	Resets all BGP connections.
<i>ipaddress</i> soft-in	Specifies a connection to be reset.
soft-in	(Optional)Soft inbound reset issuing a route refresh.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.
9.4	New parameters added: bgp process and soft-in
12.4	New parameters added: bgp dampening and flap-statistic

Usage Guidelines

Not available.

Example

This example shows how to clear all BGP connections.

```
DmSwitch#clear ip bgp *  
DmSwitch#
```

Related Commands

Command	Description
<code>show ip route bgp</code>	Shows the IP routing table.

clear ip dhcp server

```
clear ip dhcp server leases all
```

Description

Clear DHCP server leases database..

Syntax

Not available.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear the DHCP server leases database.

```
DmSwitch#clear ip dhcp server leases all
All leases will be lost. Are you sure ? <y/N> y
DmSwitch#
```

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.

Command	Description
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

clear ip dhcp snooping

```
clear ip dhcp snooping { database | statistics }
```

Description

Clears counters on DHCP Snooping statistic table and deletes DHCP Snooping database entries.

Syntax

Parameter	Description
database	Deletes all DHCP Snooping database entries.
statistics	Clears all DHCP Snooping statistic counters.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear the entire DHCP Snooping Database entries and how to reset DHCP Snooping statistic table.

```
DmSwitch#clear ip dhcp snooping database
DmSwitch#
DmSwitch#clear ip dhcp snooping statistics
DmSwitch#
```

Related Commands

Command	Description
<code>ip dhcp snooping vlan binding</code>	Creates a DHCP Snooping Database entry
<code>show ip dhcp snooping database</code>	Shows DHCP Snooping Database informations.
<code>show ip dhcp snooping statistics</code>	Shows DHCP Snooping statistics.

clear ip ospf

```
clear ip ospf [ process { vrf vrf_name } ]
```

Description

Clear OSPF routing data.

Syntax

Parameter	Description
process vrf <i>vrf_name</i>	Reset OSPF process.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	New parameters added: ospf process

Usage Guidelines

Not available.

Example

This example shows how to reset the OSPF process.

```
DmSwitch#clear ip ospf process
DmSwitch#
```

Related Commands

Command	Description
<code>show ip route ospf</code>	Shows the IP routing table.

clear ip path-mtu-discovery cache

```
clear ip path-mtu-discovery cache [ ip-address ]
```

Description

Clear Path MTU Discovery cache entries.

Syntax

Parameter	Description
<i>ip-address</i>	Clear only cache entries with given destination ip address

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear all Path MTU Discovery entries.

```
DmSwitch#clear ip path-mtu-discovery cache
DmSwitch#
```

Related Commands

Command	Description
<code>show ip</code> <code>path-mtu-discovery cache</code>	Shows the IP Path MTU Discovery cache entries.
<code>show ipv6</code> <code>path-mtu-discovery cache</code>	Shows the IPv6 Path MTU Discovery cache entries.
<code>clear ipv6</code> <code>path-mtu-discovery cache</code>	Clear IPv6 Path MTU Discovery cache.

clear ip rip

```
clear ip rip [ process ]
```

Description

Clear RIP routing data.

Syntax

Parameter	Description
process	Reset RIP process.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	New parameters added: rip process

Usage Guidelines

Not available.

Example

This example shows how to reset the RIP process.

```
DmSwitch#clear ip rip process
DmSwitch#
```

Related Commands

Command	Description
default-metric	Defines the default metric of RIP protocol.
distance	Defines the administrative distance of RIP protocol.
network	Associates a network with a RIP routing process.
passive-interface	Suppresses RIP routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIP protocol.
router rip	Enables and accesses the RIP configuration.
show ip rip	Shows the RIP process parameters.
show ip rip neighbor	Shows RIP neighbors
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIP protocol.

clear ipv6 bgp

```
clear ipv6 bgp [ { dampening ipv6address/mask | flap-statistic ipv6address/mask |  
process | * {soft-in} | ipv6address {soft-in} ]
```

Description

Clear BGPv4 connections.

Syntax

Parameter	Description
dampening	Clear dampening information and unsuppress route.
flap-statistics	Clear route flap statistics.
process	Resets the BGPv4 process.
* soft-in	Resets all BGPv4 connections.
<i>ipv6address</i> soft-in	Specifies a connection to be reset.
soft-in	(Optional)Soft inbound reset issuing a route refresh.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.
9.4	New parameters added: bgp process and soft-in
12.4	New parameters added: bgp dampening and flap-statistic

Usage Guidelines

Not available.

Example

This example shows how to clear all BGP connections.

```
DmSwitch#clear ipv6 bgp *  
DmSwitch#
```

Related Commands

Command	Description
<code>show ipv6 route bgp</code>	Shows the IPv6 routing table.

clear ipv6 ospfv3

```
clear ipv6 ospfv3 [process]
```

Description

Clear OSPFv3 routing data.

Syntax

Parameter	Description
process	Reset OSPFv3 process.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	New parameters added: ospfv3 process

Usage Guidelines

Not available.

Example

This example shows how to reset the OSPFv3 process.

```
DmSwitch#clear ipv6 ospfv3 process
DmSwitch#
```

Related Commands

Command	Description
<code>show ipv6 route ospf</code>	Shows the IPv6 routing table.

clear ipv6 path-mtu-discovery cache

```
clear ipv6 path-mtu-discovery cache [ ipv6-address ]
```

Description

Clear Path MTU Discovery cache entries.

Syntax

Parameter	Description
<i>ipv6-address</i>	Clear only cache entries with given destination IPv6 address

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear all Path MTU Discovery entries.

```
DmSwitch#clear ipv6 path-mtu-discovery cache
DmSwitch#
```

Related Commands

Command	Description
<code>show ipv6 path-mtu-discovery cache</code>	Shows the IPv6 Path MTU Discovery cache entries.
<code>show ip path-mtu-discovery cache</code>	Shows the IP Path MTU Discovery cache entries.
<code>clear ip path-mtu-discovery cache</code>	Clear IP Path MTU Discovery cache.

clear ipv6 ripng

```
clear ipv6 ripng [ process ]
```

Description

Clear RIPng routing data.

Syntax

Parameter	Description
process	Reset RIPng process.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	New parameters added: ripng process

Usage Guidelines

Not available.

Example

This example shows how to reset the RIPng process.

```
DmSwitch#clear ip ripng process
DmSwitch#
```

Related Commands

Command	Description
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

clear logging

```
clear logging { flash | ram } [ internal ]
```

Description

Deletes log messages from flash or RAM memory.

Syntax

Parameter	Description
flash	Deletes log messages from flash memory.
ram	Deletes log messages from RAM memory.
internal	Deletes internal events from memory. This option requires authentication.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.0	The optional internal was introduced.

Usage Guidelines

Not available.

Example

This example show how to delete log messages from flash.

```
DmSwitch#clear logging flash
DmSwitch#
```

You can verify that the information was deleted by entering the **show logging** privileged EXEC command.

Related Commands

Command	Description
<code>logging facility</code>	Sets the facility type for remote logging.
<code>logging history</code>	Configures the level of local events.
<code>logging host</code>	Configures a remote syslog server.
<code>logging on</code>	Enables the logging of events.
<code>logging sendmail</code>	Enables and configures the sending of logs via e-mail.
<code>logging trap</code>	Configures the level of events that will be sent to remote syslog.
<code>show logging</code>	Shows logging configuration.

clear lldp

```
clear lldp { counters | neighbors }
```

Description

Clears LLDP counters or table of neighbors.

Syntax

Parameter	Description
counters	Clears all counters: global and for all ports.
neighbors	Clears entire neighbors table.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to clear UNI error counters.

```
DmSwitch#clear lldp neighbors
DmSwitch#
```

You can verify that the information was deleted by entering the **show lldp neighbors** privileged EXEC command.

Related Commands

Command	Description
show lldp	Shows LLDP configuration information.

Command

`show lldp counters`

`show lldp neighbor`

`lldp`

Description

Shows LLDP counters information.

Shows LLDP neighbor information.

Enables the LLDP operation in the DmSwitch.

clear mac-address-table

```
clear mac-address-table [ { ethernet [ unit-number/ ] port-number | port-channel  
channel-group-number | vlan vlan-number unicast | vpn vpn-id } ]
```

Description

Deletes dynamically learned L2 entries from MAC address table.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Clears the entries from the specified unit and port.
port-channel <i>channel-group-number</i>	(Optional) Clears the entries from the specified port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
vlan <i>vlan-number</i>	(Optional) Clears the entries from the specified VLAN. The VLAN must be specified in accordance with the VLAN configured in the switch. (Range: 1-4094)
vpn <i>vpn-id</i>	(Optional) Clears the entries from the specified VPN.
mrouter	Deletes multicast routers entries.
multicast	Deletes multicast entries.
unicast	Deletes unicast entries.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
10.0	New parameter vpn .

Usage Guidelines

Entering this command without parameters, the entire dynamic unicast table will be cleared.

Example

This example shows how to clear specific port unicast entries from MAC address table.

```
DmSwitch#clear mac-address-table ethernet 20 unicast
DmSwitch#
```

You can verify that the information was deleted by entering the **show mac-address-table** privileged EXEC command.

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table.

clear meter

clear meter [*meter-number*]

Description

Clears the packet counters of the meter.

Syntax

Parameter	Description
<i>meter-number</i>	(Optional) Clears the packet counters of a specified meter. (Range: 1-63)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced. Before this was called clear meters .

Usage Guidelines

Entering this command without parameters, all meter counters will be cleared.

Example

This example shows how to clear the counters of meter 3.

```
DmSwitch#clear meter 3
DmSwitch#
```

Related Commands

No related command.

clear mpls ^[1] ^[3] ^[6]

clear mpls

Description

This command resets all MPLS products - LDP, RSVP and VPNs.

Syntax

Parameter	Description
mpls	Reset MPLS products.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is very similar to **mpls ldp graceful-restart**. Both commands reset all MPLS products. There is just one difference, **clear mpls** does not change graceful-restart configuration.

Example

This example shows how to reset the MPLS products.

```
DmSwitch#clear mpls
DmSwitch#
```

You can verify that the MPLS products were restarted by entering the **show mpls ldp neighbor** privileged EXEC command or the **show mpls te traffic-eng tunnels** privileged EXEC command.

Related Commands

Command	Description
<code>show mpls ldp neighbor</code>	Shows the status of LDP sessions.
<code>show mpls te traffic-eng tunnels</code>	Shows Traffic Engineering Tunnel Information
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.

clear mpls l2vpn ^[1] ^[3] ^[5]

```
clear mpls l2vpn counters [ vpn id]
```

Description

Deletes entries from the MPLS L2VPN counters.

Syntax

Parameter	Description
counters	Clear MPLS counters.
vpn id	(optional) The VPN identifier.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to delete the entry that contains the specified vpn.

```
DmSwitch#clear mpls l2vpn counters vpn 900
DmSwitch#
```

Example 2

This example shows how to delete all the entries.

```
DmSwitch#clear mpls l2vpn counters
DmSwitch#
```

Related Commands

Command	Description
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.

clear mpls ldp ^[1] ^[3] ^[6]

```
clear mpls { ldp }
```

Description

Restart MPLS LDP components - BVM, AFM3107, DMLBI, LDP-PM and LDP-SC.

Syntax

Parameter	Description
ldp	Restart MPLS LDP components.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.10	This command was introduced.
15.0	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to restart the MPLS LDP components.

```
DmSwitch#clear mpls ldp
DmSwitch#
```

You can verify that the MPLS LDP components were restarted by entering the **show mpls l2vpn** privileged EXEC command or the **show mpls ldp neighbor** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show mpls ldp database</code>	List LSP database
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.
<code>show mpls ldp neighbor</code>	Shows the status of LDP sessions.

clear mpls-oam [1] [3] [6]

```
clear mpls-oam { db }
```

Description

Deletes entries from the MPLS OAM database.

Syntax

Parameter	Description
db	Delete all the information on the MPLS OAM database.
db handle <i>handle-id</i>	(optional) Clear only the entry specified by handle.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to delete the entry that contains the specified handle.

```
DmSwitch#clear mpls-oam db handle 12456
DmSwitch#
```

You can verify that the information was deleted by entering the **show mpls oam db handle 12345** privileged EXEC command or the **show mpls oam db** privileged EXEC command.

Example 2

This example shows how to delete all the entries.

```
DmSwitch#clear mpls-oam db
DmSwitch#
```

You can verify that the information was deleted by entering the **show mpls oam db** privileged EXEC command.

Related Commands

Command	Description
show mpls oam	Shows MPLS OAM information.

clear spanning-tree counters

```
clear spanning-tree counters [ ethernet { all | [ unit-number/ ] port-number | range {  
[ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } | instance instance-  
index | port-channel channel-group-number ]
```

Description

Clears the spanning-tree counters for a specific instance, for specific interfaces or for all instances and interfaces.

Syntax

Parameter	Description
ethernet	(Optional) Clears Ethernet port(s).
all	Clears the per-interface counters for all Ethernet ports on all instances.
[<i>unit-number/</i>] <i>port-number</i>	Clears the per-interface counters for a specific unit and port on all instances.
range { [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i> }	Clears the per-interface counters for a range of specific units and ports on all instances.
instance <i>instance-index</i>	(Optional) Clears the instance global counters and the instance per-interface counters on all interfaces for a specific instance . (Range: 0-15)
port-channel <i>channel-group-number</i>	(Optional) Clears the per-interface counters for a specific port channel on all instances. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The spanning-tree counters exist on a per instance basis (such as the topology changes counter) or on a per

instance and interface basis (such as the transmitted and received BPDUs counters). Instance counters are cleared when a specific instance or all instances are specified. Interface counters are cleared when a specific interface, a specific instance or all instances are specified.

Entering this command without parameters, all instances and interfaces will be cleared.

Example

This example shows how to clear the spanning-tree counters for instance 1.

```
DmSwitch#clear spanning-tree counters instance 1
DmSwitch#
```

You can verify that the counters were cleared by entering the **show spanning-tree** *instance* privileged EXEC command.

Related Commands

Command	Description
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
show spanning-tree	Shows spanning-tree configuration and status.

clear spanning-tree detected-protocols

```
clear spanning-tree detected-protocols [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } | port-channel channel-group-number ]
```

Description

Restarts the spanning-tree protocol migration mechanism for specific interfaces or for all interfaces.

Syntax

Parameter	Description
ethernet	(Optional) Resets Ethernet port(s).
all	Restarts for all Ethernet ports.
[<i>unit-number/</i>] <i>port-number</i>	Restarts for a specific unit and port.
range { [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i> }	Restarts for a range of specific units and ports.
port-channel <i>channel-group-number</i>	(Optional) Restarts for a specific port-channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

When using the RSTP or MSTP modes for spanning-tree the equipment can enter a compatibility mode in order to interoperate with bridges using the original Spanning-Tree Protocol (802.1D). This is a per-interface process that occurs based on the type of received BPDUs.

However, those newer protocols do not implement a mechanism to automatically exit the compatibility mode. You must use this command when it is needed, which will occur when a connected bridge changes its spanning-

tree mode from STP to a newer protocol version.

Entering this command without parameters, all interfaces will be reseted.

Example

This example shows how to reset the detected protocol version for interface ethernet 1/1.

```
DmSwitch#clear spanning-tree detected-protocols ethernet 1/1
DmSwitch#
```

You can verify that the detected version was reset by entering the **show spanning-tree instance interface** privileged EXEC command.

Related Commands

Command	Description
spanning-tree mode	Configures the spanning-tree mode.
show spanning-tree	Shows spanning-tree configuration and status.

clear snmp counters

```
clear snmp counters [ ethernet { all | [ unit-number/ ] port-number | range [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } | port-channel { port-number } ]
```

Description

Clear the snmp counters on an ethernet interface, a port-channel or all ports.

Syntax

Parameter	Description
ethernet all	(Optional) Clears the snmp counters on all ethernet ports.
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Clears the snmp counters on a specified unit and port. (Range: 1-1/1-24)
ethernet range { [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i> }	(Optional) Clears the snmp counters for a specific range of units and ports. (Range: 1-1/1-28)
port-channel <i>port-number</i>	(Optional) Clears the snmp counters on a specified port-channel. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

If you enter **clear snmp counters** without parameters, the counters on all ports will be cleared. Attempts to clear a port that is in a port-channel will fail, you need to clear the port-channel or remove the interface ethernet from it. The execution of this command will not clear the counters shown by command **show interfaces counters**.

Example

This example shows how to clear the snmp counters on interface ethernet port 1.

```
DmSwitch#clear snmp counters ethernet 1
DmSwitch#
```

The example below shows how to clear the snmp counters on the port-channel 5.

```
DmSwitch#clear snmp counters port-channel 5
DmSwitch#
```

For both examples above, you can verify that the information was deleted consulting the counters by snmp.

Related Commands

Command	Description
<code>clear interfaces counters</code>	Shows the interface counters information.

clear stacking saved-topology

`clear stacking saved-topology`

Description

Clear stacking saved topology information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Unsaved topology does not ensure complete formation of stacking, and may fail in data traffic when performed operations on the stack, especially the operations causing split.

Recommend saving the topology information.

Example

This example shows how to clear stacking saved topology information.

```
DmSwitch#clear stacking saved-topology
DmSwitch#
```

You can verify that the information was deleted by entering the **show stacking saved-topology** privileged EXEC command.

Related Commands

Command	Description
show stacking	Show stacking information

Command	Description
<code>show stacking</code>	Show stacking saved topology
<code>saved-topology</code>	
<code>stacking</code>	Manage stacked switches

clock set

clock set { *time day month year* }

Description

Configures the system date and time.

Syntax

Parameter	Description
<i>time</i>	Specifies the time in hh:mm:ss format. (Range: 0-23/0-59/0-59)
<i>day</i>	Specifies the day of month. (Range: 1-31)
<i>month</i>	Specifies the month of year. (Range: 1-12)
<i>year</i>	Specifies the year. (Range: 1970-2037)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the system time and date.

```
DmSwitch#clock set 10:00:00 10 12 2030
DmSwitch#
```

This configuration can be verified by entering the **show clock** user EXEC command.

Related Commands

Command	Description
<code>clock timezone</code>	Specifies the time zone.
<code>show clock</code>	Shows the system clock and time zone.
<code>show uptime</code>	Shows the system clock, system uptime and load average.

configure

configure

Description

Enables the global configuration mode.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the global configuration mode.

```
DmSwitch#configure
DmSwitch(config)#
```

Related Commands

No related command.

copy

copy capture *filename* { **tftp** *ip-address**ipv6-address* [*filename*] | **scp** *ip-address**ipv6-address* [*filename*] }

copy core-dump *filename* [**standby-mpu** | **unit** *unit-number*] **tftp** *ip-address* [*filename*]

copy dump *filename* { **tftp** *ip-address**ipv6-address* [*filename*] | **scp** *ip-address**ipv6-address* [*filename*] }

copy default-config { **flash-config** *index* [*name*] | **running-config** [**unit** *unit-number*] | **startup-config** [*index* [*name*]] }

copy firmware [*index*] **standby-mpu**

copy flash-config *index* { **flash-config** *index* [*name*] | **running-config** | **tftp** *ip-address* [*filename*] | **scp** *ip-address**ipv6-address* [*filename*] }

copy log-assert **tftp** *ip-address* [*filename*]

copy log-flash **tftp** *ip-address**ipv6-address* [*filename*]

copy log-flash-internal **tftp** *ip-address**ipv6-address* [*filename*]

copy log-ips **tftp** *ip-address* [*filename*]

copy log-mem-dump **tftp** *ip-address* [*filename*]

copy log-mem-stat **tftp** *ip-address* [*filename*]

copy log-pd **tftp** *ip-address* [*filename*]

copy log-ipc **tftp** *ip-address* [*filename*]

copy log-ram **tftp** *ip-address**ipv6-address* [*filename*]

copy log-ram-internal **tftp** *ip-address**ipv6-address* [*filename*]


```
copy profile-config metro { flash-config index [ name ] | running-config [ unit
unit-number ] | startup-config [ index [ name ] ] }
```

```
copy running-config { flash-config index [ name ] | startup-config [ index [ name ] ] |
tftp ip-address [ filename ] | scp ip-addressip-v6-address [ filename ] }
```

```
copy scp ip-addressip-v6-address filename { firmware [ unit { unit-number | range first-unit-
number last-unit-number } ] | flash-config index | running-config | startup-config [
index ] }
```

```
copy startup-config { flash-config index [ name ] | running-config | tftp ip-address
[ filename ] }
```

```
copy tftp ip-address filename { firmware [ unit { unit-number | range first-unit-number last-
unit-number } ] | flash-config index | running-config | startup-config [ index ] }
```

Description

Copies an equipment configuration or firmware from an origin to a destination.

Syntax

Parameter	Description
capture <i>filename</i>	Specifies a name of a packet capture file.
core-dump <i>filename</i>	Specifies a file name of application core dump.
default-config	Default configuration of DmSwitch.
flash-config <i>index</i>	Specifies a flash configuration memory position. (Range: 1-4)
dump <i>filename</i>	Specifies a file name of an dump.
log-flash	Specifies log from flash.
log-flash-internal	Specifies internal log from flash.
log-ram	Specifies log from RAM.
log-ram-internal	Specifies internal log from RAM.
profile-config metro	Specifies predefined DmSwitch profile configuration.
running-config	Current configuration running in DmSwitch.
startup-config	Configuration in the flash memory that is set as startup.
tftp <i>ip-address</i> <i>filename</i>	Specifies the server where the configuration, core-dump or firmware will be captured/sent and its filename.
scp <i>ip-address</i> <i>ip-v6-address</i> <i>filename</i>	Specifies the server where the configuration, core-dump or firmware will be captured/sent and its filename.

Parameter**tftp** *ip-address***scp** *ip-address**ip6-address***standby-mpu****firmware***name**filename**unit-number***range** *first-unit-number last-unit-number***Description**

Specifies the server where the configuration will be captured. Since the filename is not specified, when sending a flash-config/startup-config the filename is the name of the configuration, or `<Hostname>_<FlashIndex>` if the configuration has no name. The filename is "running" when sending running-config.

Specifies the server where the configuration will be captured. Since the filename is not specified, when sending a flash-config/startup-config the filename is the name of the configuration, or `<Hostname>_<FlashIndex>` if the configuration has no name. The filename is "running" when sending running-config.

Specifies that the command will be executed for the standby MPU.

Indicates that the transferred file must be saved as a firmware. This new firmware will be saved in a position other than the one that has the running firmware.

(Optional) When you save a configuration to a flash position, you can specify a name for the configuration.

(Optional) When you save a configuration to a file using tftp, you can specify a filename.

(Optional) Specifies the unit where the transferred file must be saved as a firmware.

(Optional) Specifies a range of units where the transferred file must be saved as a firmware.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
6.6	The options log-flash and log-ram were introduced.
13.4	IPv6 address support to scp.
13.6	Added dumps support.
14.0	The options log-flash-internal and log-ram-internal were introduced.
14.0	Added standby-mpu option for copy of coredumps.

Usage Guidelines

It is not possible copy a configuration to a **profile-config** or to the **default-config**.

If you specify **startup-config** as the destination of the copy command and you do not specify a flash configuration memory position, the configuration will be saved in the flash configuration memory position that is marked as startup, keeping the same name. When you execute the same command and specify a memory position, it will be copied and marked as startup, and you will be able to optionally set a name.

If you copy a configuration from TFTP server to DmSwitch, the name of the configuration can not be specified. It will use the same name of the file that is being copied.

When you copy a firmware from TFTP server to DmSwitch, you will only have to specify the name of the file to be transferred. Then, looking at the installed firmware, you will only be able to see their versions.

Before using a TFTP Server, it is necessary to configure the switch IP parameters.

Before using a IPv6 Server, it is necessary to configure the switch IPv6 parameters.

DmSwitch has two firmware positions in memory. When you copy a new firmware from TFTP Server, it will be copied to the position that is not the running one. If there is a firmware in that position, it will be overwritten.

The currently available predefined profile is: **metro** (configurations to be used with Metropolitan Area Networks).

Examples

This first example shows how to copy the running-config to configuration 4 in flash memory, setting it as startup configuration.

```
DmSwitch#copy running-config startup-config 4 example_name
Saving configuration in flash 4...
Done.
Setting startup-config to 4.
DmSwitch#
```

You can verify the configurations of flash and firmware by entering the **show flash** privileged EXEC command.

This second example shows how to copy the new firmware from TFTP Server to DmSwitch.

```
DmSwitch#copy tftp 10.10.10.20 DmSwitch.im firmware
Fetching image...
Image size is 7510432 bytes.
Checking image...
Image is ok.
```

```
Erasing firmware 1...
Writing image to firmware 1...
Progress: 7510432 bytes (100%) written...
Done.
Use the "reboot" command to run the new firmware.
DmSwitch#
```

You can verify the configurations of firmware by entering the **show firmware** privileged EXEC command.

Related Commands

Command	Description
diff	Compares and shows the differences between two configurations.
erase	Erases spare firmware or configuration position.
clear capture	Clear packet capture files.
clear core-dump	Clears applications core dump files.
clear dump	Clears dump files.
select	Selects the startup firmware and flash for the next reboot.
show firmware	Shows firmware information.
show flash	Shows flash information.
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.
show startup-config	Shows the startup flash configuration.
show core-dump	Shows the files stored in a core files directories.
show dump	Shows the files stored in the dumps directory.

debug

```
debug { all | aaa { accounting | authorization | authentication } | apply | arp { protection | rx | tx } | cpu { tx | rx } | dhcp snooping [ db | control ] | dot1x { event | packet-decode | packet-hex | state [ ethernet [ unit-number/ ] port-number ] } | eaps | egr-mgr | elmi { event | packet-decode | packet-hex | state [ ethernet [ unit-number/ ] port-number ] } | erps | gvrp | icmp { tx | rx } | igmp [ detail ] | intf-mgr | ipc { local | stacking } | l3core [ host ] | l3proto { ips-log | ldp-mem-dump [ clear ] | mem-log | pd-log [ clear | detail { full | summary } ] | filter { exclude | include } text | level { audit | exception | none | problem } } } | lacp | link | link-flap | logs | mpls { frr-mgr | hardware | lib { db | hw | proc } } | multicast | oam | path-mtu-discovery | ptp | stp | vrf | vrrp }
```

```
no debug { all | aaa { accounting | authorization | authentication } | apply | arp { tx | rx } | cpu { tx | rx } | dhcp snooping [ db | control ] | dot1x { event | packet-decode | packet-hex | state [ ethernet [ unit-number/ ] port-number ] } | eaps | egr-mgr | elmi { event | packet-decode | packet-hex | state [ ethernet [ unit-number/ ] port-number ] } | erps | gvrp | icmp { tx | rx } | igmp [ detail ] | intf-mgr | ipc { local | stacking } | l3core [ host ] | l3proto { ips-log | mem-log | pd-log } | lacp | link | link-flap | logs | mpls { frr-mgr | hardware | lib { db | hw | proc } } | multicast | oam | path-mtu-discovery | ptp | stp | vrf | vrrp }
```

Description

Enables the printing of debug messages related to the selected option.

Inserting **no** as a prefix for this command will disable debugging for the specified feature inserted as a parameter.

Syntax

Parameter	Description
all	Enables debug messages for all possible options of this command.
oam	Enables debug messages for OAM.
aaa	Enables debug messages for authorization, accounting and authentication protocols such as RADIUS and TACACS+.
accounting	Enables debug messages for accounting protocols such as RADIUS and TACACS+.
authorization	Enables debug messages for authorization protocols such as TACACS+.
authentication	Enables debug messages for authentication protocols such as RADIUS and TACACS+.
apply	Enables debug messages for APPLY time measurement.
arp protection	Enables debug messages for ARP protection feature.

Parameter	Description
arp rx	Enables debug messages for ARP packets received at CPU.
arp tx	Enables debug messages for ARP packets transmitted from CPU.
cpu tx	Enables debug messages for packets transmitted from CPU.
cpu rx	Enables debug messages for packets received at CPU.
dhcp snooping	Enables debug messages of DHCP Snooping feature.
dhcp snooping db	Enables debug messages about DHCP Snooping database.
dhcp snooping control	Enables debug messages about sending and receiving DHCP Snooping messages and packet inspection.
dot1x event	Enables debug messages for 802.1X events.
dot1x packet-decode	Enables debug messages for decoded 802.1X packets.
dot1x packet-hex	Enables debug messages for 802.1X packets in hexadecimal format.
dot1x state	Enables debug messages for 802.1X state machines.
eaps	Enables debug messages for EAPS.
egr-mgr	Enables debug messages for Egress Manager hardware control block.
elmi event	Enables debug messages for E-LMI events.
elmi packet-decode	Enables debug messages for decoded E-LMI packets.
elmi packet-hex	Enables debug messages for E-LMI packets in hexadecimal format.
elmi state	Enables debug messages for E-LMI state machines.
erps	Enables debug messages for ERPS.
gvrp	Enables debug messages for GVRP.
icmp tx	Enables debug messages for ICMP packets transmitted from CPU.
icmp rx	Enables debug messages for ICMP packets received at CPU.
igmp [detail]	Enable debug message for IGMP.
intf-mgr	Enables debug messages for INTF Manager hardware control block.
ipc local	Enable debug message for local IPC.
ipc stacking	Enable debug message for stacking IPC.
l3core	Enables debug messages about routes at L3 hardware interaction subsystem.
l3core host	Enables debug messages about hosts at L3 hardware interaction subsystem.
l3proto ips-log	Enables logging of internal messages. Does not print messages on screen.
l3proto ldp-mem-dump	Dump LDP/PW/Tunnel internal memory contents.
l3proto ldp-mem-dump clear	Clear all internal memory dump files.
l3proto mem-log	Enable dump of memory statistics.

Parameter	Description
<code>l3proto pd-log</code>	Enables debug messages for L3 routing protocols.
<code>l3proto pd-log clear</code>	Clear L3 protocols debug log file.
<code>l3proto pd-log detail full</code>	Enables L3 protocols debug fully detailed messages.
<code>l3proto pd-log detail summary</code>	Enables L3 protocols debug summarized messages.
<code>l3proto pd-log filter exclude text</code>	Filter excluding specified <i>text</i> .
<code>l3proto pd-log filter include text</code>	Filter only specified <i>text</i> .
<code>l3proto pd-log level audit</code>	Enables problem, exception and audit logs.
<code>l3proto pd-log level exception</code>	Enables problem and exception logs.
<code>l3proto pd-log level none</code>	Disables all logs.
<code>l3proto pd-log level problem</code>	Enables problem logs.
<code>lACP</code>	Enables debug messages for LACP.
<code>link</code>	Enables debug messages for link state changes on interfaces.
<code>link-flap</code>	Enables debug messages for link-flap.
<code>logs</code>	Enables debug messages from system logs.
<code>mpls frr-mgr</code>	Enables debug messages for Fast Re-Route manager hardware control block.
<code>mpls hardware</code>	Enables debug messages for general MPLS hardware interaction.
<code>mpls lib</code>	Enables all debug messages for Label Information Base hardware control block.
<code>mpls lib db</code>	Enables debug messages for Label Information Base database.
<code>mpls lib hw</code>	Enables debug messages for Label Information Base hardware interaction.
<code>mpls lib proc</code>	Enables debug messages for Label Information Base process.
<code>multicast</code>	Enables debug messages for multicast protocols.
<code>path-mtu-discovery</code>	Enables debug messages for Path MTU Discovery.
<code>stp</code>	Enables debug messages for STP.
<code>vrf</code>	Enables debug messages for VRF events.
<code>vrrp</code>	Enables debug messages for VRRP.

Default

No default is defined.

Command Availability

L3CORE and L3PROTO debugs are only on models with Layer 3 functionality.

MPLS and VRF debugs are only on models with MPLS functionality.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	Debugging messages were added for: ARP, GVRP, ICMP, OSPF and RIP.
5.0	Debugging messages were added for: VRRP.
9.4	Replaced BGP, OSPF and RIP by L3PROTO. Introduced L3CORE and MULTICAST messages.
10.0	Updated L3CORE and L3PROTO debugs. Introduced MPLS and VRF debugs.
11.0	Debugging messages were added for authentication, authorization and accounting protocols.
11.2	Introduced l3core host option.
11.2	Added "intf-mgr" option in MPLS debug. Update syntax of MPLS debugs.
12.0	Added "elmi" option in debug.
12.0	Introduced link-flap option.
12.2	Added "dot1x" option in debug.
13.0	Added "ipc" option in debug.
13.0	Added "tx" and "rx" options for debug arp,cpu and icmp.
13.4	Added DHCP Snooping debugs.
13.4	Moved options egr-mgr and inft-mgr from debug mpls hierarchy to debug hierarchy.
13.6	Added "erps" option in debug.
13.6	Added ARP Protection debugs.
13.0	Added apply time option in debug.
14.2	Added Path MTU Discovery debugs.
14.2	Introduced PW/Tunnel internal memory dump.

Usage Guidelines

This command enables the printing of debug messages in the current session of the command-line interface. Messages are generated for relevant events from each feature that has debugging enabled. This is a per-session option, not shared nor stored across sessions.

The **ldp-mem-dump** command creates a snapshot of control-plane internal memory contents (memory dump) when invoked, becoming inactive a few milliseconds later. For that reason, this debug option is not listed in **show debugging** command.

WARNING: The use of **debug all** or other verbose debug messages under serial interface may cause it to become inaccessible. Be careful.

Example

This example shows how to enable the printing of debug messages for STP.

```
DmSwitch#debug stp
DmSwitch#
```

You can verify that the option is enabled by entering the **show debugging** user EXEC command.

Related Commands

Command	Description
show debugging	Shows the current debugging status.
logging debug	Configures logging of debug messages.

debug cfm

```
debug cfm { event | packet-decode | packet-hex | states } { ais | cc | lb | lt | dm } md  
text ma text { mep id value | mip { ethernet unit/port | port-channel portchannel } }
```

no debug cfm

Description

Enables the printing of debug messages for CFM protocol.

Inserting **no** as a prefix for this command will disable debugging for CFM protocol.

Syntax

Parameter	Description
events	Enable debugging of CFM events
packets	Enable debugging of CFM packets (decoded output)
packets-hex	Enable debugging of CFM packets (raw packet dump)
states	Enable debugging of CFM state machines
ais	Enable debug for Alarm Indication Signal protocol
cc	Enable debug for Continuity Check protocol
lb	Enable debug for Loopback protocol
lt	Enable debug for Linktrace protocol
dm	Enable debug for Delay Measurement protocols
md	Enable debug for a Maintenance Domain (MD)
<i>text</i>	MD Name
ma	Enable debug for a Maintenance Association (MA)
<i>text</i>	MA Name
mep	Enable debug for Maintenance End Point (MEP)
id	MEP identifier
<i>value</i>	MEP ID value
mip	Enable debug for Maintenance Intermediate Point (MIP)
ethernet	Enable debug for a MIP for an Ethernet port
port-channel	Enable debug for a MIP for a Port-channel
<i>unit/port</i>	Unit number/Ethernet interface number
<i>portchannel</i>	Port-channel interface number

Default

Disabled by default.

Commands Modes

User EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command enables the printing of CFM debug messages in the current session of the command-line interface. Messages are generated for each type of debug configured.

This is a per-session option, not shared nor stored across sessions.

Example

This example shows how to enable the printing of debug messages for CFM packets.

```
DmSwitch#debug cfm event cc md MD ma MA mep id 1
DmSwitch#Jan 1 00:16:33.046721 : Ethernet 1/1: CC event at MD 'MD ', MA 'MA ', MEP ID 1:
Transmitted a CCM in VLAN 1 to MAC Address 01:80:C2:00:00:35
Jan 1 00:16:33.747024 : Ethernet 1/1: CC event at MD 'MD ', MA 'MA ', MEP ID 1:
Received a CCM from remote MEP ID 2 with Sequence Number 1534, RDI 0, Port Status Up, ...
```

Related Commands

Command	Description
show debugging	Shows the current debugging status.

debug ip-tunnel

[no] debug ip-tunnel [db | fsm | hw]

Description

Enables the printing of debug messages for the IPv6/IPv4 tunneling.

Inserting **no** as a prefix for this command will disable debugging for Tunneling IPv6 in IPv4 protocol.

Syntax

Parameter	Description
db	Enables debug messages about database informations of the IPv6/IPv4 tunneling module.
fsm	Enables debug messages about the finite state machine of the IPv6/IPv4 tunneling module.
hw	Enables debug messages about the IPv6/IPv4 tunneling module at L3 hardware.

Default

Disabled by default.

Commands Modes

User EXEC

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command enables the printing of IP-Tunnel debug messages in the current session of the command-line interface. Messages are generated for each type of debug configured. If no debug option is provided, all categories are enabled.

Example

This example shows how to enable the printing of debug messages for all IP-Tunnel debug options.

```

DmSwitch#debug ip-tunnel
DmSwitch#Jan  1 00:01:51.611807 : IP_TUN_FSM | IP_Tunnel_FSM
Jan  1 00:01:51.611823 : IP_TUN_FSM | Process input 10
Jan  1 00:01:51.611840 : IP_TUN_DB | FSM state is 12 (IP tunnel 1)
Jan  1 00:01:51.611858 : IP_TUN_FSM | input 10, old state 12, new state 9, action 13
Jan  1 00:01:51.611875 : IP_TUN_DB | Update FSM parameters of the IP tunnel 1 with input
10 and FSM state 9
Jan  1 00:01:51.611893 : IP_TUN_FSM | M: Finish to configure tunnel parameters
(tunnel 1)
Jan  1 00:01:51.612084 : IP_TUN_DB | Get source IP address 11.11.11.11
(IP tunnel 1)
Jan  1 00:01:51.612112 : IP_TUN_DB | Get destination IP address 10.10.10.10
(IP tunnel 1)
Jan  1 00:01:51.612131 : IP_TUN_DB | Tunnel type is: 6over4 (IP tunnel 1)
Jan  1 00:01:51.612149 : IP_TUN_HW | Set vid=950, intf_id=2
Jan  1 00:01:51.613745 : IP_TUN_DB | Configure INTF for VLAN 950 (IP tunnel 1)

```

Related Commands

Command	Description
show debugging	Shows the current debugging status.

debug lldp

```
[no] debug lldp { packet-decode | packet-hex | state } { all | rx | tx } { ethernet  
[ unit-number/ ] port-number }
```

```
[no] debug lldp event { ethernet [ unit-number/ ] port-number }
```

Description

Enables the printing of debug messages for LLDP protocol.

Inserting **no** as a prefix for this command will disable debugging for LLDP protocol.

Syntax

Parameter	Description
events	Enable debugging of LLDP events
packets	Enable debugging of LLDP packets (decoded output)
packets-hex	Enable debugging of LLDP packets (raw packet dump)
states	Enable debugging of LLDP state machines
all	Debug for both RX and TX
rx	Debug on receipt of packets
tx	Debug on transmission of packets
<i>unit/port</i>	Unit number/Ethernet interface number

Default

Disabled by default.

Commands Modes

User EXEC

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command enables the printing of LLDP debug messages in the current session of the command-line inter-

face. Messages are generated for each type of debug configured.

This is a per-session option, not shared nor stored across sessions.

Example

This example shows how to enable the printing of debug messages for LLDP packets.

```
DmSwitch#debug lldp packet-decode tx ethernet 1
DmSwitch#Jan 1 00:24:04.371415 : Ethernet 1/1: LLDP PDU TX Packet:
< [ChassisID (4): 00:04:DF:16:A6:00] [PortID (5): Port0] [TTL: 20] [PortDesc: Ethernet 1]
[SysName: DM4000] [SysDesc: DATACOM, DM4001, ETH] [SysCap: Brid*, Rout, ] [MgmtAddr->
(0: (IPV4 (1)) addr 6.6.6.6, intfNumb (ifIndex (2)), 6001 , OID: 1.3.6.1.4.1.3709.1.2.64) ]
[PortVLANID: ] [PortProtVLANID-> ] [VLANName-> ] [ProtID-> ] [MAC/PHY: AutnegSts: Sup/Dis,
MAUType: 1000BTFD, AutnegCap: 10BTHD, 10BTFD, 100BTXHD, 100BTXFD, FDXPAUSE, FDXSPAUSE,
1000BASETFD, ] [PwrMDI: ] [LinkAgg: ] [MaxFramesize: ] [ MED-> (NetPol: ) (LocID: )
(ExtPwrMDI-> ) (Inv-> ) ] >
```

Related Commands

Command	Description
show debugging	Shows the current debugging status.

debug port-security

[no] debug port-security { event | mac-sticky | state }

Description

Enables the printing of debug messages for Port-Security.

Inserting **no** as a prefix for this command will disable debugging for Port-Security.

Syntax

Parameter	Description
events	Enable debugging of port-security events
mac-sticky	Enable debugging of port-security sticky learning
states	Enable debugging of port-security state machines

Default

Disabled by default.

Commands Modes

User EXEC

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command enables the printing of port-security debug messages in the current session of the command-line interface. Messages are generated for each type of debug configured.

This is a per-session option, not shared nor stored across sessions.

Example

This example shows how to enable the printing of debug messages for port-security.

```
DmSwitch#debug port-security state
DM4000#
```


Related Commands

Command	Description
<code>show debugging</code>	Shows the current debugging status.

debug oam

```
debug oam { event | packet-decode | packet-hex } ethernet { [ unit-number/ ] port-number }
```

```
no debug oam [ { event | packet-decode | packet-hex } ethernet { [ unit-number/ ] port-number } ]
```

Description

Enables the printing of debug messages for OAM protocol.

Inserting **no** as a prefix for this command will disable all debugs or a specific debug for OAM protocol.

Syntax

Parameter	Description
event ethernet [<i>unit-number</i>] <i>port-number</i>	Enables debug messages for OAM event per unit/port.
packet-decode ethernet [<i>unit-number</i>] <i>port-number</i>	Enables debug messages for OAM packet decoded per unit/port.
packet-hex ethernet [<i>unit-number</i>] <i>port-number</i>	Enables debug messages for OAM packet in hex format per unit/port.

Default

Disabled by default.

Commands Modes

User EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command enables the printing of OAM debug messages in the current session of the command-line interface. Messages are generated for each type of debug configured.

This is a per-session option, not shared nor stored across sessions.

Example

This example shows how to enable the printing of debug messages for OAM packets.

```
DmSwitch#debug oam event ethernet 2
DmSwitch#Dec 31 23:59:04.872930 : Ethernet 1/2: Port blocked by OAM
Dec 31 23:59:06.872948 : Ethernet 1/2: Port unblocked by OAM
```

Related Commands

Command	Description
show debugging	Shows the current debugging status.
show debugging oam	Shows the current OAM debugging status.

debug openflow

debug openflow

no debug openflow

Description

Enables the printing of debug messages for OpenFlow protocol.

Inserting **no** as a prefix for this command will disable the printing of debug messages for OpenFlow protocol.

Default

Disabled by default.

Commands Modes

User EXEC

Command History

Release	Modification
OF-1.0.5	This command was introduced.

Usage Guidelines

This command enables the printing of OpenFlow debug messages in the current session of the command-line interface. Messages are generated for packet-in/out and flow reception/remotion events.

To use this command you must be in the command-line interface root.

This is a per-session option, not shared nor stored across sessions.

Example

This example shows how to enable the printing of debug messages for OpenFlow packets.

```
DmSwitch#debug openflow
Jan  1 03:38:06.079098 : OpenFlow packet OUT message received: unit 1, port 9, packet len 78,
ethertype 86dd
Jan  1 03:38:06.672030 : Filter received: id 0, ingress, group prio 0, filter prio 32767, |
matches: ingress port(s) 13, | actions: drop, | msg: filter_installed, ret_val: 0
Jan  1 03:38:07.676309 : OpenFlow packet IN message received: unit 1, port 3, packet len 94,
ethertype 86dd
Jan  1 03:38:06.678828 : Filter removed: id 0
```

Related Commands

Command	Description
<code>show debugging</code>	Shows the current debugging status.

diff

```
diff { default-config } { default-config | flash-config index | running-config |  
startup-config | profile-config metro }
```

```
diff { flash-config index } { default-config | flash-config index | running-config  
| startup-config | profile-config metro }
```

```
diff { running-config } { default-config | flash-config index | running-config |  
startup-config | profile-config metro }
```

```
diff { startup-config } { default-config | flash-config index | running-config |  
startup-config | profile-config metro }
```

```
diff { profile-config metro } { default-config | flash-config index |  
running-config | startup-config | profile-config metro }
```

Description

Compares and shows the differences between two configurations saved in flash memory.

Syntax

Parameter	Description
default-config	Default configuration of DmSwitch.
flash-config <i>index</i>	Specifies a flash configuration memory position. (Range: 1-4)
profile-config metro	Specifies predefined DmSwitch profile configuration.
running-config	Currently configuration running in DmSwitch.
startup-config	Configuration in the flash memory that is set as startup.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The difference output shows three lines of unified context.

Example

This example illustrates how to compare a supposed running-config with default-config.

```
DmSwitch#diff running-config default-config
@@ -15,7 +15,7 @@
!
interface vlan 1
  name DefaultVlan
- ip address 10.10.10.10/24
+ ip address 192.168.0.25/24
  set-member untagged ethernet all
!
spanning-tree 1
DmSwitch#
```

Related Commands

Command	Description
copy	Copies configuration and firmware.
erase	Erases spare firmware or configuration position.
select	Selects the startup firmware and flash for the next reboot.
show flash	Shows flash information.
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.
show startup-config	Shows the startup flash configuration.

dot1x initialize ethernet

dot1x initialize ethernet { [*unit-number/*] *port-number* }

Description

Force initialization of 802.1x protocol on a chosen ethernet port.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>port-number</i>	Configuration for a specific unit and port.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Force initialization of all protocol state machines. Authenticated users will be disconnected and protocol will be restarted in the requested interface.

Example

This example shows how to initialize 802.1X protocol on ethernet port 2.

```
DmSwitch#dot1x initializa ethernet 2
DmSwitch#
```

You can verify the 802.1X status at port 2 by entering the **show dot1x interface ethernet 2** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>dot1x reauthenticate ethernet</code>	Reauthenticate the suplicant at a specific port.
<code>show dot1x</code>	Shows 802.1X information.

dot1x reauthenticate ethernet

dot1x reauthenticate ethernet { [*unit-number/*] *port-number* }

Description

Reauthenticate the suplicant at a chosen ethernet port.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>port-number</i>	Configuration on a specific unit and port.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Force reauthentication of supplicants; if the new authentication succeeds, user is not disconnected and no data is lost. If authentication fails, user is disconnected. When user is authenticated by captive-portal, he loses network connectivity and must manually provide his credentials to reestablish network connection.

Example

This example shows how to reauthenticate 802.1X protocol on ethernet port 2.

```
DmSwitch#dot1x reauthenticate ethernet 2
DmSwitch#
```

You can verify the 802.1X status at port 2 by entering the **show dot1x interface ethernet 2** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>dot1x initialiaze ethernet</code>	Initialize 802.1X at a chosen port.
<code>show dot1x</code>	Shows 802.1X information.

erase

erase { **firmware** *index* | **flash-config** *index* }

Description

Erases spare firmware or configuration position.

Syntax

Parameter	Description
firmware <i>index</i>	Erases the specified firmware. (Range: 1-2)
flash-config <i>index</i>	Erases the specified configuration. (Range: 1-4)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to erase a configuration and the spare firmware.

```
DmSwitch#erase flash-config 1
DmSwitch#erase firmware 1
DmSwitch#
```

You can verify that both memory positions were cleared by entering the **show flash** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
copy	Copies configuration and firmware.
diff	Compares and shows the differences between two configurations.
select	Selects the startup firmware and flash for the next reboot.
show firmware	Shows firmware information.
show flash	Shows flash information.
show flash-config	Shows the configuration stored in a specific flash position.
show startup-config	Shows the startup flash configuration.

exit

exit

Description

Exits the current command-line interface session. This command is also used to return to higher levels in the configuration tree.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

All modes.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

You can also return to higher levels in the configuration tree issuing **Ctrl+d**, or go directly to the command-line interface root with **Ctrl+z**.

Example

This example shows how to use the exit in the two cases where it can be applied: go to higher levels in the configuration tree and logout the command-line interface.

```
DmSwitch#configure
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#exit
DmSwitch(config)#exit
DmSwitch#exit

DmSwitch login:
```

Related Commands

No related command.

help

help

Description

Returns a description of the interactive help system.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

All modes.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to access help.

```
DmSwitch#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

DmSwitch#
```

Related Commands

No related command.

dump

dump

Description

Generate an dump file. This file is encrypted and can be send to a server using the copy command.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to generate an dump file.

```
DmSwitch#dump
The dump file dump_2014_Feb_14_15:03:12.txt was generated.
DmSwitch#
```

Related Commands

Command	Description
show dump	Shows the files stored in the dumps directory.
copy	Copies configuration and firmware.
clear dump	Clears dump files.

light unit

light unit [*unit-number*]

Description

Displays the unit number of the DmSwitch in a DM4100 stack.

Syntax

Parameter	Description
<i>unit-number</i>	(Optional) Displays on frontal lights which DmSwitch in a DM4100 stack is the specified unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Entering this command without parameters, all unit numbers in the stack will be lit.

Example

This example will display the frontal LED status indications of the number 1 switch in the stack.

```
DmSwitch#light unit 1
DmSwitch#
```

Related Commands

No related command.

memory unit *unit* external ^{[5][7]}

```
memory unit unit external { disable | mac-address-table | route-table-ipv4  
| route-table-ipv6 | mixed { mac-table entries route-table-ipv4 entries |  
route-table-ipv4 entries route-table-ipv6 entries }
```

Description

Configures the external memory partitioning.

Syntax

Parameter	Description
<i>unit</i>	Specifies the unit number.
disable	Do not use the external memory.
mac-address-table	Sets all external memory for MAC Table.
route-table-ipv4	Sets all external memory for IPV4 Route Table.
route-table-ipv6	Sets all external memory for IPV6 Route Table.
mixed mac-table <i>entries</i>	Sets MAC Table size.
mixed route-table-ipv4 <i>entries</i>	Sets IPV4 Route Table size.
mixed route-table-ipv6 <i>entries</i>	Sets IPV6 Route Table size.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
6.0	This command was introduced.
14.0	One more option to mixed item, allowing to configure external memory with both IPv4 and IPv6 entries.

Usage Guidelines

This command may require a reboot in switch to be effective.

When enable external memory for MAC table, internal memory is used for system entries, static entries and specific feature entries.

Example

This example illustrates how to disable the external memory. .

```
DmSwitch#memory unit 1 external disable
% Warning:
Reboot required to effect changes

DmSwitch#
```

Related Commands

Command	Description
show memory external	Shows memory configuration.

Output modifiers

[| { **after** | **begin** | **exclude** | **include** } *expression*]

Description

Filter text output of current command.

Syntax

Parameter	Description
after	(Optional) Prints lines after matching a pattern.
begin	(Optional) Prints lines which begin matches a pattern.
exclude	(Optional) Prints lines unmatching a pattern.
include	(Optional) Prints lines matching a pattern.
<i>expression</i>	Regular expression to be used as a pattern. The following metacharacters must be backslashed: , (,), {, } and +.

Default

No default is defined.

Command Modes

This option is available for commands with .

Command History

Release	Modification
6.0	Options begin , exclude and include were introduced.
13.0	Option after was introduced.

Usage Guidelines

Some commands may produce large text output, making troubleshooting and configuration/status management a difficult task.

These options are designed to filter text output of some (but not all) commands, mainly those with more intensive text output.

The text output of some commands may be filtered using a rule (include, exclude, begin, after) and an extended regular expression.

Example

This example illustrates how to filter the output of **show running-config**. The usual output of that command is very similar to this:

```
DmSwitch#show running-config
Building configuration...
!
hostname DmSwitch
!
username admin access-level 15
username admin password 7 d033e22ae348aeb5660fc2140aec35850c4da997
username guest access-level 0
username guest password 7 35675e68f4b5af7b995d9205ad0fc43842f16450
!
ip telnet server
ip http server
ip http secure-server
no ip ssh server
!
ip snmp-server community public ro
!
interface vlan 1
 name DefaultVlan
 ip address 192.168.0.25/24
 set-member untagged ethernet all
!
spanning-tree 1
spanning-tree 1 vlan all
!
```

The same command is now executed filtering the output to display only lines containing 'ip' or 'vlan':

```
DmSwitch#show running-config | include ip|vlan
Building configuration...
ip telnet server
ip http server
ip http secure-server
no ip ssh server
ip snmp-server community public ro
 ip address 192.168.0.25/24
DmSwitch#show running-config | exl ip
```

The same command is now executed filtering the output to display all lines after matching 'vlan 1':

```
DmSwitch#show running-config | after vlan 1
interface vlan 1
 name DefaultVlan
 ip address 192.168.0.25/24
 set-member untagged ethernet all
!
spanning-tree 1
spanning-tree 1 vlan all
!
```

ping

```
ping { destination-host [ cos cos-value ] [ count count-value ] [ df ] [ dscp dscp-value ] [ interval interval-value ] [ size size-value ] [ source source-address ] }
```

Description

Sends ICMP echo messages.

Syntax

Parameter	Description
<i>destination-host</i>	Specifies the IP address or hostname of the destination host.
cos <i>cos-value</i>	(Optional) Class of Service (CoS) value sent within ethernet frame header. (Range: 0-7).
count <i>count-value</i>	(Optional) Replies attempts. (Range: 1-1000000).
df	(Optional) Don't Fragment (DF) flag to prohibit fragmentation.
dscp <i>dscp-value</i>	(Optional) Differentiated Services Code Point (DSCP) value sent within IP header. (Range: 0-63).
interval <i>interval-value</i>	(Optional) Interval between sent packets (in seconds). (Range: 0.1-60.0).
size <i>size-value</i>	(Optional) ICMP datagram size (in bytes). (Range: 0-65468).
source <i>source-address</i>	(Optional) IPv4 source address.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.6	New optional parameter was introduced: source .
12.2	New optional parameters were introduced: cos , df , dscp .
3.1	This command was introduced.

Usage Guidelines

The **ping** command is used to test for connectivity to a specific host.

If a **ping** request fails, the switch continues to send **ping** messages until it is interrupted. Press **Ctrl+C** to interrupt a **ping** request.

You must configure DNS in order to use a hostname in the *destination-host* field.

Example

This example shows how to send ICMP echo messages to a remote IP device.

```
DmSwitch#ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=2.1 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=2.1 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=2.0 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=2.0 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.0/2.0/2.1 ms
DmSwitch#
```

Related Commands

Command	Description
ping vrf	Sends ICMP echo messages from a specific VRF to a remote IP device.

ping6

```
ping6 { destination-host [ cos cos-value ] [ count count-value ] [ df ] [ dscp dscp-value ] [ interval interval-value ] [ size size-value ] [ vlan vlan-id ] [ source source-address ] }
```

Description

Sends ICMPv6 echo messages.

Syntax

Parameter	Description
<i>destination-host</i>	Specifies the IPv6 address or hostname of the destination host.
cos <i>cos-value</i>	(Optional) Class of Service (CoS) value sent within ethernet frame header. (Range: 0-7).
count <i>count-value</i>	(Optional) Replies attempts. (Range: 1-1000000).
df	(Optional) Don't Fragment (DF) flag to prohibit fragmentation.
dscp <i>dscp-value</i>	(Optional) Differentiated Services Code Point (DSCP) value sent within IPv6 header. (Range: 0-63).
interval <i>interval-value</i>	(Optional) Interval between sent packets (in seconds). (Range: 0.1-60.0).
size <i>size-value</i>	(Optional) ICMPv6 datagram size (in bytes). (Range: 0-65468).
vlan <i>vlan-id</i>	(Optional) Output VLAN to send packets when <i>destination-host</i> is a Link-Local address. (Range: 1-4094).
source <i>source-address</i>	(Optional) IPv6 source address.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.6	New optional parameter was introduced: source .
12.2	New optional parameters were introduced: cos , df , dscp , interval , size .
12.0	This command was introduced.

Usage Guidelines

The **ping6** command is used to test for connectivity to a specific host.

If a **ping6** request fails, the switch continues to send **ping6** messages until it is interrupted. Press **Ctrl+C** to interrupt a **ping6** request.

You must configure DNS in order to use a hostname in the *destination-host* field.

Example

This example shows how to send ICMPv6 Echo messages to a remote IPv6 device.

```
DmSwitch#ping6 2001:0db8:85a3::7344
PING 2001:0db8:85a3::7344 (2001:0db8:85a3::7344): 56 data bytes
64 bytes from 2001:0db8:85a3::7344: icmp_seq=0 ttl=64 time=2.1 ms
64 bytes from 2001:0db8:85a3::7344: icmp_seq=1 ttl=64 time=2.1 ms
64 bytes from 2001:0db8:85a3::7344: icmp_seq=2 ttl=64 time=2.0 ms
64 bytes from 2001:0db8:85a3::7344: icmp_seq=3 ttl=64 time=2.0 ms

--- 2001:0db8:85a3::7344 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.0/2.0/2.1 ms
DmSwitch#
```

Related Commands

No related command.

ping mpls ^[1] ^[3] ^[6]

```
ping mpls { ldp ip-address/mask | rsvp tunnel-id } [ background ] [ count value ] [ destination ip-address ] [ dsm ] [ exp priority ] [ interval seconds ] [ reply-mode { udp-ipv4 | router-alert } ] [ size value ] [ padding value ] [ timeout seconds ] [ ttl value ] [ verbose ]
```

Description

Check MPLS data plane of each router along an label switched path (LSP) by sending MPLS "echo request" message within the specified LSP.

Syntax

Parameter	Description
ldp <i>ip-address/mask</i>	Specifies the LSP type as LDP for a FEC and Prefix Length
rsvp <i>tunnel-id</i>	Specifies the LSP type as RSVP tunnel with the specific tunnel ID.
background	(Optional) Runs command in background.
count <i>value</i>	(Optional) Specifies the number of times to resend MPLS echo request. Range: 1-10000. Default: 5
destination <i>ip-address</i>	(Optional) Specifies an 127/8 address as destination.
dsm	(Optional) Send a DownStream Mapping TLV.
exp <i>priority</i>	(Optional) Specifies the EXP bits value in the MPLS header of packets. Range: 0-7. Default: 0
interval <i>seconds</i>	(Optional) Specifies the interval (in seconds) to resend packets. Range: 1-600. Default: 1
reply-mode udp-ipv4	(Optional) Specifies IPv4 UDP as the reply mode for MPLS echo reply packet. Default: udp-ipv4.
reply-mode router-alert	(Optional) Specifies IPv4 UDP with router alert as the reply mode for MPLS echo reply packet. Default: udp-ipv4.
size <i>value</i>	(Optional) Specifies the packet size in bytes.
padding <i>value</i>	(Optional) Specifies value to fill the pad TLV. Default: 0xFF.
timeout <i>seconds</i>	(Optional) Specifies the timeout interval (in seconds). Default: 2 seconds.
ttl <i>value</i>	(Optional) Specifies the TTL value for the MPLS echo request. Default: 255.
verbose	(Optional) Enable the verbose output of commands.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ping mpls** command is used to check the operability of each router along an specific LSP by sending an MPLS "echo request" packet within the LSP, according to RFC 4379.

Example

This example shows how to test an LDP LSP to FEC 100.100.100.1/32, sending packets to destination address 127.0.0.100

```
DmSwitch#ping mpls ldp 100.100.100.1/32 destination 127.0.0.100
LDP FEC: 100.100.100.1/32
```

```
LSP Ping transaction ID 1: 5 messages with 100 bytes
Reply mode: Reply via UDP IPv4
Interval 1000 ms, Timeout 2000 ms, TTL 255, EXP 0x0
Seq. 1 from 100.100.100.1, return 3 (1), 16.5 ms
Seq. 2 from 100.100.100.1, return 3 (1), 14.7 ms
Seq. 3 from 100.100.100.1, return 3 (1), 14.8 ms
Seq. 4 from 100.100.100.1, return 3 (1), 15.1 ms
Seq. 5 from 100.100.100.1, return 3 (1), 14.7 ms
```

```
[min/avg/max] (ms): 14.710/15.189/16.523
Loss rate: 0.000 %
```

```
Session 1 terminated successfully
```

```
DmSwitch#
```

Example with DownStream Mapping

This example shows how to test an LDP LSP to FEC 100.100.100.3/32 with a DownStream Mapping TLV

```
DmSwitch#ping mpls ldp 100.100.100.3/32 dsm ttl 1
```

```
LSP Ping transaction ID 1:
Number of messages: 5
Message size: 100 bytes
Reply mode: Reply via UDP IPv4
Interval 1000 ms, Timeout 2000 ms, TTL 1, EXP 0x0
Seq. 1 from 100.100.100.1, return 3 (1), 16.5 ms
[DS Router: 100.100.100.2, DS Iface: 100.100.100.2, MTU: 1500, Depth Limit: 255]
{Label: 19 | Exp: 0 | BoS: 0 | Protocol: 4}
```

```

    {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}
Seq. 2 from 100.100.100.1, return 3 (1), 14.7 ms
[DS Router: 100.100.100.2, DS Iface: 100.100.100.2, MTU: 1500, Depth Limit: 255]
    {Label: 19 | Exp: 0 | BoS: 0 | Protocol: 4}
    {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}
Seq. 3 from 100.100.100.1, return 3 (1), 14.8 ms
[DS Router: 100.100.100.2, DS Iface: 100.100.100.2, MTU: 1500, Depth Limit: 255]
    {Label: 19 | Exp: 0 | BoS: 0 | Protocol: 4}
    {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}
Seq. 4 from 100.100.100.1, return 3 (1), 15.1 ms
[DS Router: 100.100.100.2, DS Iface: 100.100.100.2, MTU: 1500, Depth Limit: 255]
    {Label: 19 | Exp: 0 | BoS: 0 | Protocol: 4}
    {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}
Seq. 5 from 100.100.100.1, return 3 (1), 14.7 ms
[DS Router: 100.100.100.2, DS Iface: 100.100.100.2, MTU: 1500, Depth Limit: 255]
    {Label: 19 | Exp: 0 | BoS: 0 | Protocol: 4}
    {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}

[min/avg/max] (ms): 14.710/15.189/16.523
Loss rate: 0.000 %

Session 1 terminated successfully

DmSwitch#
```

Example with DownStream Mapping and verbose output

This example shows how to test an LDP LSP to FEC 100.100.100.3/32 with a DownStream Mapping TLV and verbose output

```

DmSwitch#ping mpls ldp 100.100.100.1/32 dsm ttl 1 verbose

LSP Ping transaction ID 1:
Number of messages: 5
Message size: 100 bytes
Reply mode: Reply via UDP IPv4
Interval 1000 ms, Timeout 2000 ms, TTL 255, EXP 0x0
Seq. 1 from 100.100.100.1, return 3 (1), 16.5 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
    DS Router: 100.100.100.2, DS Iface: 100.100.100.2
    MTU: 1500, Depth Limit: 255
    There are 2 labels on response:
        {Label: 19 | Exp: 0 | BoS: 0 | Protocol: RSVP-TE}
        {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}
Seq. 2 from 100.100.100.1, return 3 (1), 14.7 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
    DS Router: 100.100.100.2, DS Iface: 100.100.100.2
    MTU: 1500, Depth Limit: 255
    There are 2 labels on response:
        {Label: 19 | Exp: 0 | BoS: 0 | Protocol: RSVP-TE}
        {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}
Seq. 3 from 100.100.100.1, return 3 (1), 14.8 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
    DS Router: 100.100.100.2, DS Iface: 100.100.100.2
    MTU: 1500, Depth Limit: 255
    There are 2 labels on response:
        {Label: 19 | Exp: 0 | BoS: 0 | Protocol: RSVP-TE}
```

```

        {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}
Seq. 4 from 100.100.100.1, return 3 (1), 15.1 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
    DS Router: 100.100.100.2, DS Iface: 100.100.100.2
    MTU: 1500, Depth Limit: 255
    There are 2 labels on response:
        {Label: 19 | Exp: 0 | BoS: 0 | Protocol: RSVP-TE}
        {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}
Seq. 5 from 100.100.100.1, return 3 (1), 14.7 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
    DS Router: 100.100.100.2, DS Iface: 100.100.100.2
    MTU: 1500, Depth Limit: 255
    There are 2 labels on response:
        {Label: 19 | Exp: 0 | BoS: 0 | Protocol: RSVP-TE}
        {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}

[min/avg/max] (ms): 14.710/15.189/16.523
Loss rate: 0.000 %

Session 1 terminated successfully

DmSwitch#

```

Related Commands

Command	Description
show mpls ldp database	List LSP database
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information
trace mpls	Discover the path packets take along an MPLS LSP.

ping vrf

```
ping vrf { [ VRF Name ] [ destination-host ] [ cos cos-value ] [ count count-value ] [ df ] [ dscp dscp-value ] [ interval interval-value ] [ size size-value ] [ source source-address ] }
```

Description

Sends ICMP echo messages from a VRF.

Syntax

Parameter	Description
<i>VRF Name</i>	Specifies the VRF name.
<i>destination-host</i>	Specifies the IP address or hostname of the destination.
cos <i>cos-value</i>	(Optional) Class of Service (CoS) value sent within ethernet frame header. (Range: 0-7).
count <i>count-value</i>	(Optional) Replies attempts. (Range: 1-1000000).
df	(Optional) Don't Fragment (DF) flag to prohibit fragmentation.
dscp <i>dscp-value</i>	(Optional) Differentiated Services Code Point (DSCP) value sent within IP header. (Range: 0-63).
interval <i>interval-value</i>	(Optional) Interval between sent packets (in seconds). (Range: 0.1-60.0).
size <i>size-value</i>	(Optional) ICMP datagram size (in bytes). (Range: 0-65468).
source <i>source-address</i>	(Optional) IPv4 source address.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.8	This command was introduced.

Usage Guidelines

The **ping vrf** command is used to test for connectivity to a specific host.

If a **ping vrf** request fails, the switch continues to send **ping vrf** messages until it is interrupted. Press **Ctrl+C** to interrupt a **ping vrf** request.

You must configure DNS in order to use a hostname in the *destination* field.

Example

This example shows how to send ICMP echo messages from VRF *blue* to a remote IP device.

```
DmSwitch#ping vrf blue 172.16.78.17
PING 172.16.78.17 (172.16.78.17) from 172.16.78.2 : 56(84) bytes of data.
64 bytes from 172.16.78.17: icmp_req=1 ttl=64 time=0.148 ms
64 bytes from 172.16.78.17: icmp_req=2 ttl=64 time=0.084 ms
64 bytes from 172.16.78.17: icmp_req=3 ttl=64 time=0.081 ms
64 bytes from 172.16.78.17: icmp_req=4 ttl=64 time=0.083 ms
64 bytes from 172.16.78.17: icmp_req=5 ttl=64 time=0.084 ms

--- 172.16.78.17 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.081/0.096/0.148/0.026 ms
DmSwitch#
```

Related Commands

Command	Description
ping	Sends ICMP echo messages to a remote IP device.
ping mpls	Check MPLS data plane and LSP connectivity.

process

```
process process-name { restart | start | stop [force] }
```

```
process cli { pid | all } stop [force ]
```

```
process main { restart | start }
```

Description

Through this command it's possible to fire actions to managed processes.

Syntax

Parameter	Description
<i>process-name</i>	Name of the managed process to be executed an action.
<i>pid</i>	PID of a CLI process.
restart	Restart selected managed process.
start	Start selected managed process.
stop <i>force</i>	Stop selected managed process.
all	All CLI processes.

Default

Disabled.

Command Modes

User EXEC.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Through this command it's possible to fire actions to managed processes. The current managed processes are: cli, httpd, httpsd, main, snmpd, snmpd, traps, lldpd, multicasted, dcltd, rpediag, ipcrecorder, eventd, psmd, auditd, dot1xd, httpd_captive, httpsd_captive, watchdog and cpumond.

Example

This example shows how stop the "traps" process.

```
DmSwitch#process traps stop force
% Warning:
Stopping a process may cause traffic disruption or loss of management channels
Are you sure? <y/N> y
DmSwitch#
```

Related Commands

Command	Description
show processes	Shows managed processes information.

reboot

reboot [**unit** *number* | [**hard**] | [**ports-up**] | **ports-up** | **hard** | **at** *hour* | **in** { **minutes** *minutes* | **hours** *hours* [**minutes** *minutes*] } | **cancel** | **standby-mpu** [**hard**]]

Description

Reboots the switch.

Syntax

Parameter	Description
unit <i>number</i>	(Optional) Reboot unit specified by number. (Range: 1-8)[1]
ports-up	(Optional) Reboot with protocols down and ports up.
at <i>minutes</i>	(Optional) Reboot at specified time. (hh:mm:ss)
in <i>minutes</i>	(Optional) Reboot after a time interval in minutes. (Range: 1-59)
cancel	(Optional) Cancel a scheduled reboot.
standby-mpu	(Optional) Reboot standby MPU [2]
hard	(Optional) Perform hard reset [3]

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.0	Hard reset option was introduced for rebooting standby-MPU or a single unit.
14.4	Hard reset option was introduced for rebooting the entire chassis.

Usage Guidelines

Using **reboot** without any parameters will make the switch reboot with protocols and ports down.

Example

This example shows how to reboot the switch.

```
DmSwitch#reboot
System will be restarted. Continue? <y/N> y
```

Related Commands

No related command.

Notes

[1] - Range 1-8 available only to DM4000 Switches.

[1] - Reboot last interface card cause reboot all on DM4000 Switches with redundancy.

[2] - Standby-MPU only available in DM4000 Switches with redundancy.

[3] - Hard reset may cause data loss, use with caution. It's only available in DM4000 Switches with redundancy.

redundancy ^[5]

redundancy nsf-id *id*

redundancy switch-to-standby

redundancy legacy-port

no redundancy legacy-port

Description

Redundancy configuration and operation.

Syntax

Parameter	Description
nsf-id <i>id</i>	Sets the Non-stop Forwarding (NSF) ID in the active MPU. (Range: 0x01-0xFF)
switch-to-standby	Perform MPU switchover manually.
legacy-port	Enable legacy-port mode.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.
13.4	The option legacy-port was introduced.

Usage Guidelines

For Non-stop Forwarding feature to work properly during a switchover, both MPU cards must have the same MAC address. Setting **redundancy nsf-id** will cause a virtual MAC address to be assigned to the active MPU card. The same ID should be used for both MPU cards.

The Legacy Port feature is intended to enable update of MPUs running firmware older than 12.2. Using **no** as a prefix for this command will disable legacy-port mode.

Examples

This example shows how to set the nsf-id on both MPU cards.

```
DmSwitch#redundancy nsf-if 0x01
DmSwitch#redundancy switch-to-standby
Are you sure? <y/N> y
```

Login again to the new active MPU.

```
DmSwitch#redundancy nsf-if 0x01
DmSwitch#reboot
System will be restarted. Continue? <y/N> y
```

This example shows how to update a MPU using legacy-mode:

```
DmSwitch#redundancy legacy-port
% Warning: Legacy Mode will detect only MPU with FW lower than 12.2.
Enter redundancy legacy-port Mode <y/N> y
DmSwitch#copy firmware 1 standby-mpu
Saving firmware in standby MPU...
Writing firmware...
Progress: 100% written...
Done.
Use the "reboot standby-mpu" command to run the new firmware.
DmSwitch#reboot standby-mpu
Standby MPU will be restarted. Continue? <y/N> y
DmSwitch#
```

Related Commands

Command	Description
show redundancy-status	Shows redundancy information

remote-devices force ethernet

remote-devices force ethernet [*unit-number/*] *port-number*

Description

Force configuration of remote device.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>port-number</i>	Entry Unit number/Ethernet interface number.(Range: 1-1/1-28)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to force configuration of remote device.

```
DmSwitch#remote-devices force ethernet 10
DmSwitch#
```

Related Commands

Command	Description
show remote-devices	Remote device management configuration and status.

select

```
select { firmware firmware-index { unit unit-number | standby-mpu } | startup-config
{ index | default } }
```

Description

Selects the startup firmware and flash for the next reboot.

Syntax

Parameter	Description
firmware <i>firmware-index</i>	Indicates the firmware to be marked as startup for the next reboot of DmSwitch. (Range: 1-2)
unit <i>unit-number</i>	(Optional) Indicates the unit where the firmware is to be marked as startup.
standby-mpu	(Optional) Indicates standby mpu where the firmware is to be marked as startup.
startup-config	Configuration in the flash memory that will be set as startup.
<i>index</i>	Specifies the position of configuration in flash memory that will be marked as startup. (Range: 1-4)
default	Specifies that the default configuration will be the startup configuration.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to mark configuration 1 in flash memory as startup.

```
DmSwitch#select startup-config 1
DmSwitch#
```

You can verify that the specified configuration was set as startup by entering the **show flash** privileged EXEC command.

Related Commands

Command	Description
copy	Copies configuration and firmware.
diff	Compares and shows the differences between two configurations.
erase	Erases spare firmware or configuration position.
show firmware	Shows firmware information.
show flash	Shows flash information.
show flash-config	Shows the configuration stored in a specific flash position.
show startup-config	Shows the startup flash configuration.

show arp aging-time

show arp aging-time

Description

Shows arp aging-time configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the ARP aging time configuration.

```
DmSwitch#show arp aging-time
  ARP Aging time: 300 seconds
DmSwitch#
```

Related Commands

Command	Description
arp aging-time	Defines the aging time of all entries in the Data plane's ARP table.

show authentication

show authentication

Description

Shows information about login authentication method and its precedence.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show information about login authentication method and its precedence.

```
DmSwitch#show authentication
Login authentication method by precedence:
    (1) Local database
    (2) RADIUS server
    (3) TACACS server

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
authentication login	Defines the login authentication method and its precedence.
tacacs-server host	Configures the TACACS server IP address.

Command	Description
tacacs-server key	Configures the TACACS server key string.
radius-server acct-port	Configures the default RADIUS server accounting port.
radius-server auth-port	Configures the default RADIUS server authentication port.
radius-server host	Configures a specific RADIUS server.
radius-server key	Configures the default RADIUS server key string.
radius-server retries	Configures the RADIUS server retries.
radius-server timeout	Configures the RADIUS server timeout.
show radius-server	Shows RADIUS server information.
show running-config	Shows the current operating configuration.
show tacacs-server	Shows global TACACS information and all configured servers.

show backup-link

show backup-link

Description

Shows backup-link status information of all interfaces.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.6	This command was introduced.

Usage Guidelines

This command shows the backup-link status information.

Example

This example illustrates how to show backup-link status information.

```
DmSwitch#show backup-link
```

Main Interface	Backup Interface	Preemption delay (sec)	Action	Link Main	Status Backup	State	Time to Preempt
Eth 1/1	Eth 1/2	35	BLOCK	UP	BLOCK	MAIN	-
Pch 1	Eth 1/12	-	SHUTDOWN	UP	DOWN	MAIN	-

```
DmSwitch#
```

Related Commands

Command	Description
switchport backup-link	Configure a backup-link.

Command	Description
<code>show interface switchport</code>	Shows switchport information.

show batch

show batch

Description

Shows the existing batch files and their contents.
Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

With this command show, you can also see the batch file execution schedule.

Example

This example illustrates how to show the batch file.

```
DmSwitch#show batch
Batch 1: enable
Date       : min 0 hour 7 day-of-month all month all day-of-week 6
Commands List:
    configure
    interface vlan 2
    ip address 10.11.13.13/24
    exit

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include

Command	Description
batch index date	Schedules the execution of batch file.
batch index disable	Disables the batch file execution.
batch index enable	Enables the batch file execution in accordance with its schedules.
batch index remark	Specifies a remark for a batch file.
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch new	Creates a new batch file.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.

show bridge-ext

show bridge-ext

Description

Shows bridge extension information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the bridge extension information.

```
DmSwitch#show bridge-ext
Global GVRP status:          Disabled
DmSwitch#
```

Related Commands

No related command.

show bpdu-protect

show bpdu-protect

Description

Shows the BPDU protect port status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
9.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the bpdu-protect information.

```
DmSwitch#show bpdu-protect
Global BPDU protect: Disabled
  Block      Time to
Interface  Enabled  Limit   time   Mode        State    Unblock
-----
Eth 1/ 1   No       30      10     Block all   Ok       0       s
Eth 1/ 2   No       30      10     Block all   Ok       0       s
Eth 1/ 3   No       30      10     Block all   Ok       0       s
Eth 1/ 4   No       30      10     Block all   Ok       0       s
Eth 1/ 5   No       30      10     Block all   Ok       0       s
Eth 1/ 6   No       30      10     Block all   Ok       0       s
Eth 1/ 7   No       30      10     Block all   Ok       0       s
Eth 1/ 8   No       30      10     Block all   Ok       0       s
Eth 1/ 9   No       30      10     Block all   Ok       0       s
Eth 1/10   No       30      10     Block all   Ok       0       s
Eth 1/11   No       30      10     Block all   Ok       0       s
Eth 1/12   No       30      10     Block all   Ok       0       s

DmSwitch#
```

Related Commands

No related command.

Command	Description
<code>switchport bpdu_protect</code>	Protect BPDU configuration for an interface.

show cable-diagnostics

show cable-diagnostics [**ethernet** [*unit-number/*] *port-number*]

Description

Performs cable diagnostics.

Output modifiers are available for this command.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Shows the diagnostics filtered by a specific unit and port.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
14.10.8	Pair indexing was made compliant with TIA/EIA 568B.
15.0	Error margin in length measurement is always shown; This document was updated.

Usage Guidelines

When issuing this command without parameters the cable diagnostics of all ports will be shown. Notice: diagnostics are not reliable for a port that has the PoE feature enabled.

Example

This example illustrates how to show cable diagnostics for unit 1 port 12. and ports.

```
DmSwitch#show cable-diagnostics ethernet 12
Port  Link  Speed  Status      Pair  Pair Status  Pair Length (error)
----  -
1/22  Up      1000   Ok          1     Ok           4 m (+/- 10 m)
                2     Ok           4 m (+/- 10 m)
```

```

DmSwitch#
3      Ok      6 m (+/- 10 m)
4      Ok      4 m (+/- 10 m)

```

Pair Status Description

Status	Definition
OK	The pair is good and well terminated.
Open	The pair is open and is not terminated.
Short	The pair pins are shorted together.
Crosstalk	Excessive crosstalk between pairs or different pairs shorted together.
Open/Short	Couldn't determine whether the pair state is Open or Short.
Error	Error probing the pair for diagnostics.
N/A	Diagnostics not supported for port/pair.

Pair Indexing Reference

Pair	RJ45 (TIA/EIA 568A)	RJ45 (TIA/EIA 568B)
1	Pins 4 and 5	Pins 4 and 5
2	Pins 3 and 6	Pins 1 and 2
3	Pins 1 and 2	Pins 3 and 6
4	Pins 7 and 8	Pins 7 and 8

Related Commands

Command	Description
<code>output modifiers</code>	Options to filter text output: after, begin, exclude and include

show capture file

show capture file *filename* [**detail**] [**filter** *string_filter*]

Description

Show packets captured contained in a file stored in the DmSwitch.

Syntax

Parameter	Description
<i>filename</i>	Name of the file that contains the captured packets.
detail	Show packet details.
filter <i>string_filter</i>	Filter to display captured packets(in pcap-filter format).

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

This command show packets captured contained in a file stored in the DmSwitch.

Examples

This example illustrates how to show the packets contained in a file(s).

```
DmSwitch#show capture file logger.pcap

 1  0.000000 192.168.1.168 -> 199.16.156.102 IP TCP (0x06)
 2  0.000234 192.168.1.168 -> 199.16.156.102 IP TCP (0x06)
 3  0.823756 192.168.1.168 -> 194.244.45.118 IP TCP (0x06)
 4  0.824161 192.168.1.168 -> 194.244.45.118 IP TCP (0x06)
 5  2.867540 192.168.1.168 -> 173.194.39.48 IP TCP (0x06)
 6  2.867772 192.168.1.168 -> 173.194.39.48 IP TCP (0x06)
 7  2.869802 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)
 8  2.869826 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)
```

```

 9   2.869844 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)
10   2.870093 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)

```

```
DmSwitch#
```

This example illustrates how to show the packets details contained in a file(s).

```
DmSwitch#show capture file logger.pcap detail
```

```

Frame 1 (66 bytes on wire, 66 bytes captured)
  Arrival Time: Feb 26, 2014 22:27:21.264611000
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 66 bytes
  Capture Length: 66 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:data]
Ethernet II, Src: d0:e1:40:4b:1c:d2 (d0:e1:40:4b:1c:d2), Dst: 3c:e0:72:2f:a8:3b (3c:e0:72:2f:a8:3b)
  Destination: 3c:e0:72:2f:a8:3b (3c:e0:72:2f:a8:3b)
    ....0 .... = IG bit: Individual address (unicast)
    ....0 .... = LG bit: Globally unique address (factory default)
  Source: d0:e1:40:4b:1c:d2 (d0:e1:40:4b:1c:d2)
    ....0 .... = IG bit: Individual address (unicast)
    ....0 .... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.168 (192.168.1.168), Dst: 199.16.156.102 (199.16.156.102)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    ....0. = ECN-Capable Transport (ECT): 0
    ....0. = ECN-CE: 0
  Total Length: 52
  Identification: 0x1468 (5224)
  Flags: 0x04 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0x0095 [correct]
    [Good: True]
    [Bad : False]
  Source: 192.168.1.168 (192.168.1.168)
  Destination: 199.16.156.102 (199.16.156.102)
Data (32 bytes)
...
DmSwitch#

```

Related Commands

Command	Description
<code>clear capture</code>	Clear packet capture files.
<code>show capture files</code>	Shows a list of files containing packet captures.
<code>show capture realtime</code>	Show packets captured in realtime.

show capture files

show capture files

Description

Shows the packet capture files stored in the DmSwitch.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command shows the packet capture files stored in the DmSwitch;.

Example

This example illustrates how to show the packet capture file(s).

```
DmSwitch#show capture files
Packet capture file          Size      Date
-----
capture_2013_Dec_01_00:02:26_00.pcap      2992 Thu Dec  1 00:02:29 2013
capture_2013_Dec_01_00:02:30_00.pcap      2012 Thu Dec  1 00:02:32 2013

Total:                                5004

DmSwitch#
```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture realtime	Show packets captured in realtime.

show capture realtime

show capture realtime *sniffer_id* [**detail**] [**filter** *string_filter*]

Description

Show packets captured in realtime in the DmSwitch.

Syntax

Parameter	Description
<i>sniffer_id</i>	Instance sniffer with an active capture.
detail	Show packet details.
filter <i>string_filter</i>	Filter to display captured packets(in pcap-filter format).

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

This command shows packets captured in realtime in the DmSwitch.

Examples

This example illustrates how to show the packets in realtime.

```
DmSwitch#show capture realtime 1

 1  0.000000 192.168.1.168 -> 199.16.156.102 IP TCP (0x06)
 2  0.000234 192.168.1.168 -> 199.16.156.102 IP TCP (0x06)
 3  0.823756 192.168.1.168 -> 194.244.45.118 IP TCP (0x06)
 4  0.824161 192.168.1.168 -> 194.244.45.118 IP TCP (0x06)
 5  2.867540 192.168.1.168 -> 173.194.39.48 IP TCP (0x06)
 6  2.867772 192.168.1.168 -> 173.194.39.48 IP TCP (0x06)
 7  2.869802 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)
 8  2.869826 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)
 9  2.869844 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)
```

```

10    2.870093 192.168.1.168 -> 89.30.102.146 IP TCP (0x06)

DmSwitch#

```

This example illustrates how to show the packets details in realtime.

```

DmSwitch#show capture file 1 detail

Frame 1 (66 bytes on wire, 66 bytes captured)
  Arrival Time: Feb 26, 2014 22:27:21.264611000
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 66 bytes
  Capture Length: 66 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:data]
Ethernet II, Src: d0:e1:40:4b:1c:d2 (d0:e1:40:4b:1c:d2), Dst: 3c:e0:72:2f:a8:3b (3c:e0:72:2f:a8:3b)
  Destination: 3c:e0:72:2f:a8:3b (3c:e0:72:2f:a8:3b)
Address: 3c:e0:72:2f:a8:3b (3c:e0:72:2f:a8:3b)
  ....0. .... = IG bit: Individual address (unicast)
  ....0. .... = LG bit: Globally unique address (factory default)
  Source: d0:e1:40:4b:1c:d2 (d0:e1:40:4b:1c:d2)
Address: d0:e1:40:4b:1c:d2 (d0:e1:40:4b:1c:d2)
  ....0. .... = IG bit: Individual address (unicast)
  ....0. .... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.168 (192.168.1.168), Dst: 199.16.156.102 (199.16.156.102)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
  ....0. = ECN-Capable Transport (ECT): 0
  ....0. = ECN-CE: 0
  Total Length: 52
  Identification: 0x1468 (5224)
  Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0x0095 [correct]
[Good: True]
[Bad : False]
  Source: 192.168.1.168 (192.168.1.168)
  Destination: 199.16.156.102 (199.16.156.102)
Data (32 bytes)
...

DmSwitch#

```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture files	Shows a list of files containing packet captures.

show cesop

show cesop unit *unit-number*

Description

Shows information about global CESoP configurations.

Syntax

Parameter	Description
<i>unit-number</i>	Unit number.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display information about CESoP configuration of unit 1.

```
DM4000#show cesop unit 1
CESoP unit 1 global configuration:
  Idle Byte:                0xFF
DM4000#
```

Related Commands

Command	Description
---------	-------------

Command	Description
<code>cesop idle-byte</code>	the Section called <i>cesop idle-byte</i> in Chapter 3

show cfm

show cfm

Description

Connectivity Fault Management (CFM) information.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows Connectivity Fault Management (CFM) information.

```
DmSwitch#show cfm
CFM State: enabled
DmSwitch#
```

Related Commands

Command	Description
show cfm delay-statistics	Delay Measurement (DM) information.
show cfm error	Error information about CFM configuration.
show cfm linktrace	Linktrace Messages (LTM) information .
show cfm md	Maintenance Domain (MD) information.

show cfm mep

```
show cfm mep [ direction {down|up} ] [ level {level} ] [ vlan {vlan id} ] [ interface
{ethernet [ unit-number/ ] port-number | port-channel channel-group-number } ] [ fail ] [
summary ]
```

Description

Maintenance End Point (MEP) information.

Syntax

Parameter	Description
direction { <i>up</i> <i>down</i> }	Filters meps by direction
fail	Filters meps on fail state
interface	Filters meps by interface
level <i>level</i>	Filters meps by level
vlan <i>vlan</i>	Filters meps by vlan
summary	Formats output as a summary of maps on a simple table

Command Modes

Global configuration.

Command History

Release	Modification
14.4	Summary command was modify.

Usage Guidelines

Not available.

Example

This example shows the usage of the command

```
DmSwitch#show cfm mep direction up level 5 summary
```

Local MEPID	MD/MA Name	Level	VID	Port	Defect List	Fault State
1	md, ma	5	5	Eth 1/1	----- --	Reset

Defect list flags:

- (A) AIS defect
- (R) RDI sent by some remote MEP
- (E) Erroneous CCM received
- (X) Cross connection condition detected
- (L) Loss of CCM from some remote MEP
- (N) Some remote MEP not found
- (B) Local interface blocked
- (D) Local interface down

Remote MEPID	MD/MA Name	Sender ID	MEP State	Time since last CFM conn. state change
2	md, ma	Not present	OK	1 h, 35 m, 15 s
3	md, ma	Not present	OK	1 h, 35 m, 6 s

MEP State:

- (OK) CFM connection ok and remote ok
- (Block) CFM connection ok and remote MEP blocked
- (Down) CFM connection ok and remote MEP down
- (ActShut) CFM connection ok and remote MEP down due action shutdown
- (Idle) CFM connection idle (local MEP blocked)
- (Fail) CFM connection fail
- (Start) CFM connection starting
- (--) Remote MEP not found yet

DmSwitch#

Related Commands

Command	Description
show cfm delay-statistics	Delay Measurement (DM) information.
show cfm error	Error information about CFM configuration.
show cfm linktrace	Linktrace Messages (LTM) information .

show cfm delay-statistics

```
show cfm delay-statistics { md md-name ma ma-name remote-mep id mep-id }
```

Description

Delay Measurement (DM) information.

Syntax

Parameter	Description
md <i>md-name</i>	Specifies Maintenance Domain (MD) name.
ma <i>ma-name</i>	Specifies Maintenance Association (MA) name.
remote-mep id <i>mep-id</i>	Insert a destination MEP ID. (Range: 1-8191)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows Delay Measurement (DM) information.

```
DmSwitch#show cfm delay-statistics md 11 ma 11 remote-mep id 2
MEP Identifier: 1, MAC address: 00:04:DF:17:FD:C8
Remote MEP identifier: 2, MAC address: 00:04:DF:64:BE:2B
DM Way: Two-way delay

Delay measurement statistics (microsecond):
      Frame      Delay
        1        2103

Avg delay (us):                2103
Avg delay variation (us):       0
DmSwitch#
```

Related Commands

Command	Description
<code>show cfm error</code>	Error information about CFM configuration.
<code>show cfm linktrace</code>	Linktrace Messages (LTM) information .
<code>show cfm md</code>	Maintenance Domain (MD) information.

show cfm error

```
show cfm error { vlan vlan-id ethernet [ unit-number/ ] port-number }
```

Description

Error information about CFM configuration.

Syntax

Parameter	Description
vlan <i>vlan-id</i>	Specifies VLAN id. (Range: 1-4096)
ethernet [<i>unit-number/</i>] <i>port-number</i>	Specifies the Unit number/ Ethernet interface number.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows error information about CFM configuration.

```
DmSwitch#show cfm error vlan 118 ethernet 4/48
No CFM Leak was found
No Conflicting VIDs were found
No Excessive Levels were found
No Overlapped Levels were found

DmSwitch#
```

Related Commands

Command	Description
show cfm delay-statistics	Delay Measurement (DM) information.

Command	Description
<code>show cfm linktrace</code>	Linktrace Messages (LTM) information .
<code>show cfm md</code>	Maintenance Domain (MD) information.

show cfm linktrace

```
show cfm linktrace { md md-name ma ma-name mep id mep-id }
```

Description

Linktrace Messages (LTM) information.

Syntax

Parameter	Description
md <i>md-name</i>	Specifies Maintenance Domain (MD) name.
ma <i>ma-name</i>	Specifies Maintenance Association (MA) name.
mep id <i>mep-id</i>	Insert a MEP ID value. (Range: 1-8191)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows Linktrace (LTM) information.

```
DmSwitch#show cfm linktrace md MD_1 ma MA_1 mep id 11
```

```
Linktrace messages sent:
```

```
Sent to 00:04:DF:17:31:3A, Transaction ID 0
```

Seq.	TTL	From	Relay	Egress Data	Ingress Data	Forwarding	
		OUI/ID	Action			Last	Next
1	63	00:04:DF	RlyHit	00:00:00 None	17:31:3A Ok	19:54:14	17:31:2E
MEP at 00:04:DF:17:31:3A							

```
DmSwitch#
```

Related Commands

Command	Description
<code>show cfm delay-statistics</code>	Delay Measurement (DM) information.
<code>show cfm error</code>	Error information about CFM configuration.
<code>show cfm md</code>	Maintenance Domain (MD) information.

show cfm md

```
show cfm md { md md-name ma ma-name { mep id mep-id | mip } }
```

Description

Maintenance Domain (MD) information.

Syntax

Parameter	Description
md <i>md-name</i>	Specifies Maintenance Domain (MD) name.
ma <i>ma-name</i>	Specifies Maintenance Association (MA) name.
mep id <i>mep-id</i>	Insert a MEP ID value. (Range: 1-8191)
mip	Shows Maintenance Intermediate Point (MIP) information

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows Maintenance Domain (MD) information.

```
DmSwitch#show cfm md MD_1

Maintenance Domain (MD):
  Level:                    5
  Format:                   Character String
  Length:                   2
  Name:                     md
  MHF Creation:              defMHFNone
  Sender ID TLV:             sendIdNone
  Fault Alarm Address:       Not transmitted

DmSwitch#
```

Related Commands

Command	Description
<code>show cfm delay-statistics</code>	Delay Measurement (DM) information.
<code>show cfm error</code>	Error information about CFM configuration.
<code>show cfm linktrace</code>	Linktrace Messages (LTM) information .

show cfm probe delay-measurement

`show cfm probe delay-measurement probe id`

Description

CFM Probe Delay Measurement (DM) information.

Syntax

Parameter	Description
<i>probe id</i>	Specifies Probe identifier.

Command Modes

Global configuration.

Command History

Release	Modification
11.2.10	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows CFM Probe Delay Measurement (DM) information.

```
DmSwitch#show cfm probe delay-measurement 3
Delay-measurement (DM) Probe:
  Interval (s):          0
  DM parameters: not configured
  Last statistics:
    Average delay:       0
    Average delay variation: 0
    Packet loss:         0%
DmSwitch#
```

Related Commands

Command	Description
<code>show cfm</code>	Connectivity Fault Management (CFM) information.

Command	Description
<code>show cfm delay-statistics</code>	Delay Measurement (DM) information.
<code>show cfm error</code>	Error information about CFM configuration.
<code>show cfm linktrace</code>	Linktrace Messages (LTM) information .
<code>show running-config</code>	Shows the current operating configuration.

show clock

show clock

Description

Shows the system clock and time zone.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the system clock and time zone.

```
DmSwitch#show clock
Wed Aug  9 12:42:27 2006
Timezone is BRA -0300
DmSwitch#
```

Related Commands

Command	Description
clock set	Configures the system date and time.
clock timezone	Specifies the time zone.
show uptime	Shows the system clock, system uptime and load average.

show core-dump

show core-dump [**all** | **standby-mpu** | **unit** *unit-number*]

Description

Shows the files stored in a core files directories.

Syntax

Parameter	Description
all	(Optional) Shows core files of all units.
standby-mpu	(Optional) Shows core files of the standby-mpu.
unit <i>unit-number</i>	(Optional) Indicates the unit for which the core files will be shown. (Range: 1-8)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.
14.0	Added standby-mpu option.

Usage Guidelines

This command shows the core file(s) stored in the DmSwitch.

Example

This example illustrates how to show the core dump file(s).

```
DmSwitch#show core-dump
Core dump file                               Size          Date
-----
issu_test.13888.713.31d8870b.core.gz        2585649        Thu Jan 1 00:13:16 1970
pktd_tq3.13859.466.ac3cc07d.core.gz         3867136        Thu Jan 1 00:09:11 1970
Total:                                       6452785
DmSwitch#
```

Related Commands

Command	Description
<code>output modifiers</code>	Options to filter text output: after, begin, exclude and include
<code>copy</code>	Copies configuration and firmware.
<code>clear core-dump</code>	Clears applications core dump files.

show counter

This command has different options for DmSwitch 3000 and DM4000 families.

Command structure for DmSwitch 3000

```
show counter [ id counter-id | filter filter-id | sort remark | table ]
```

Command structure for DM4000

```
show counter { configuration [ filter filter-id | id counter-id | sort remark | ingress | egress ] | values [ filter filter-id | id counter-id | ingress | egress ] | table { [ ingress | egress ] [ values | configuration ] } }
```

Description

Shows counters values and configurations.

Output modifiers are available for this command.

Syntax

Parameter	Description
configuration	Shows filter counters configuration.
values	Shows filter counter values.
filter <i>filter-id</i>	(Optional) Counter by filter ID.
id <i>counter-id</i>	(Optional) Counter by ID.
sort remark	(Optional) Sorting method.
ingress	Ingress counter configuration.
egress	Egress counter configuration.
table ingress values	(Optional) Shows ingress stage counter values in a table, updates automatically.
table ingress configuration	(Optional) Shows ingress stage counter configuration in a table, updates automatically.
table egress values	(Optional) Shows egress stage counter values in a table, updates automatically.
table egress configuration	(Optional) Shows egress stage counter configuration in a table, updates automatically.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
11.0	Table parameter was introduced.
11.6	<i>ingress</i> <i>egress</i> parameter was added.

Usage Guidelines

Entering this command without parameters, all ingress counters information will be shown.

Example

This example illustrates how to show the counters values and configuration

```
DmSwitch(config)#show counter values
  ID  Filter              Upper Counter Value      Lower Counter Value
  ---  -
    1
    2
DmSwitch#
```

Example for dynamic table

This example illustrates shows a dynamic table printout when running in DM4000, showing some configuration modes. This command assumes a minimum screen of 24x80 (24 lines per 80 columns), without maximum value. Page navigation is available when number of itens exceeds number of lines. Keys are U (goes 'up' in listing), D (goes 'down' in listing), and space bar to change between data visualization.

```
Counter
Id      Remark              Mode              Filter
      Upper Lower      Type      (# of)
=====
1      A_remark_message      none   all      byte      (0)
2      counter_number_two    all    none    byte      (0)
```

```
=====
spacebar->toggle screen  ESC->exit
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
counter	Configures a counter to be used by a filter
clear counter	Clears filter counters.
filter	Creates or configures a traffic filter

show cpu

```
show cpu arp-table [ filter vlan [ sort { ip|mac|vlan } | summary ] | summary | sort { ip|mac|vlan } ]
```

```
show cpu counters queues { rx|dropped } [ unit unit-number ]
```

```
show cpu egress-block
```

```
show cpu memory [ all | detail | standby-mpu | unit unit-number ]
```

```
show cpu protocol priority [ default | l2-protocol | tunnel | management | unknown ]
```

```
show cpu usage [ all | detail | standby-mpu | unit unit-number ]
```

```
show cpu packets
```

Description

Shows CPU information related to processing, memory and network.

Output modifiers are available for this command.

There is detailed information for the following commands in their respective pages:

```
show cpu arp-table
show cpu counters queues
show cpu egress-block
```

Syntax

Parameter	Description
memory	Shows CPU RAM information.
unit <i>unit-number</i>	Shows CPU RAM information of unit.
standby-mpu	Shows CPU RAM information of standby MPU.
detail	Shows CPU RAM information detailed.
all	Shows CPU RAM information of all units.
packets	Shows CPU network traffic information.

Parameter	Description
protocol	Shows protocols configuration.
priority	Shows the packets priority (CoS).
default	Shows the l2 protocols packets priority.
l2-protocol	Shows the unknown packets priority.
tunnel	Shows the tunneled packets priority.
unknown	Shows the default packet priority.
management	Shows priority of management packets.
usage	Shows CPU processing and tasks information.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.0	This command was introduced. It includes two removed commands: show cpu-usage and show memory .
7.6	The option protocol was introduced.
13.0	The options unit , standby-mpu and all were introduced in show cpu memory and usage.

Usage Guidelines

Not available.

Example

This example illustrates how to show CPU memory information.

```
DmSwitch#show cpu memory
```

```
Processor Memory Information of local unit:
```

```
Date : Thu Jan 1 13:50:52 1970
```

15s	1min	5min	30min			
Memory Total (MB)	1011	1011	1011	1011		
Memory Used (MB)	364	364	364	362		
Memory Free (MB)	647	647	647	649		
Memory Buffers (MB)	20	20	20	20		

DmSwitch#

This example illustrates how to show CPU network traffic information.

```
DmSwitch#show cpu packets
CPU Received Packets:
-----
802.1X:                1
ARP:                   489
EAPS:                  0
GVRP:                  0
IGMP:                  0
IPv4:                  610
L2 Protocol Tunnelling: 0
L2 Unknown Source:    0
LACP:                  0
Loopback Detection:    6112
OAM:                   0
PVST:                  0
Slow Protocols:        0
STP:                   3046
VTP:                   0
DmSwitch#
```

This example illustrates how to show the CPU utilization.

```
DmSwitch#show cpu usage

Processor Utilization Information of local unit:

Date : Thu Jan  1 13:52:06 1970

15s      1min      5min      30min
CPU Total (%)          7.5      6.2      6.1      6.1
CPU User (%)           6.1      4.6      4.6      4.6
CPU System (%)         1.4      1.6      1.5      1.5
CPU Niced (%)          0.0      0.0      0.0      0.0
CPU IO Wait (%)        0.0      0.0      0.0      0.0
CPU HW Interrupt (%)   0.0      0.0      0.0      0.0
CPU SW Interrupt (%)   0.0      0.0      0.0      0.0
Tasks Total           193      192      191      191
Tasks Running          1        1        1        1
Tasks Sleeping         191      191      190      190
Tasks Stopped          0        0        0        0
Tasks Zombie           1        0        0        0
Tasks U. Sleep         0        0        0        0

...

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
cpu-dos-protect	CPU Protection configuration.
show uptime	Shows the system clock, system uptime and load average.

Command	Description
<code>show cpu arp-table</code>	Shows ARP table information.
<code>show cpu counters queues</code>	Shows counters of CPU interface queues.
<code>show cpu egress-block</code>	Shows the rules for blocking forwarding of packets by the CPU.

show cpu egress-block

show cpu egress-block

Description

Shows the rules for blocking forwarding of packets by the CPU.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.5	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the CPU Egress-Block information.

```
DmSwitch(config)#cpu egress-block ethernet range 1/2 1/3 ingress ethernet range 1/2 1/3 vlan all
DmSwitch(config)#exit
DmSwitch#show cpu egress-block ethernet range 1/2 1/3 ingress ethernet range 1/2 1/3 vlan all
CPU Egress Block 1
  Egress:          Eth1/2 to Eth1/3
  Ingress:         Eth1/2 to Eth1/3
  VLAN:            All
  Discarded packets: 0

DmSwitch#
```

Related Commands

Command	Description
---------	-------------

Command	Description
<code>cpu egress-block</code>	Configures the switch to block CPU traffic from a specified Ethernet interface to another for a set of VLAN IDs.

show cpu-dos-protect

`show cpu-dos-protect [[unit] queues]`

Description

Shows the CPU denial of service protection information.

Syntax

Parameter	Description
<code>unit</code>	(Optional) Show CPU Protect information about a specific unit.
<code>queues</code>	(Optional) Show CPU Protect information about queues.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.
7.8	The queue information was introduced.
11.6	The arp request, l3-slow-path and reserved-multicast blocking information were introduced.
13.6.4	The option block subnet-broadcast was introduced.
14.0	The option queue was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the CPU denial of service protection information.

```
DmSwitch#show cpu-dos-protect
CPU DoS protect:
  Global rate limit: Disabled
  Protect CPU from destination lookup fail: Disabled
  Protect CPU from L3 slow path packets: Enabled
```

```
Protect CPU from reserved multicast packets: Enabled
Protect CPU from subnet broadcast packets: Enabled
Protect CPU from undesired ARP request: Enabled
```

```
DmSwitch#show cpu-dos-protect queues
```

```
CPU Global max-pps: 2000
```

Queue	Target	Weight	Rate Limit (pps)
47	Stacking ATP Discovery	SP	2000
46	Stacking ATP	SP	2000
45	OAM	1	1000
44	EAPS	1	500
43	ERPS	1	500
42	CFM	1	1000
41	STP	1	500
40	BPDU Tunneling	1	500
39	E-LMI	1	250
38	LACP	1	500
37	Dot1X	1	500
36	L2 Move	1	100
35	ARP	1	1000
34	GARP	1	500
33	IGMP	1	1000
32	ICMPv6	1	1000
31	VRRP	1	500
30	LBD	1	500
29	BGP	1	500
28	OSPF	1	500
27	RIP	1	500
26	RIPng	1	500
25	IS-IS	1	500
24	bfd	1	1000
23	RSVP	1	1000
22	LDP	1	500
21	Telnet	1	500
20	TFTP	1	500
19	SNTP	1	500
18	HTTP	1	500
17	SNMP	1	500
16	DHCP	1	500
15	SSH	1	500
14	LLDP	1	750
13	ICMPv4	1	300
12	Unknown Mcast PIM	1	500
11	L3 Slowpath	1	200
10	Unicast	1	500
9	MPLS OAM	1	1000
8	HTTPS	1	500
7	Unused	-	-
6	Unused	-	-
5	Unused	-	-
4	Unused	-	-
3	Reserved IPv4 Mcast	1	20
2	Multicast	1	200
1	Broadcast	1	100
0	Others	1	100

```
DmSwitch#
```

Related Commands

Command	Description
<code>cpu-dos-protect</code>	CPU Protection configuration.

show cpu arp-table

```
show cpu arp-table [ filter vlan [ sort { ip | mac | vlan } | summary ] | summary | sort { ip | mac | vlan } ]
```

Description

Shows ARP table sorted (or not) information, or a summary of all or filtered by vlan.

Output modifiers are available for this command.

Syntax

Parameter	Description
filter <i>vlan</i>	Shows the ARP table from CPU filtered by a given vlan id.
sort { ip mac vlan }	Shows the ARP table from CPU sorted by given on or more of three options of criteria.
summary	Shows the number of entries on the ARP table.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	Command is appended to show cpu options.
13.0	Options filter , sort and summary were introduced.
13.0	Added permanent (Perm) column to the command output table.

Usage Guidelines

Not available.

Example

This example illustrates how to show the ARP table.

```
DmSwitch#show cpu arp-table
```

IP Address	MAC address	VLAN	Perm
-----	-----	----	----
10.11.12.13	00:15:F2:59:B1:07	1	N

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
show cpu	Shows CPU information.
cpu-dos-protect	CPU Protection configuration.
show uptime	Shows the system clock, system uptime and load average.

show cpu counters queues

```
show cpu counters queues { rx | dropped } [ unit unit-number ]
```

Description

Shows counters of received or dropped packets for CPU interface queues.

Syntax

Parameter	Description
rx	Shows counters of received packets.
dropped	Shows counters of dropped packets.
unit <i>unit-number</i>	(Optional) Shows counters for specific unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.0	Command is appended to show cpu options.

Usage Guidelines

If you enter this command without specifying an unit, counters for all units will be shown.

Counters for units with MPUs are not shown, once the CPU packets are received through the other units.

Example

This example illustrates how to show the CPU counters queues.

```
DmSwitch#show cpu counters queues rx unit 1
Unit 1:

Queue 0 - Rx packets: 0
Queue 1 - Rx packets: 0
Queue 2 - Rx packets: 0
Queue 3 - Rx packets: 0
Queue 4 - Rx packets: 0
```

```

Queue 5 - Rx packets: 0
Queue 6 - Rx packets: 0
Queue 7 - Rx packets: 0
Queue 8 - Rx packets: 0
Queue 9 - Rx packets: 0
Queue 10 - Rx packets: 0
Queue 11 - Rx packets: 0
Queue 12 - Rx packets: 0
Queue 13 - Rx packets: 0
Queue 14 - Rx packets: 0
Queue 15 - Rx packets: 0
Queue 16 - Rx packets: 0
Queue 17 - Rx packets: 0
Queue 18 - Rx packets: 0
Queue 19 - Rx packets: 0
Queue 20 - Rx packets: 0
Queue 21 - Rx packets: 0
Queue 22 - Rx packets: 0
Queue 23 - Rx packets: 0
Queue 24 - Rx packets: 0
Queue 25 - Rx packets: 0
Queue 26 - Rx packets: 0
Queue 27 - Rx packets: 0
Queue 28 - Rx packets: 0
Queue 29 - Rx packets: 0
Queue 30 - Rx packets: 0
Queue 31 - Rx packets: 0
Queue 32 - Rx packets: 0
Queue 33 - Rx packets: 0
Queue 34 - Rx packets: 0
Queue 35 - Rx packets: 0
Queue 36 - Rx packets: 0
Queue 37 - Rx packets: 0
Queue 38 - Rx packets: 0
Queue 39 - Rx packets: 0
Queue 40 - Rx packets: 0
Queue 41 - Rx packets: 2141
Queue 42 - Rx packets: 0
Queue 43 - Rx packets: 0
Queue 44 - Rx packets: 0
Queue 45 - Rx packets: 0
Queue 46 - Rx packets: 0
Queue 47 - Rx packets: 0

```

DmSwitch#

Related Commands

Command	Description
clear cpu counters queues	Clear counters of CPU interfaces queues.
cpu-dos-protect	CPU Protection configuration.

show debug-counters rx

```
show debug-counters rx { all | attack | discard | drop | received/others [ unit  
unit-number ] }
```

Description

Shows the debug counters configuration.

Output modifiers are available for this command.

Syntax

Parameter	Description
all	Shows configuration for all RX groups.
attack	Shows configuration for attack group.
discard	Shows configuration for discard group.
drop	Shows configuration for drop group.
received/others	Shows configuration for received/others group.
unit <i>unit-number</i>	Shows configuration for a specific unit.

Default

If the parameter unit is not used, the command will show the configuration of all the units.

Command Modes

User EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Example

This example illustrates the usage of the command

```
DmSwitch#show debug-counters rx attack
Attack:
    disabled      dsfrag      DOS fragment error packets
    disabled      dsicmp      DOS ICMP error packets
    disabled      dsl3he      DOS L3 header error packets (only applicable to packet
from 10GE port)
    disabled      dsl4he      DOS L4 header error packets (only applicable to packet
```



```
from 10GE port)
    disabled          macsaequalmacda      DOS Attack L2 Packets MACSA equals to MACDA
DmSwitch#
```

Related Commands

Command	Description
debug-counters rx	Shows the interface counters information.
show interface counters	Shows the interface counters information.

show debugging

show debugging

Description

Shows the current debugging status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the process debugging status.

```
DmSwitch#show debugging
STP debugging status: disabled
LACP debugging status: disabled
Link debugging status: disabled
EAPS debugging status: disabled

DmSwitch#
```

Related Commands

Command	Description
debug	Enables the printing of debug messages.

show debugging cfm

show debugging cfm

Description

Shows the current CFM debugging status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the CFM process debugging status.

```
DmSwitch#show debugging cfm

MD: MD, MA: MA, MEP ID 1:
  Events:      AIS, CC, DM,
  Packets:     None
  Packets-hex: LB, LT,
  States:     None

DmSwitch#
```

Related Commands

Command	Description
debug	Enables the printing of debug messages.

show debugging dot1x

show debugging dot1x

Description

Shows the current 802.1X debugging status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the dot1x debugging status. This example has 802.1X packet in hexadecimal debug enable.

```
DmSwitch#show debugging dot1x
Eth 1/1:
Packet-hex: enabled

DmSwitch#
```

Related Commands

Command	Description
debug	Enables the printing of debug messages.
dot1x system-auth-control	Configures global options for 802.1X.

show debugging elmi

show debugging elmi

Description

Shows the current E-LMI debugging status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the dot1x debugging status. This example has E-LMI event debug enable.

```
DmSwitch#show debugging elmi
Eth 1/1:
Event: enabled

DmSwitch#
```

Related Commands

Command	Description
debug	Enables the printing of debug messages.
elmi	Enters on Ethernet Local Management Interface protocol configuration mode.

show debugging oam

show debugging oam

Description

Shows the current OAM debugging status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the OAM process debugging status.

```
DmSwitch#show debugging oam
```

```

OAM debugging
-----
          Packet
Port      Event      Decode      Hex
-----
1/ 1      enabled      --          --
1/ 2              --          --
1/ 3              --          Tx          --
1/ 4              --          Tx/Rx       --
1/ 5              --          --          Rx
1/ 6              --          --          Tx/Rx
1/ 7              --          --          --
1/ 8              --          --          --
1/ 9              --          --          --
1/10              --          --          --
1/11              --          --          --
1/12              --          --          --
```

```
1/13      --      --      --  
  
DmSwitch#
```

Related Commands

Command	Description
debug	Enables the printing of debug messages.

show dot1x

```
show dot1x
```

```
show dot1x interface ethernet unit-number/port-number [ detail ]
```

```
show dot1x interface ethernet range first-unit-number/first-port-number  
last-unit-number/last-port-number [ detail ]
```

```
show dot1x interface ethernet all [ detail ]
```

Description

Shows 802.1X information.

Output modifiers are available for this command.

Syntax

Parameter	Description
interface ethernet all	Show 802.1X information on all ports
interface ethernet range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Show 802.1X information of a given range of ports
interface ethernet [<i>unit-number/</i>] <i>port-number</i>	Show 802.1X information of a specific given port
detail	Show all 802.1X information not given by default

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
12.2	Added more options for showing information on specifics ports
14.0	Introduced accounting informations.

Usage Guidelines

This command shows the 802.1X global status, the port access mode for clients, the supplicant MAC address, uptime, timeout and the authorization status for the port.

Example

This example illustrates how to show the 802.1X information.

```
DmSwitch#show dot1x
System configuration:
  Global enable                      Enabled
  Protocol version:                  2.0
  Capabilities:                      Authenticator
  Captive Portal VLAN:               1130
  Maximum users (Multi-auth ports): 1024
  Total users (Multi-auth ports):    60
  Accounting:                        Enabled
  Accounting interval (s):            600
  Accounting traffic monitoring:      Enabled

DMSwitch#show dot1x interface ethernet 2/10
Ethernet 2/10:
  Configuration:
    Port control:                    Auto
    Host mode:                       Single
    Controlled directions:           Both
    Quiet period (s):                 60
    Server timeout (s):               30
    Re-authentication:               Enabled
    Maximum re-authentication tries: 10
    Re-authentication period (s):     30
    Key transmission:                 Disabled
    MAC Authentication:               Disabled
    Captive Portal:                   Disabled
    Guest VLAN:                       None
    Restricted VLAN:                  None
    Maximum users on port:            16
  -----
  Supplicant:                        00:04:DF:67:62:B1
  Status:
    Port status:                     Authorized
    Authenticated by:                 AAA Server
    Operational controlled directions: Both
    Authenticator PAE state:          Authenticated
    Backend authentication state:     Idle

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
dot1x accounting	Configures global options for 802.1X RADIUS accounting.
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.

Command	Description
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x re-auth-max</code>	Sets the maximum EAP request/identity packet retransmissions.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>dot1x re-auth-enable</code>	Enables or disables periodic re-authentication.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x quiet-period</code>	Defines dot1x quiet period timeout value.

show dscp-table

show dscp-table

Description

Shows Differentiated Services Code Point mapping table.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
7.6.4	This command was introduced.

Usage Guidelines

Entering this command you will see all DSCP mapping configuration, i.e., DSCP to DSCP, 802.1p and color.

Example

This example illustrates how to show DSCP table.

```
DmSwitch#show dscp-table
DSCP Src  DSCP Dst  802.1p  Color  |  DSCP Src  DSCP Dst  802.1p  Color
-----
          0          1          0 green  |          32          50          5 green
          1          1          0 green  |          33          50          5 green
          2          2          0 green  |          34          50          5 green
          3          3          0 green  |          35          50          5 green
          4          4          0 green  |          36          50          5 green
          5          5          7 red    |          37          50          5 green
          6          6          7 red    |          38          50          5 green
          7          7          7 red    |          39          50          5 green
          8          8          7 red    |          40          50          5 green
          9          9          7 red    |          41          50          5 green
         10         10          0 green  |          42          50          5 green
         11         11          0 green  |          43          50          5 green
         12         12          0 green  |          44          50          5 green
         13         13          0 green  |          45          50          5 green
         14         14          0 green  |          46          50          5 green
         15         20          3 green  |          47          50          5 green
```

```

16      16      0 green |      48      50      5 green
17      17      0 green |      49      50      5 green
18      18      0 green |      50      50      5 green
19      19      0 green |      51      50      5 green
20      20      0 red   |      52      50      5 green
21      21      0 red   |      53      50      5 green
22      22      0 red   |      54      50      5 green
23      23      0 red   |      55      50      5 green
24      24      0 red   |      56      50      5 green
25      25      0 red   |      57      50      5 green
26      26      0 green |      58      50      5 green
27      27      0 green |      59      50      5 green
28      28      0 green |      60      50      5 green
29      29      0 green |      61      50      5 green
30      50      5 green |      62      50      5 green
31      50      5 green |      63      50      5 green

```

DmSwitch#

Related Commands

Command	Description
dscp-table	Configure Differentiated Services Code Point mappings

show eaps

show eaps [**detail** | **id** *domain*]

Description

Shows EAPS settings.

Output modifiers are available for this command.

Syntax

Parameter	Description
detail	(Optional) Shows more details of EAPS settings.
id <i>domain</i>	(Optional) Shows only the EAPS settings from the specified domain.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

Entering this command without parameters, all EAPS domains will be shown.

Example

This example illustrates how to show the EAPS settings from the domain 1.

```
DmSwitch#show eaps id 1
Global configuration:
EAPS hardware forwarding: Disabled
```

```
Domain ID:          1
Domain Name:        test
```



```

State:                Links-Up
Mode:                 Transit
Encapsulation Mode:   Standard
Hello Timer interval: 1 sec
Fail Timer interval:  3 sec
Pre-forwarding Timer: 6 sec (learned)      Remaining:  0 sec
Last update from:     (none)
Primary port:         Eth1/25              Port status: Up
Secondary port:       Eth1/26              Port status: Blocked
Control VLAN ID:      101
Protected VLAN group IDs: 1

DmSwitch#

```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
eaps hw-forwarding	Enables EAPS hardware forwarding in DmSwitch.
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show running-config	Shows the current operating configuration.

show elmi

show elmi [**interface ethernet** { **all** | [*unit-number/*] *port-number* | **range** [*first-unit-number/*] *first-port-number* [*last-unit-number/*] *last-port-number* } [**detail**]]

Description

Shows Ethernet Local Management Interface settings.

Syntax

Parameter	Description
all	Displays configuration and status information for all units and ports.
[<i>unit-number/</i>] <i>port-number</i>	Displays configuration and status information for a specific unit and port.
range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Displays configuration and status information for a range of units and ports.
detail	(Optional) Displays detailed configuration and status information.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, all interfaces status will be shown.

Example

This example illustrates how to show the ELMI configuration of a specific port.

```
DmSwitch#show elmi interface ethernet 1
Interface Ethernet 1/1 (UNI-C) (00:04:DF:14:6D:E7):
  Configuration:
```

```
    Polling timer (s):          10
    Polling counter:           360
    Status counter:            3
    List of EVCs:              No EVC is configured

DmSwitch#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
elmi	Enters on Ethernet Local Management Interface protocol configuration mode.
uni-c	Creates or edits User Network Interface (UNI) on Customer Edge devices.
uni-n	Creates or edits User Network Interface (UNI) on Provider Edge devices.

show erps

show erps [**detail** | **id** *domain*]

Description

Shows ERPS settings.

Output modifiers are available for this command.

Syntax

Parameter	Description
detail	(Optional) Shows more details of ERPS settings.
id <i>domain</i>	(Optional) Shows only the ERPS settings from the specified domain.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

If this command is executed without parameters, all ERPS domains are shown.

Example

This example illustrates how to show the ERPS settings from the domain 1.

```
DmSwitch#show erps id 1
Domain ID:                1
Domain Name:
State:                    IDLE
Mode:                     RPL owner
HW Forwarding:            Disabled
Guard Timer (ms):         500
WTR Timer (min):          5
```

```

Holdoff Timer (ms):          0
Port 0:                     Eth1/11      Port status: Blocked
Port 1:                     Eth1/12      Port status: Unblocked
Control VLAN ID:            4000
Protected VLAN group IDs:    1
Accept topology change of domains:

```

```
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

show filter

```
show filter [ action-type { counter | monitor | qos | security | vlan } | id filter-id  
| pre-ingress { ethernet [ unit-number/ ] port-number | id filter-id } | ingress { ethernet  
[ unit-number/ ] port-number | id filter-id } | egress { ethernet [ unit-number/ ] port-number |  
id filter-id } | meter meter-id | resources [ full ] | priority-usage [ ingress | egress |  
pre-ingress ] | sort remark | state { disabled | enabled }
```

Description

Shows filters information.

Output modifiers are available for this command.

Syntax

Parameter	Description
action-type counter	(Optional) Shows filters with counter actions.
action-type monitor	(Optional) Shows filters with monitoring actions.
action-type qos	(Optional) Shows filters with QoS actions.
action-type security	(Optional) Shows filters with security actions.
action-type vlan	(Optional) Shows filters with VLAN actions.
id filter-id	(Optional) Specifies the filter ID.
ingress ethernet [unit-number/] port-number	(Optional) Filters by an ingress port.
ingress id filter-id	(Optional) Filters by an ingress filter id.
egress ethernet [unit-number/] port-number	(Optional) Filters by an egress port.
egress id filter-id	(Optional) Filters by an egress filter id.
meter meter-id	(Optional) Filters by an meter ID.
resources full	(Optional) Shows full filter resources.
resources	(Optional) Shows filter resources of used priorities.
priority-usage [ingress egress pre-ingress]	(Optional) Shows table of filter priorities and its enabled qualify sets.
sort remark	(Optional) Sorts by filter remark.
state disabled	(Optional) Shows only disabled filters.
state enabled	(Optional) Shows only enabled filters.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
11.6	<i>ingress</i> <i>egress</i> parameter was added.
13.0	<i>priority-usage</i> parameter was added.
13.4	<i>egress</i> parameter was added in DM4100 boards.

Usage Guidelines

Entering this command without parameters, all filters will be shown.

Example

This example illustrates how to show the filters configuration.

```
DmSwitch#show filter ingress
Filter 1: enabled, priority 8
  Actions:    permit
  Matches:    All packets
  Ingress:    Eth1/20

Filter 2: enabled, priority 10
  Actions:    deny
  Matches:    destination-ip host 10.10.10.80
  Ingress:

Filter 3: enabled, priority
  Actions:    monitor
  Matches:    vlan 2
  Ingress:

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
meter	Configures a meter to be used by a filter
filter	Creates or configures a traffic filter

show firmware

show firmware [**all** | **summary** | **standby-mpu** | **unit** *unit-number*]

Description

Shows firmware information.

Syntax

Parameter	Description
all	(Optional) Shows firmware information of all units.
summary	(Optional) Shows firmware information summary for all units.
unit <i>unit-number</i>	(Optional) Indicates the unit for which the firmware information will be shown. (Range: 1-8)[1]
standby-mpu	(Optional) Shows firmware information for standby-mpu.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the firmware(s) image(s) information stored in the DmSwitch. Entering this command without parameters, all images information will be shown.

Example

This example illustrates how to show the firmware information.

```
DmSwitch#show firmware
Running firmware:
  Firmware version: 3.1
  Stack version:    1
  Compile date:     Wed Jun  7 14:29:23 UTC 2006
```



```
Flash firmware:
  ID  Version                Date                Flag  Size
  1    3.1                07/06/2006 14:29:30  RS    7510368
  2    3.0                08/05/2006 20:47:21             7420088

Flags:
  R - Running firmware.
  S - To be used upon next startup.
  E - Empty/Error

DmSwitch#
```

Related Commands

Command	Description
copy	Copies configuration and firmware.
erase	Erases spare firmware or configuration position.
select	Selects the startup firmware and flash for the next reboot.
show flash	Shows flash information.

Notes

[1] - Range 1-8 available only to DM4000 Switches.

show flash

show flash

Description

Shows flash information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the firmware(s) image(s) and the flash positions information stored in the DmSwitch.

Example

This example illustrates how to show the flash information.

```
DmSwitch#show flash
```

```
BootLoader version: 1.1.2-1
```

```
Flash firmware:
```

ID	Version	Date	Flags	Size
1	3.1	07/06/2006 14:29:30	RS	7510368
2	3.0	08/05/2006 20:47:21		7420088

```
Flash config:
```

ID	Name	Date	Flags	Size
1	EAPS	07/05/2006 19:20:35		443
2	METRO	15/08/2006 00:17:43		3044
3	TEST	01/03/2006 08:24:15		443
4	DEFAULT	19/04/2006 11:03:48	S	452

```
Flags:
```

```
R - Running firmware.
```

```
S - To be used upon next startup.
```

```
E - Empty/Error
```

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
copy	Copies configuration and firmware.
diff	Compares and shows the differences between two configurations.
erase	Erases spare firmware or configuration position.
select	Selects the startup firmware and flash for the next reboot.
show firmware	Shows firmware information.
show flash-config	Shows the configuration stored in a specific flash position.
show startup-config	Shows the startup flash configuration.

show flash-config

show flash-config *index*

Description

Shows the configuration stored in a specific flash position.

Output modifiers are available for this command.

Syntax

Parameter	Description
<i>index</i>	Specifies a flash configuration memory position. (Range: 1-4)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the stored configuration in a specific flash memory position. It also shows the configuration in the same structure that the information presented in the **show running-config** command.

Example

This example illustrates how to show the flash configuration from the flash 4.

```
DmSwitch#show flash-config 4
Building configuration...
!
hostname DmSwitchTest
!
username admin access-level 15
username admin password 7 d033e22ae348aeb5660fc2140aec35850c4da997
username guest access-level 0
```

```

username guest password 7 35675e68f4b5af7b995d9205ad0fc43842f16450
!
ip telnet server
ip http server
ip http secure-server
no ip ssh server
!
ip snmp-server community public ro
!
interface vlan 1
  name VLAN_Test
  ip address 192.168.110.1/24
  set-member untagged ethernet all
!
spanning-tree 1
spanning-tree 1 vlan all
!
DmSwitch#

```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
copy	Copies configuration and firmware.
diff	Compares and shows the differences between two configurations.
erase	Erases spare firmware or configuration position.
select	Selects the startup firmware and flash for the next reboot.
show flash	Shows flash information.
show running-config	Shows the current operating configuration.
show startup-config	Shows the startup flash configuration.

show garp

```
show garp { timer [ ethernet [ unit-number/ ] port-number | port-channel channel-group-number ] }
```

Description

Shows GARP properties.

Syntax

Parameter	Description
timer	Specifies the GARP timer parameters.
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Shows parameters of a specific unit and port.
port-channel <i>channel-group-number</i>	(Optional) Shows parameters of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the GARP time properties of a specific Ethernet port.

```
DmSwitch#show garp timer ethernet 1
Eth 1/1 GARP timer status:
  Join timer:      20
  Leave timer:     60
  Leaveall timer: 1000
DmSwitch#
```

Related Commands

Command	Description
<code>bridge-ext gvrp</code>	Enables GVRP globally for the switch.
<code>garp timer</code>	Set values for GARP timers.
<code>show gvrp</code>	Shows GVRP configuration.
<code>show running-config</code>	Shows the current operating configuration.
<code>switchport gvrp</code>	Enables GVRP for a specific port.

show gvrp

```
show gvrp { configuration [ ethernet [ unit-number/ ] port-number | port-channel
channel-group-number ] }
```

Description

Shows GVRP configuration.

Output modifiers are available for this command.

Syntax

Parameter	Description
configuration	Specifies the GVRP configuration.
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Shows parameters of a specific unit and port.
port-channel <i>channel-group-number</i>	(Optional) Shows parameters of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-32)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the GVRP configuration of a specific Ethernet port.

```
DmSwitch#show gvrp configuration ethernet 5
Eth 1/5:
  GVRP configuration: Disabled
DmSwitch#
```


Related Commands

Command	Description
<code>output modifiers</code>	Options to filter text output: after, begin, exclude and include
<code>bridge-ext gvrp</code>	Enables GVRP globally for the switch.
<code>garp timer</code>	Set values for GARP timers.
<code>show garp timer</code>	Shows GARP properties.
<code>show running-config</code>	Shows the current operating configuration.
<code>switchport gvrp</code>	Enables GVRP for a specific port.

show hardware-status

show hardware-status

Description

Shows the hardware status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the power supply and fans status, if the alarm input and output are turned on or turned off, and if the DmSwitch has optical modules connected.

In order to alarm out some fail in the PSU, fans or any alarm input, it is necessary to enable external alarm output.

Example

This example illustrates how to show the hardware status.

```
DmSwitch#show hardware-status
```

Unit	Power		Fans				Alarms In		Alarm	Temperature
	Main	RPU	1	2	3	4	1	2	Out	[Celsius]
1	Ok	Ok	Ok	Ok	Ok	Ok	Off	Off	Off	50

```
RPU
```

```
---
```

Unit	Power	Status
1	300000 mW	OK

```
Transceiver Presence
-----

Unit 1
  2  4  6  8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50

    1  3  5  7  9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49

Unit Fan  Status  Speed (RPM)  expected speed(RPM)
-----
  1    1    Fail      8720      11363 (9658 to 14771)
  1    2    Fail      8620      11363 (9658 to 14771)
  1    3    Fail      8152      11363 (9658 to 14771)
  1    4     Ok     10000           > 7500

DmSwitch#
```

Related Commands

Command	Description
external-alarm	Enables the external alarm through the DB9 or RJ45 alarm interface.

show hardware-status fans fuses

show hardware status fans fuses

Description

Shows status of fuses in the fan module.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

The status of all fuses present in the fan module are shown when this command is issued. Blown fuses (with "Fail" status) can help diagnose fan failure on DM4008 fan modules. Each fuse protects the power supply of two fans:

Fuse	Fans
1	1 and 2
2	3 and 4
3	5 and 6
4	7 and 8

Example

This would be the output of the command if fuses 3 and 4 were blown:

```
DmSwitch#show hardware-status fans fuses

Fuse 1: OK
Fuse 2: OK
```

```
Fuse 3:  Fail
Fuse 4:  Fail

DmSwitch#
```

Related Commands

No related commands.

show hardware-status transceivers detail

```
show hardware status transceivers detail [ ethernet { [ unit-number/ ] port-number } ]
```

Description

Shows details about hardware transceivers.

Syntax

Parameter	Description
ethernet [unit-number/] port-number	(Optional) Shows details about hardware transceivers on a specified unit and port. (Range:1-1/1-28)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

Entering this command without parameters, all informations about optical modules connected will be shown.

Example

This example illustrates how to show the details about transceiver connected in port 28.

```
DmSwitch#show hardware-status transceivers detail
Information of port 1/28
Vendor information:
  Vendor Name:          DATACOM
  Manufacturer:        APAC Opto
  Part Number:          LS48-E3U-TC-N-DD
  Media:                Single Mode (SM)
  Ethernet Standard:    [Not available]
  Connector:            LC
Digital Diagnostic:
  Temperature:          23 C
```

Voltage 3.3V:	3.4V
Current:	21.0mA
Tx-Power:	1.5dBm
Rx-Power:	off
DmSwitch#	

Related Commands

No related command.

show hardware-status transceivers presence

`show hardware status transceivers presence`

Description

Shows the presence of optical modules in the switch.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

This command shows the presence of optical modules in the switch.

Example

This example illustrates how to show the presence of optical module in port 24.

```
DmSwitch#show hardware-status transceivers presence
```

```
Transceiver Presence
-----
Unit 1
      2  4  6  8 10 12 14 16 18 20 22 24 26 28
                        X
      1  3  5  7  9 11 13 15 17 19 21 23 25 27

DmSwitch#
```


Related Commands

Command	Description
<code>show interfaces status</code>	Shows interface configuration status.
<code>show interfaces link</code>	Shows interfaces link.

show history

show history

Description

Lists the last commands entered in current session.
Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to list the last commands entered:

```
DmSwitch#show history
1: configure
2: hostname SWA
3: exit
4: show history
SWA#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include

show hqos

```
show hqos [ hqos-id [ service [ service-id ] ] ]
```

Description

Show HQoS information.

Syntax

Parameter	Description
<i>hqos-id</i>	(Optional) Show HQoS domain of the specified ID.
service	(Optional) Show all services of the specified HQoS domain.
service <i>service-id</i>	(Optional) Show the service specified by service-id of the selected HQoS domain.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.4	This command was introduced.

Usage Guidelines

Entering this command without parameters, all HQoS domains will be shown.

Example

This example illustrate how to show the HQoS domains.

```
DmSwitch#show hqos
```

```
H-QoS domain 1: priority 1
  Ingress:      Eth1/5
  VLAN:         1
  Rate-limit:   0 kbit/s
  Burst size:   4 kbyte
```

```
H-QoS domain 2: priority 8
  Ingress:      Eth1/1 to Eth1/48
  VLAN:         2
  Rate-limit:   64 kbit/s
  Burst size:   16 kbyte
DmSwitch#
```

This another example displays how the services of the HQoS domain 1 are exhibited.

```
DmSwitch#show hqos 1 service
```

```
H-QoS service 1:
  DSCP:         10
  CIR:          4032 kbit/s
  CBS:          4 kbyte
  PIR:          10048 kbit/s
  PBS:          4 kbyte
```

```
H-QoS service 2:
  DSCP:         20
  CIR:          6016 kbit/s
  CBS:          4 kbyte
  PIR:          10048 kbit/s
  PBS:          4 kbyte
DmSwitch#
```

Related Commands

Command	Description
hqos	Creates or configures an HQoS domain
service	Creates or configures an HQoS service

show interfaces bundle

```
show interfaces bundle { all | [unit-number/ ] bundle-id | range { [first-unit-number/ ] first-bundle-id [ last-unit-number/ ] last-bundle-id } }
```

Description

Show information about bundle interfaces.

Syntax

Parameter	Description
all	Display information about all bundle interfaces.
<i>unit-number/] bundle-id</i>	Bundle index.
range { [<i>first-unit-number/] first-bundle-id</i> [<i>last-unit-number/] last-bundle-id</i> }	Range of bundle interfaces.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display information about bundle interface 5 of unit 1.

```
DM4000#show interfaces bundle 1/5
Bundle 1/5 Interface:
Basic Configuration:
  Enable:                Enabled
  Name:                  Not set
  Packet delay:          2.000 ms
  Jitter-buffer:         10.000 ms
  VLAN:                  2200
```

```

    Priority          7
    QinQ:            -
    Priority          -
    PSN type:        UDP

Advanced Configuration:
  Packet loss Threshold: 1.00 %
  Lost Packet Fill:     Repeat Last Data
  R bit send RAI:       Disabled
  Jitter Buffer History:
    Enable:             Enabled
    Interval:           1200 sec

TDM channel:
  Type:               E1C
  Index:              5
  Initial timeslot:    0
  Number of timeslots: 32

UDP:
  Destination Bundle:  5
  Destination IP Address: 1.1.1.2
  IP Next Hop:         -
  Source IP Address:   1.1.1.1/16
  DSCP:                0

Tests:
  Ethernet Bert test:  Disabled
  TDM Bert test:       Enabled
  Loop test:           Disabled

Details:
  Min. Jitter Buffer:   4.000 ms
  Max. Jitter Buffer:   124.000 ms
  Packet Size:         562 bytes
  Payload Size:        512 bytes
  Packet rate:         500 Pkts/s
  Throughput:          2264000 bits/s

DM4000#

```

Related Commands

Command	Description
name	Defines bundle circuit name
destination-bundle	Defines destination bundle id
destination-ip-address	Defines bundle destination ip address
destination-mac	Defines destination mac address
dscp	Configures DSCP for destination IP address
ecid	Configure ECID
ip-next-hop	Defines bundle ip-next-hop
jitter-buffer	Defines bundle jitter-buffer size
lops-limits	Configure LOPS limits.
packet-delay	Defines a value for packet-delay
psn-type	Configure psn-type.

Command	Description
source-ip-address	Defines bundle source ip address
tdm-channel	Maps bundle in E1 interface
test	Configures tests for the bundle interface
timeslots	Configures inicial timeslot and how many are used.
vlan	Defines which vlan current bundle interface will use.

show interfaces counters

```
show interfaces counters [ detail | summary | bundle { all | range
[ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number | [ unit-number/ ]
bundle-id [ jitter-buffer-history [ detail ] ] } | ptp [ unit-number/ ] ptp-id | {
pwe3-chipset unit unit-number | ptp-chipset unit unit-number | ethernet
[ unit-number/ ] port-number | port-channel channel-group-number | stacking [
unit-number/ ] stack-port } [ debug | detail | summary | queue ]]
```

Description

Shows the interface counters information.

Output modifiers are available for this command.

Syntax

Parameter	Description
debug	(Optional) Shows only the debug counters (only available for ethernet and port-channel).
detail	(Optional) Shows detailed counters information.
summary	(Optional) Shows only the iftable counters.
queue	(Optional) Shows information about transmitted and dropped packets in the eight CoS queues.
pwe3-chipset unit unit-number	(Optional)Shows pseudowire chipset counters of a specific unit.
ptp-chipset unit unit-number	(Optional)Shows precision time protocol chipset counters of a specific unit.
ethernet [unit-number/] port-number	(Optional) Shows counters of a specific unit and port.
ptp [unit-number/] ptp-id	(Optional) Shows counters of a specific ptp interface. (Range: 1-16)
port-channel channel-group-number	(Optional) Shows counters of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
bundle all	(Optional) Shows description of all bundle interfaces.
bundle range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	(Optional) Shows description for a specific range of units and ports.
bundle bundle-id	(Optional) Shows counters of a specific unit and bundle interface. (Range: 1-256)
bundle bundle-id	(Optional) Shows historic jitter-buffer occupation values of a specific unit and bundle interface. (Range: 1-256)
jitter-buffer-history	
stacking [unit-number/] stack-port	(Optional) Shows counters of a specific stacking port. (Range: depends on the switch model and can be viewed with CLI's built-in help -- press "?").

Default

Summary.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.2	The commands bundle, ptp, ptp-chipset and pwe3-chipset were introduced.
13.4	The "debug" option was introduced.

Usage Guidelines

If you enter this command without parameters, all interface counters will be shown.

Example 1

This example illustrates how to show the counters of a specific Ethernet port.

```
DmSwitch#show
interfaces counters ethernet 1
Eth 1/1
Octets input : 140553
Octets output : 344253
Unicast input : 1061
Unicast output : 1052
Discard input : 0
Discard
output : 0
Error input : 0
Error output : 0
Unknown protos input : 0
QLen : 0
DmSwitch#
```

Example 2

This example illustrates how to show the counters of the first stacking port (S1) of unit 4.

```
DmSwitch#show
interfaces counters stacking 4/S1
Stacking Port 4/S1
Octets input : 948409
Octets output : 1123459
Unicast input : 8591
Unicast output : 8592
```

```
Discard
input : 0
Discard output : 0
Error input : 0
Error output : 0
Unknown protos input : 0
QLen : 0
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
clear interface counters	Clear interface counters.
clear counter	Clears filter counters.
debug-counters rx	Shows the interface counters information.
show debug counters rx	Shows debug-counters RX configuration.

show interfaces description

```
show interfaces description [ ethernet { all | [ unit-number/ ] port-number | range  
[ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } | port-channel  
channel-group-number ]
```

Description

Shows interface description.

Syntax

Parameter	Description
ethernet all	(Optional) Shows description of all ethernet ports.
ethernet <i>[unit-number/] port-number</i>	(Optional) Shows description of a specific unit and port. (Range: 1-1/1-28)
ethernet range { <i>[first-unit-number/] first-port-number [last-unit-number/] last-port-number</i>	(Optional) Shows description for a specific range of units and ports. (Range: 1-1/1-28)
port-channel <i>channel-group-number</i>	(Optional) Shows interface description of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

Entering this command without parameters, all interface descriptions will be shown.

Example

This example illustrates how to show the description of a specific port.

```
DmSwitch#show interfaces description ethernet 28
Eth 1/28:  Description of the interface ethernet port 28
DmSwitch#
```

Related Commands

No related command.

Command	Description
description	Inserts a description for an interface.

show interfaces e1c

```
show interfaces e1c { all | [ unit-number/ ] e1c-id | range { [ first-unit-number/ ]  
first-e1c-id [ last-unit-number/ ] last-e1c-id } }
```

Description

Show information about e1c interfaces.

Syntax

Parameter	Description
all	Display information about all e1c interfaces.
mappings [unit-number/] e1c-id	Display timeslot mappings of a given E1C interface.
[unit-number/] bundle-id	E1C index.
range { [first-unit-number/] first-bundle-id [last-unit-number/] last-bundle-id	Range of e1c interfaces.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to display information about e1c interfaces from 5 to 7 of unit 1.

```
DM4000#show interfaces e1c range 1/5 1/7  
E1C 1/5 Interface:  
Configuration:  
  Enable: Enable  
  Line Type: PCM30 w/ CAS  
  
E1C 1/6 Interface:
```

```

Configuration:
  Enable:          Disable
  Line Type:       Unframed

E1C 1/7 Interface:
Configuration:
  Enable:          Disable
  Line Type:       Unframed

DM4000#

```

Related Commands

Command	Description
circuit-name	Defines bundle circuit name
destination bundle	Defines destination bundle id
destination-ip-adress	Defines bundle destination ip address
dscp	Configures DSCP for destination IP address
ip-next-hop	Defines bundle ip-next-hop
jitter buffer	Defines bundle jitter-buffer size
packet delay	Defines a value for packet-delay
tdm channel	Maps bundle in E1 interface
timeslots	Configures inicial timeslot and how many are used.

show interfaces e1c mappings

show interfaces e1c mappings [*unit-number/*] *e1c-id*

Description

Show information about E1C interfaces.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>e1c-id</i>	Display timeslot mappings of a given E1C interface.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to display information about e1c interfaces from 5 to 7 of unit 1.

```
DM4000#show interfaces e1c mappings 1
```

```
E1C Interface Mappings:
```

```
-----  
| TS      | 0| 1| 2| 3| 4| 5| 6| 7| 8| 9|10|11|12|13|14|15|  
| Bundle  | 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1|  
-----  
| TS      |16|17|18|19|20|21|22|23|24|25|26|27|28|29|30|31|  
| Bundle  | 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1|  
-----
```

```
* Unavailable  
- Not used
```

DM4000#

Related Commands

Command	Description
circuit-name	Defines bundle circuit name
destination bundle	Defines destination bundle id
destination-ip-adress	Defines bundle destination ip address
dscp	Configures DSCP for destination IP address
ip-next-hop	Defines bundle ip-next-hop
jitter buffer	Defines bundle jitter-buffer size
packet delay	Defines a value for packet-delay
tdm channel	Maps bundle in E1 interface
timeslots	Configures inicial timeslot and how many are used.

show interfaces g704

```
show interfaces g704 { all | [ unit-number/ ] g704-id | range { [ first-unit-number/ ]  
first-g704-id [ last-unit-number/ ] last-g704-id } }
```

Description

Show information about g704 interfaces.

Syntax

Parameter	Description
all	Display information about all g704 interfaces.
mappings [unit-number/] g704-id	Display timeslot mappings of a given G704 interface.
[unit-number/] bundle-id	G704 index.
range { [first-unit-number/] first-bundle-id [last-unit-number/] last-bundle-id }	Range of g704 interfaces.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display information about g704 interfaces from 5 to 7 of unit 1.

```
DM4000#show interfaces g704 range 1/5 1/7  
G704 1/5 Interface:  
Configuration:  
  Enable: Enable  
  Line Type: PCM30 w/ CAS  
  Sync Source: System  
Test:
```

```

LAL:          Enable
LDL:          Disable

G704 1/6 Interface:
Configuration:
  Enable:      Disable
  Line Type:   Unframed
  Sync Source: Adaptive
  Bundle:      1/1
Test:
  LAL:         Disable
  LDL:         Enable

G704 1/7 Interface:
Configuration:
  Enable:      Disable
  Line Type:   Unframed
  Sync Source: Adaptive
  Bundle:      1/2
Test:
  LAL:         Disable
  LDL:         Disable

DM4000#

```

Related Commands

Command	Description
circuit-name	Defines bundle circuit name
destination bundle	Defines destination bundle id
destination-ip-adress	Defines bundle destination ip address
dscp	Configures DSCP for destination IP address
ip-next-hop	Defines bundle ip-next-hop
jitter buffer	Defines bundle jitter-buffer size
packet delay	Defines a value for packet-delay
tdm channel	Maps bundle in E1 interface
timeslots	Configures inicial timeslot and how many are used.

show interfaces g704 mappings

show interfaces g704 mappings [*unit-number/*] *g704-id*

Description

Show information about G704 interfaces.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>g704-id</i>	Display timeslot mappings of a given G704 interface.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display information about g704 interfaces from 5 to 7 of unit 1.

```
DM4000#show interfaces g704 mappings 1
```

```
G704 Interface Mappings:
```

```
-----
| TS      | 0| 1| 2| 3| 4| 5| 6| 7| 8| 9|10|11|12|13|14|15|
| Bundle  | 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1|
-----
| TS      |16|17|18|19|20|21|22|23|24|25|26|27|28|29|30|31|
| Bundle  | 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1| 1|
-----
```

```
* Unavailable
- Not used
```

DM4000#

Related Commands

Command	Description
circuit-name	Defines bundle circuit name
destination bundle	Defines destination bundle id
destination-ip-adress	Defines bundle destination ip address
dscp	Configures DSCP for destination IP address
ip-next-hop	Defines bundle ip-next-hop
jitter buffer	Defines bundle jitter-buffer size
packet delay	Defines a value for packet-delay
tdm channel	Maps bundle in E1 interface
timeslots	Configures inicial timeslot and how many are used.

show interfaces link

show interfaces link [**vlan** *vlan-id*]

Description

Shows interfaces link.

Syntax

Parameter	Description
vlan <i>vlan-id</i>	(Optional) Shows link configuration of a specific vlan. The vlan must be specified in accordance with the vlan configured in the switch. (Range: 1-4094)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, all interfaces link will be shown.

Example

This example illustrates how to show the interfaces link status of the VLAN ID 1.

```
DmSwitch#show interfaces link vlan 1

Speed:    (t-) 10Mbit/s, (h-) 100Mbit/s, (g-) 1Gbit/s, (x-) 10Gbit/s
Duplex:    (-h) Half, (-f) Full
Blocked:   (LF) Link-flap, (LB) Loopback, (UD) Unidirectional, (1X) 802.1X
           (BL) Backup-link, (ST) Spanning-Tree, (EA) EAPS
Config.:   (SD) Shutdown

Unit 1
      2  4  6  8 10 12 14 16 18 20 22 24 26 28
```

hf

1 3 5 7 9 11 13 15 17 19 21 23 25 27

DmSwitch#

Related Commands

Command	Description
show interfaces status	Shows interface configuration status.
show hardware-status transceivers presence	Shows the hardware status transceivers presence.

show interfaces local-tunnel [\[1\]](#) [\[3\]](#) [\[5\]](#)

```
show interfaces local-tunnel
```

Description

Shows the local tunnel interfaces information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command shows all local tunnel interfaces information.

Example

This example illustrates how to show the local tunnel interfaces.

```
DmSwitch#show interfaces local-tunnel
Local-tunnel endpoint    Adm/Oper
  Ltn E1                  Up/Up
  Ltn E2                  Up/Up

DmSwitch#
```

Related Commands

Command	Description
<code>interface local-tunnel</code>	Enables the local tunnel interface configuration mode.

show interfaces loopback

show interfaces loopback [*loopback-number*]

Description

Shows the interfaces loopback information.

Syntax

Parameter	Description
<i>loopback-number</i>	(Optional) Loopback interface number. (Range: 0-7)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
6.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, all loopbacks will be shown.

Example

This example illustrates how to show the interfaces loopback number 0.

```
DmSwitch#show interfaces loopback 0
  Loopback 0:      Up
  IP address:      192.168.111.30/32
  MPLS:            Enable

DmSwitch#
```

Related Commands

Command	Description
<code>interface loopback</code>	Enables the interface loopback configuration mode.
<code>mpls enable</code>	Enables MPLS on the specified loopback interface.

show interfaces ptp

```
show interfaces ptp { all | [ unit-number/ ] ptp-id | range { [ first-unit-number/ ] first-  
ptp-id [ last-unit-number/ ] last-ptp-id } }
```

Description

Show information about pseudo wire interfaces.

Syntax

Parameter	Description
all	Display information about all ptp interfaces.
[unit-number/] ptp-id	unit (optional) and ptp interface index. (Range:1-1/1-16)
range { [first-unit-number/] first-ptp-id [last-unit-number/] last-ptp-id }	Range of ptp interfaces.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display information about ptp interface 1 of unit 1.

```
DM4000#show interfaces ptp 1/1  
DM4000#show interfaces ptp 1/1  
PTP unit 1 Global Configuration:  
  Operation Mode:          ordinary master  
  Domain id:              0  
  Enable:                 no  
  
PTP 1/1 Interface:
```

```

Configuration:
  Role: master

  Source IP Address: -
  Destination IP Address: -
  IP Next Hop: -
  VLAN: 1
    Priority 0
  Announce Rate: 1 pkts/s
  Delay Request Rate: 16 pkts/s
  Sync Rate: 64 pkts/s
  Name: abc
  Enable: no

DM4000#

```

Related Commands

Command	Description
announce-rate	Defines a value for announce messages rate
delay-req-rate	Defines a value for slave request rate
destination-ip-address	Defines destination ip address.
ip-next-hop	Defines the ip address of the next network hop.
name	Naming ptp interface.
source-ip-address	Defines ptp source ip address
sync-rate	Defines a value for synchronization rate
vlan	Defines which vlan current ptp interface use.

show interfaces sdh

```
show interfaces sdh { all | range { [ first-unit-number/ ] first-sdh-id [ last-unit-number/ ] last-sdh-id } | [ unit-number/ ] sdh-id [ vc4 vc4-id { vc12 vc12-klm ] ] }
```

Description

Show information about SDH interfaces.

Syntax

Parameter	Description
all	Display information about all sdh interfaces.
range { [first-unit-number/] first-sdh-id [last-unit-number/] last-sdh-id	Range of sdh interfaces.
[unit-number/] sdh-id	Unit (optional) and sdh interface index. (Range:1-1/1-4)
vc4 vc4-id	Shows VC4 information.
vc12 vc12-klm	Shows VC12 information.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to display information about SDH interface 1 of unit 1.

```
DmSwitch#show interfaces sdh 1
SDH 1/1 Interface:
Configuration:
  Enable:                Yes
  Hierarchy:              STM-1
```

```
Path-trace (J0):
  Evaluation:           Disabled
  Type:                String
  Tx string:           -
  Tx byte:             0
  Rx string:           -
  Rx byte:             0

Tests:
  Laser force on:       Disabled
  Laser force off:      Enabled
  Backend loop:         Disabled
  Front loop:           Enabled
```

Related Commands

Command	Description
test	Configures tests for the sdh interface
show sdh-map	Show the mappings of SDH interfaces.

show interfaces status

```
show interfaces status [ ethernet [ unit-number/ ] port-number ] | port-channel
channel-group-number | bundle { all | range [ first-unit-number/ ] first-port-number [ last-
unit-number/ ] last-port-number | [ unit-number/ ] bundle-id } | g704 { all | range [ first-unit-
number/ ] first-port-number [ last-unit-number/ ] last-port-number | [ unit-number/ ] g704-id } | ptp
{ all | range [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number | [
unit-number/ ] ptp-id }
```

Description

Shows interface configuration status.

Syntax

Parameter	Description
ethernet [unit-number/] port-number	(Optional) Shows configuration status of a specific unit and port. (Range:1-1/1-28)
port-channel channel-group-number	(Optional) Shows configuration status of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
bundle all	(Optional) Shows description of all bundle interfaces.
bundle range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	(Optional) Shows description for a specific range of units and ports.
bundle [unit-number/] bundle-id	(Optional) Status of the specified Bundle interface. (Range:1-1/1-256)
g704 all	(Optional) Shows description of all g704 interfaces.
g704 range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	(Optional) Shows description for a specific range of units and ports.
g704 [unit-number/] g704-id	(Optional) Status of the specified G704 interface. (Range:1-1/1-32)
ptp all	(Optional) Shows description of all PTP interfaces.
ptp range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	(Optional) Shows description for a specific range of units and ports.
ptp [unit-number/] ptp-id	(Optional) Status of the specified ptp interface. (Range:1-1/1-16)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
6.1	Ports range representation removed and added identification of enabled/disabled port-channel ports.
13.2	Added bundle, g704 and ptp interfaces status.

Usage Guidelines

Entering this command without parameters, all interfaces status will be shown.

Example

This example illustrates how to show the status configuration of a specific port.

```
DmSwitch#show interfaces status ethernet 5
Information of Eth 1/5
Basic information:
  Port type:          100TX
  MAC address:        00:04:DF:00:0C:6F
Configuration:
  Name:
  Port admin:         Up
  Speed-duplex:        Auto
  Capabilities:        10M half, 10M full, 100M half, 100M full
  Flow-control:        Disabled
  MDIX:               Auto
  LACP:               Disabled
Current status:
  Link status:         Down
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Output modifiers are available for this command.
capabilities	Configures interface port capabilities for autonegotiation.
flowcontrol	Configures Flow Control for Ethernet interfaces.
negotiation	Controls autonegotiation status for an Ethernet interface.
rate-limit	Configures rate-limits for Ethernet interfaces.
show interfaces table configuration	Shows interface's configuration table.

Command	Description
shutdown (Interface configuration)	Disables an Ethernet interface.
speed-duplex	Configures speed and duplex operation.

show interfaces switchport

show interfaces switchport [**ethernet** [*unit-number/*] *port-number*] | [**port-channel** *channel-group-number*]

Description

Shows switchport information.

Output modifiers are available for this command.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Shows switchport information of a specific unit and port.
port-channel <i>channel-group-number</i>	(Optional) Shows switchport information of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-32)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Entering this command without parameters, all interfaces switchport will be shown.

Example

This example illustrates how to show the switchport information of a specific port.

```
DmSwitch#show interfaces switchport ethernet 1
Information of Eth 1/1
Broadcast threshold:          Enabled, 500 packets/second
```

```

Multicast threshold:      Enabled, 500 packets/second
Unknown-unicast threshold: Enabled, 500 packets/second
MTU:                      9198 bytes
Ingress rate limit:      Disabled
Egress rate limit:       Disabled
Ingress Rule:            Disabled
Acceptable frame type:   All frames
Native VLAN:             1
Priority for untagged traffic: 0
GVRP status:             Disabled
Protocol VLAN:
Allowed VLAN:             1(s,u)
Forbidden VLAN:
QinQ mode:               External
TPID:                    0x8100
MAC addresses maximum:   Disabled
BPDU-block:              Disabled
BPDU-protect:            Disabled
    Limit: 30
    Block-time: 10
    Mode: Block all
DmSwitch#

```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
switchport acceptable frame types	Configures the type of frames accepted by the switch.
switchport egress block ethernet	Configures the switch to block traffic from a specified Ethernet interface to another.
switchport ingress-filtering	Enables ingress filtering
switchport mtu	Configures maximum transmission unit.
switchport qinq	Configures Double Tagging mode.
switchport storm-control	Configures packet storm control.
switchport tpid	Configures Tag Protocol ID for an interface.
switchport bpdu-protect	Protect BPDU configuration for an interface.

show interfaces table bundle

```
show interfaces table bundle { counters | status }
```

Description

Shows Bundle interface counters or status table.

Syntax

Parameter	Description
counters	Shows all enabled bundle interface counters as a table.
status	Shows all enabled bundle interfaces status as a table.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

This command displays same content as **show interfaces { counters | status } bundle** in table format, for all enabled bundles.

Example

```
DmSwitch#show interfaces table bundle status
```

Bundle	Local Bundle	Remote Bundle	TDM Local	TDM Remote	Packet Size	Next Hop	MAC
1/ 1	Ok	Ok	--	Fail	Ok	Ok	00:04:DF:62:86:A7

```
DmSwitch#show interfaces table bundle counters
```

Bundle	Buffer Overflow	Buffer Underflow	Lost Packets	Lost Packets Rate	Unexpect Seq. Num accepted	Unexpect Seq. Num dropped	Wrong Size Packets	Jitter Buffer Occup.
--------	-----------------	------------------	--------------	-------------------	----------------------------	---------------------------	--------------------	----------------------

```
-----  
1/ 1      0      2      11140      0      0      5      0      3  
  
DmSwitch#
```

Related Commands

Command	Description
show interfaces counters bundle	Shows the interface counters information.
show interfaces status bundle	Shows interface configuration status.

show interfaces table configuration

show interfaces table configuration [unit {*unit-number*}]

Description

Shows interface configuration table.

Syntax

No parameter accepted.

Parameter	Description
<i>unit-number</i>	(Optional) Shows the interfaces only from a specified unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.2	Filter results by unit was introduced.

Usage Guidelines

With this show command, you can see the status of ports, links, ports speed, flow control and ports default VLAN.

Example

This example illustrates how to show the interface configuration table.

```
DmSwitch#show interfaces table configuration
Port      Port   Link   Auto   Speed   Duplex   Flow   Pvid
          State Status Neg    Cfg    Actual  Cfg    Actual Ctrl
=====
1/1        ENABLE UP     ON     100    100     AUTO   FULL   NONE   1
1/2        ENABLE DOWN  ON     100    100     AUTO   HALF   NONE   1
1/3        ENABLE DOWN  ON     100    100     AUTO   HALF   NONE   1
```

```

1/4          ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/5          ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/6          ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/7          ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/8          ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/9          ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/10         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/11         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/12         ENABLE  UP    ON    100    100    AUTO  FULL  NONE  1
1/13         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/14         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/15         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/16         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/17         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/18         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/19         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/20         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/21         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/22         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/23         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/24         ENABLE  DOWN  ON    100          AUTO  HALF  NONE  1
1/25         ENABLE  DOWN  ON    100          AUTO  FULL  NONE  1
1/26         ENABLE  DOWN  ON    100          AUTO  FULL  NONE  1
1/27         ENABLE  DOWN  ON    100          AUTO  FULL  NONE  1
1/28         ENABLE  DOWN  ON    100          AUTO  FULL  NONE  1
=====
                                spacebar->toggle screen  ESC->exit
DmSwitch#

```

Related Commands

Command	Description
capabilities	Configures interface port capabilities for autonegotiation.
flowcontrol	Configures Flow Control for Ethernet interfaces.
negotiation	Controls autonegotiation status for an Ethernet interface.
rate-limit	Configures rate-limits for Ethernet interfaces.
show interfaces status	Shows interface configuration status.
shutdown (Interface configuration)	Disables an Ethernet interface.
speed-duplex	Configures speed and duplex operation.

show interfaces table counter

```
show interfaces table counter { total | type | error } [unit {unit-number} ]
```

Description

Shows interface counters table.

Syntax

Parameter	Description
total	Shows the interface counter table for total packets.
type	Shows the interface counter table by packets types.
error	Shows the interface counter table for error packets.
<i>unit-number</i>	(Optional) Shows the interfaces only from a specified unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.2	Filter results by unit was introduced.

Usage Guidelines

With this show command, you can see the transmitted and received packets and bytes, the transmitted and received discarded packets, the unicast, multicast and broadcast transmitted and received packets, the undersized and oversized packets, collisions and other counters.

Example

This example illustrates how to show the interface counter table for all packets.

```
DmSwitch#show interfaces table counter total
Port          Tx Pkt    Tx Byte   Rx Pkt    Rx Byte   Tx          Rx
              Count      Count     Count     Count     Discards    Discards
=====
```

```
1/1      38942      24308680      28163      4256626      0      3
1/2      6         432         0         0         0         0
1/3      6         432         0         0         0         0
1/4      6         432         0         0         0         0
1/5      6         432         0         0         0         0
1/6      6         432         0         0         0         0
1/7      6         432         0         0         0         0
1/8      6         432         0         0         0         0
1/9      6         432         0         0         0         0
1/10     6         432         0         0         0         0
1/11     6         432         0         0         0         0
1/12     30818     4753855     176036     34294571     0         107
1/13     6         432         0         0         0         0
1/14     6         432         0         0         0         0
1/15     6         432         0         0         0         0
1/16     6         432         0         0         0         0
1/17     6         432         0         0         0         0
1/18     6         432         0         0         0         0
1/19     6         432         0         0         0         0
1/20     6         432         0         0         0         0
1/21     6         432         0         0         0         0
1/22     6         432         0         0         0         0
1/23     6         432         0         0         0         0
1/24     6         432         0         0         0         0
1/25     6         432         0         0         0         0
1/26     6         432         0         0         0         0
1/27     6         432         0         0         0         0
1/28     3606      925654      2316      299384      0         0
=====
spacebar->toggle screen  ESC->exit
DmSwitch#
```

Related Commands

Command	Description
clear interface counters	Clear interface counters.
clear counter	Clears filter counters.

show interfaces table queue-l2

```
show interfaces table queue-l2 { ethernet [ unit-number/ ] port-number |  
port-channel channel-group-number }
```

Description

Shows counters of all queues for a specific interface. It has two different views, one shows values as rates or accumulative values, and the other shows values in percentage relative to the Interface's bandwidth.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	The Ethernet Interface to display queues' counters.
port-channel <i>channel-group-number</i>	The Port-channel Interface to display queues' counters. The port-channel must be specified in accordance with the port-channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
5.0	This command was introduced.
13.0	The information shown was changed. Parameters were changed.

Usage Guidelines

With this command, you can see several information for all queues of a specific Interface, such as the configured minimum and maximum bandwidth for a queue, the current output (tx) and dropped rates, the accumulative value of bytes dropped - since the start of the show, and the average output (tx) rate. The same information can be shown as a percentage value relative to the Interface's Bandwidth. To change between the two views, press *spacebar*.

NOTE: The device will not take into account 20 bytes of Ethernet Overhead (Ethernet's Preamble, Start-of-frame delimiter (SFD) and Inter-Frame Gap (IFG) bits). As a result of this, the values shown by this command, as well as the values used to shape the traffic, will be smaller than the values that are actually being sent on wire.

Example

This example illustrates how to show the queue counters of a specific port.

```
DmSwitch#show interfaces table queue-l2 ethernet 20
Interface Queue Information
```

Port 1/20:

Q	MIN (bps)	MAX (bps)	OUT (bps)	DRP (bps)	TOT DRP (Bytes)	AVG OUT(bps)
0	1.00 G	448.00 k	415.38 k	512.37 M	24.86 G	418.82 k
1	128.00 k	384.00 k	346.15 k	0.00	322.78 M	366.32 k
2	128.00 k	128.00 k	69.23 k	128.35 M	5.68 G	100.97 k
3	128.00 k	128.00 k	69.23 k	29.63 M	33.98 G	100.97 k
4	128.00 k	64.00 k	0.00	0.00	0.00	274.00
5	256.00 k	64.00 k	0.00	18.62 M	5.62 G	32.32 k
6	64.00 k	64.00 k	0.00	56.28 M	17.30 G	32.32 k
7	64.00 k	2.05 M	2.08 M	0.00	3.43 G	2.06 M

Caption:

TOT DRP: Total dropped bytes accumulated since the show began.
spacebar->toggle screen ESC->exit

DmSwitch#

This example illustrates the percentage-relative-to-link view.

```
DmSwitch#show interfaces table queue-l2 ethernet 20
Interface Queue Information
```

Port 1/20:

Q	MIN (bps)	MAX (bps)	OUT (bps)	DRP (bps)	TOT DRP (Bytes)	AVG OUT(bps)
0	100.0000 %	0.0448 %	0.0415 %	50.1708 %	--	0.0429 %
1	0.0128 %	0.0384 %	0.0346 %	0.0000 %	--	0.0369 %
2	0.0128 %	0.0128 %	0.0069 %	12.8403 %	--	0.0093 %
3	0.0128 %	0.0128 %	0.0069 %	2.9626 %	--	0.0093 %
4	0.0128 %	0.0064 %	0.0000 %	0.0000 %	--	0.0017 %
5	0.0256 %	0.0064 %	0.0000 %	2.1735 %	--	0.0032 %
6	0.0064 %	0.0064 %	0.0000 %	3.2810 %	--	0.0032 %
7	0.0064 %	0.2048 %	0.2008 %	0.0000 %	--	0.2029 %

Caption:

TOT DRP: Not valid for this view.
spacebar->toggle screen ESC->exit

DmSwitch#

Related Commands

Command	Description
show queue config	Shows queue configuration per port
clear interface queue-counters	Clear interface queue-counters.

show interfaces table utilization

```
show interfaces table utilization { packets | octets | bandwidth } [unit {unit-number} ]
```

Description

Shows the interface average utilization table.

Syntax

Parameter	Description
packets	Shows the interface utilization average table by packets per second.
octets	Shows the interface utilization average table by octets per second.
bandwidth	Shows the interface utilization average table by percentage of bandwidth.
<i>unit-number</i>	(Optional) Shows the interfaces only from a specified unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.2	Filter results by unit was introduced.

Usage Guidelines

With this show command, you can see the link status, the average and peak of transmitted and received packets per second, the average and peak of transmitted and received bytes per second, the average and peak of bandwidth utilization percentage in the data transmission and reception and the link speed.

Example

This example illustrates how to show the interface utilization average table by bytes per second.

```

DmSwitch#show interfaces table utilization bytes
Port          Link      Receive      Peak Rx      Transmit      Peak Tx
              Status    bytes/sec    bytes/sec    bytes/sec     bytes/sec
=====
1/1            UP        0            0            0            0
1/2            DOWN      0            0            0            0
1/3            DOWN      0            0            0            0
1/4            DOWN      0            0            0            0
1/5            DOWN      0            0            0            0
1/6            DOWN      0            0            0            0
1/7            DOWN      0            0            0            0
1/8            DOWN      0            0            0            0
1/9            DOWN      0            0            0            0
1/10           DOWN      0            0            0            0
1/11           DOWN      0            0            0            0
1/12           UP        73           145          960          2823
1/13           DOWN      0            0            0            0
1/14           DOWN      0            0            0            0
1/15           DOWN      0            0            0            0
1/16           DOWN      0            0            0            0
1/17           DOWN      0            0            0            0
1/18           DOWN      0            0            0            0
1/19           DOWN      0            0            0            0
1/20           DOWN      0            0            0            0
1/21           DOWN      0            0            0            0
1/22           DOWN      0            0            0            0
1/23           DOWN      0            0            0            0
1/24           DOWN      0            0            0            0
1/25           DOWN      0            0            0            0
1/26           DOWN      0            0            0            0
1/27           DOWN      0            0            0            0
1/28           DOWN      0            0            0            0
=====
spacebar->toggle screen  ESC->exit
DmSwitch#

```

Related Commands

No related command.

show interfaces test bundle

```
show interfaces test bundle { all | [ unit-number/ ] bundle-id }
```

Description

Show status of tests on bundle interface.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>bundle-id</i>	Unit number/Bundle interface number.
[<i>all</i>]	Show the bert test results of all bundles in the equipment.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows active tests on interface bundle 1.

```
DM4000#show interfaces test bundle 1
Information of Bundle Interface 1/1
Ethernet Bert test:      Disabled
TDM Bert test:          Disabled
Loop test:              Disabled

DM4000#
```

Related Commands

Command	Description
<code>g704 test</code>	Starts ldl test on g704 interface
<code>clear interface test</code>	Clear interface test.

show interfaces test sdh

show interfaces test sdh [*unit-number/*] *sdh-id*

Description

Show status of tests on a SDH interface.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>sdh-id</i>	Unit number/SDH interface number.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows active tests on interface bundle 1.

```
DM4000(config)#show interfaces test sdh 1
Information of SDH Interface 1/1
Laser force on:           Disabled
Laser force off:          Disabled
Backend loop:             Enabled
Front loop:               Disabled
DM4000(config)#
```

Related Commands

Command	Description
<code>test</code>	Configures tests for the sdh interface

show dump

show dump

Description

Shows the files stored in the dumps directory.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

This command shows the dump file(s) stored in the DmSwitch.

Example

This example illustrates how to show the dump file(s).

```
DmSwitch#show dump
Dump file                               Size          Date
-----
dump_1970_Jan_01_00:03:39.txt           1189          Thu Jan  1 00:03:42 1970
dump_1970_Jan_01_00:06:10.txt           1485          Thu Jan  1 00:06:13 1970
dump_1970_Jan_01_00:03:44.txt          11422          Thu Jan  1 00:03:50 1970
dump_2014_Mar_14_15:26:52.txt           7837          Fri Mar 14 15:26:55 2014

Total:                                21933

DmSwitch#
```

Related Commands

Command	Description
<code>dump</code>	Generate an dump file.
<code>copy</code>	Copies configuration and firmware.
<code>clear dump</code>	Clears dump files.

show ip

show ip

Description

Shows the IP configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the routing status, VLANs IP, default gateway, DNS server and SSH, HTTP, Telnet and SNMP configurations.

Example

This example illustrates how to show the IP configurations.

```
DmSwitch#show ip
IP routing is disabled

VLAN 1  10.11.12.21/24
VLAN 2  10.11.13.21/24

Default gateway: 10.11.12.13

DNS servers: 10.11.12.14 10.11.12.15

SSH Enabled
  Legacy support:      Disabled
  Timeout:             120
  Fingerprints:
    DSA: SHA256:stWKvv/4AG/EgE0xAA1Eneyce/ktqJtGqLUblQsJN1A
    RSA: SHA256:X2SpI5f1VvFNoDV3plwaaMBVIawB6seQHzc4u0+l0bo
  SSH connections limit: 8
```

```

HTTP:
  HTTP status:  Enable
  HTTP port:    80

secure HTTP:
  HTTPS status: Enable
  HTTPS port:   443

HTTP/HTTPS connections limit: 8

Telnet status:          Enable
Telnet connections limit: 8

SNMP status: Enable

SNMP Community:
  public(Read-Only)

Trap Manager:
  IP          COMMUNITY      VERSION
  10.1.1.10   management     2c

DmSwitch#

```

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
ip default-gateway	Configures the default gateway for DmSwitch.
ip dns-server	Configures the DNS servers used by DmSwitch
ip http	Configures the internal HTTP server for external access.
ip routing	Enables the IP routing.
ip snmp-server	Configures the internal SNMP server.
ip ssh	Configures the internal SSH server for external access.
ip telnet	Configures the internal Telnet server for external access.

show ip bfd neighbors

show ip bfd neighbors

Description

Shows the state of all BFD IPv4 sessions.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

This command shows all BFD IPv4 sessions, their current state and the interface by which they are established (if known).

Example

This example illustrates how to show BFD neighbors.

```
DmSwitch#show ip bfd neighbors
```

Local Addr	Remote Addr	State	Interface
10.10.1.1	10.10.1.2	Up	---

```
DmSwitch#
```

Related Commands

Command	Description
bfd interval	Configure BFD interval parameters on a VLAN.

Command	Description
<code>neighbor bfd interval</code>	Configure BFD interval parameters for a BGP neighbor.
<code>neighbor bfd enable</code>	Configure BFD interval parameters for a BGP neighbor.
<code>ip ospf bfd</code>	Configures BFD support for OSPF on a VLAN.
<code>ip route</code>	Adds a static route to the routing table.

show ipv6 bfd neighbors

show ipv6 bfd neighbors

Description

Shows the state of all BFD IPv6 sessions.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

This command shows all BFD IPv6 sessions, their current state and the interface by which they are established (if known).

Example

This example illustrates how to show BFD neighbors.

```
DmSwitch#show ipv6 bfd neighbors
```

Local Addr	Remote Addr	State	Interface
2001::1:1	2001::1:2	Up	---

DmSwitch#

Related Commands

Command	Description
bfd interval	Configure BFD interval parameters on a VLAN.

Command	Description
<code>neighbor bfd interval</code>	Configure BFD interval parameters for a BGP neighbor.
<code>neighbor bfd enable</code>	Configure BFD interval parameters for a BGP neighbor.
<code>ipv6 ospfv3 bfd</code>	Configure BFD support for OSPFv3 on a VLAN.
<code>ipv6 route</code>	Adds an IPv6 static route to the routing table.

show ip bgp

```
show ip bgp[ dampening { parameters | flap-statistics } | dampened-paths |  
labels [ cross-connections ] | neighbors [ ip-address [ advertised-routes |  
received-routes ] ] | peer-group [ name ] | summary | vpnv4 { all [ labels ] | rd  
AS-number/ip-address } | vrf [ vrf-name ] ]
```

Description

Displays entries in the BGP database. The output can be filtered to display specific properties.

Syntax

Parameter	Description
dampening { parameters flap-statistics }	(Optional) Display BGP Dampening information.
dampened-paths	(Optional) Display BGP Dampened path table.
labels [1] [3] [5]	(Optional) Display the labels BGP had received and distributed.
cross-conections [1] [3] [5]	(Optional) Display only cross-conected labels.
neighbors <i>ip address</i>	(Optional) Detailed information on TCP and BGP neighbor connections.
advertised-routes received-routes	(Optional) Either advertised or received routes of one specific neighbor can be shown.
peer-group	Detailed information on all peer groups and BGP neighbors belonging to the groups.
peer-group <i>name</i>	Detailed information on peer group <i>name</i> and BGP neighbors belonging to this specific group.
summary	(Optional) Summary of BGP neighbor status.
vpnv4 [1] [3] [5]	(Optional) Shows BGP VPNv4 routes.
all	(Optional) Filter to show BGP VPNv4 routes for all router-distinguishers.
rd { <i>AS:number</i> <i>ip-address:number</i> }	(Optional) Filter to show BGP VPNv4 routes for a specific router-distinguisher.
labels	(Optional) Displays exchanged label informations for BGP VPNv4 routes.
vrf <i>vrf-name</i>	(Optional) Show BGP IPv4 routes for a specific VRF table.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.
10.0	New filters vpnv4 and vrf added.
11.2	New filters dampening and dampened-paths added.
12.4	New filter labels added.
12.2	Peer group commands added.

Usage Guidelines

Entering this command without parameters, the unfiltered BGP information will be shown. Any additional parameter is used to display a specific information (labelbs, dampened routes, etc) or to filter the complete information to be displayed.

Examples

This example illustrates how to show the basic BGP information (without any filter).

```
DmSwitch#show ip bgp
BGP Routing with Router ID: 100.100.1.10
Admin status: up, Operational status: up
Local AS number: 10
Displaying IPv4 routes:
  Status codes: d damped, * valid, > best
  Origin codes: i IGP, e EGP, ? incomplete

  Network          Next Hop        Metric      LocPrf      Weight      Path
  -----
Total number of prefixes 0

DmSwitch#
```

This example illustrates how to show the information concerning a BGP neighbor.

```
DmSwitch#show ip bgp neighbors
BGP neighbor is 172.16.88.130, remote AS 10, local AS 10, internal link
  BGP Version 4, remote router ID 100.100.1.10
  BGP state = established, up for 16:30:24
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Advertise interval is 30 seconds
Neighbor capabilities:
  BGP-4 Multiprotocol Extensions: received
  BGP-4 Route refresh: received
  Graceful Restart: received
  Route Refresh: received
  Address family IPv4 NLRI-unicast: advertised and received
  Address family IPv6 NLRI-unicast: advertised
  Address family IPv4 MPLS-labeled-VPN: advertised and received
  Address family IPv4 NLRI-MPLS-Label: advertised and received
  Address family NSAP NLRI-unicast: received
Message Statistics:
  Received 7716 messages, 0 update messages
  Sent 7771 messages, 0 update messages
```

```

Minimum time between advertisement runs is 30 seconds
Number of connection retries: 7275
For address family: IPv4 Unicast
  Prefix received 0 (accepted 0, rejected 0)
  Prefix advertised 0
For address family: IPv4 VPN
  Prefix received 0 (accepted 0, rejected 0)
  Prefix advertised 0
For address family: IPv4 Label
  Prefix received 0 (accepted 0, rejected 0)
  Prefix advertised 0

```

DmSwitch#

This example illustrates how to show the labels information BGP has.

DmSwitch#show ip bgp labels

DmSwitch#show ip bgp labels

Number of Entries: 12

Network	Next hop	Incoming Label/ Protocol	Outgoing Label/ Protocol
100.100.100.1/32	172.16.78.1	17/BGP	ImpNull/LDP
100.100.100.1/32	172.16.78.1	24/LDP	ImpNull/LDP
100.100.100.2/32	-	16/BGP	-
100.100.100.3/32	172.16.78.9	25/LDP	ImpNull/BGP
100.100.100.4/32	172.16.78.9	26/LDP	19/BGP
100.100.100.70/32	172.16.78.1	18/BGP	ImpNull/LDP
100.100.100.70/32	172.16.78.1	27/LDP	ImpNull/LDP
172.16.78.0/29	-	19/LDP	-
172.16.78.8/31	-	22/LDP	-
172.16.78.16/29	172.16.78.9	20/LDP	ImpNull/BGP
172.16.79.0/29	-	21/LDP	-
172.16.79.8/31	-	23/LDP	-

DmSwitch#

This example illustrates how to show only the cross connections informations BGP has.

DmSwitch#show ip bgp labels cross-connections

DmSwitch#

DmSwitch#show ip bgp labels cross-connections

Number of Entries: 5

Network	Next hop	Incoming Label/ Protocol	Outgoing Label/ Protocol
100.100.100.1/32	172.16.78.1	17/BGP	ImpNull/LDP
100.100.100.3/32	172.16.78.9	25/LDP	ImpNull/BGP
100.100.100.4/32	172.16.78.9	26/LDP	19/BGP
100.100.100.70/32	172.16.78.1	18/BGP	ImpNull/LDP
172.16.78.16/29	172.16.78.9	20/LDP	ImpNull/BGP

DmSwitch#

The following 4 examples show all possible information concerning BGP-dampening feature.

This example illustrates how to show BGP-dampening information of routes advertised by eBGP peer in AS 50:

```
DmSwitch(config-router-bgp)#show ip bgp
BGP Routing with Router ID: 100.100.1.10
Admin status: up, Operational status: up
Local AS number: 100
Displaying IPv4 routes:
  Status codes: d damped, h history, * valid, > best
  Origin codes: i IGP, e EGP, ? incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 100.100.100.13/32	172.10.90.2	0	100	0 150 i	
*> 172.10.80.0/24	172.10.90.2	0	100	0 150 i	
* 172.10.90.0/24	172.10.90.2	0	100	0 150 i	
*> 172.10.95.0/24	172.10.90.2	0	100	0 150 i	
*> 172.10.200.0/24	172.10.90.2	0	100	0 150 i	
*> 172.10.201.0/24	172.10.90.2	0	100	0 150 i	
*> 172.10.202.0/24	172.10.90.2	0	100	0 150 i	
* d 100.100.100.40/32	172.10.100.1	0	100	0 50 i	
* d 172.10.80.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.95.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.100.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.101.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.102.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.103.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.104.0/24	172.10.100.1	0	100	0 50 i	
* d 172.10.110.0/31	172.10.100.1	0	100	0 50 i	

Below, only dampened paths are shown:

```
DmSwitch(config-router-bgp)#show ip bgp dampened-paths
BGP Routing with Router ID: 100.100.100.12
Admin status: up, Operational status: up
Local AS number: 100
Displaying IPv4 routes:
  Status codes: d damped, h history, * valid, > best
  Origin codes: i IGP, e EGP, ? incomplete
```

Network	Next Hop	Time Left	Path
* d 100.100.100.40/32	172.10.100.1	00:02:41	50 i
* d 172.10.80.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.95.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.100.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.101.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.102.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.103.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.104.0/24	172.10.100.1	00:02:41	50 i
* d 172.10.110.0/31	172.10.100.1	00:02:41	50 i

Total number of prefixes 9

How to show the configured BGP-dampening parameters:

```
DmSwitch(config-router-bgp)#show ip bgp dampening parameters
BGP Dampening Configuration
```

```
Half-life      : 300 secs (default)
Reuse         : 50 (default)
Suppress      : 200
Max-suppress-time : 900 secs (default)
Route-map names : damp.
```

Below, example of BGP-dampening flap-statistics:

```
DmSwitch(config-router-bgp)#show ip bgp dampening flap-statistics
BGP Routing with Router ID: 100.100.100.12
Admin status: up, Operational status: up
Local AS number: 100
Displaying IPv4 routes:
  Status codes: d damped, h history, * valid, > best
  Origin codes: i IGP, e EGP, ? incomplete
```

Network	Next Hop	Penalty	Flap Cnt	Time Left	Path
* d 100.100.100.40/32	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.80.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.95.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.100.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.101.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.102.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.103.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.104.0/24	172.10.100.1	67	4	00:02:19	50 i
* d 172.10.110.0/31	172.10.100.1	67	4	00:02:19	50 i

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show ip route vrf	Shows the RIB of the specified VRF.

show ip bgp community

```
show ip bgp community { aa:nn | internet | local-AS | no-advertise | no-export  
[exact-match] }
```

Description

Displays routes that belong to specified BGP communities.

Output modifiers are available for this command.

Syntax

Parameter	Description
<i>aa:nn</i>	Community number in aa:nn format.
internet	Internet (well-known community).
local-AS	Do not send outside local AS (well-known community).
no-advertise	Do not advertise to any peer (well-known community).
no-export	Do not export to next AS (well-known community).
exact-match	(Optional) Only routes that contain the same specified communities.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Entering this command only the routes that belong to specified BGP communities will be displayed.

Up to 16 communities can be used as input in the command.

The use of optional parameter **exact-match** will filter the routes that contain the entire set of communities entered in the command.

Examples

This example illustrates how to show the routes that belong to BGP community **internet**.

```
DmSwitch#show ip bgp community internet
BGP Routing with Router ID: 2.0.0.0
Admin status: up, Operational status: up
Local AS number: 65001
Displaying IPv4 routes:
  Status codes: s suppressed, d damped, h history, * valid, > best
  Origin codes: i IGP, e EGP, ? incomplete
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	10.10.10.0/24	10.10.10.2	0	100	0 65000	i
*>	20.20.20.0/24	10.10.10.2	0	100	0 65000	i
*>	60.60.60.0/28	10.10.10.2	0	100	0 65000	i
*>	100.100.100.12/32	10.10.10.2	0	100	0 65000	i
*>	13.13.13.0/28	20.20.20.3	0	100	0 1001	?
*>	13.13.13.16/28	20.20.20.3	0	100	0 1001	?
*>	13.13.13.32/28	20.20.20.3	0	100	0 1001	?
*>	13.13.13.48/28	20.20.20.3	0	100	0 1001	?
*>	13.13.13.64/28	20.20.20.3	0	100	0 1001	?

```
Total number of prefixes 9
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
router bgp	Enables and accesses the BGP configuration.
route-map	Create route-map or enter route-map command mode.
match community	Matches community values from routing table.
set community	Sets community values in destination routing protocol.

show ipv6 bgp

```
show ipv6 bgp [ dampening { parameters | flap-statistics } | dampened-paths |  
neighbors [ ipv6-address [ advertised-routes | received-routes ] ] | summary ]
```

Description

Displays entries in the BGP routing table.

Syntax

Parameter	Description
dampening { parameters flap-statistics }	(Optional) Display BGP Dampening information.
dampened-paths	(Optional) Display BGP Dampened path table.
neighbors <i>ipv6 address</i>	(Optional) Detailed information on TCP and BGP neighbor connections.
advertised-routes received-routes	(Optional) Either advertised or received routes of one specific neighbor can be shown.
summary	(Optional) Summary of BGP neighbor status.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command shows BGP information. Filter parameters are required.

Examples

This example illustrates how to show the information concerning to a BGP neighbor.

```
DmSwitch#show ipv6 bgp neighbors
```

```
BGP neighbor is 2001:DB8:1::, remote AS 120, local AS 1200, external link  
BGP Version 4, remote router ID 1.2.0.0
```



```

BGP state = active, never up
Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
Advertise interval is 30 seconds
Message Statistics:
  Received 0 messages, 0 update messages
  Sent 0 messages, 0 update messages
Minimum time between advertisement runs is 30 seconds
Number of connection retries: 5

BGP neighbor is 2001:DB8:2::, remote AS 121, local AS 1200, external link
BGP Version 4, remote router ID 1.2.0.0
BGP state = active, never up
Last read 00:00:19, hold time is 90, keepalive interval is 30 seconds
Advertise interval is 30 seconds
Message Statistics:
  Received 0 messages, 0 update messages
  Sent 0 messages, 0 update messages
Minimum time between advertisement runs is 30 seconds
Number of connection retries: 6

DmSwitch#

```

The following 4 examples show all possible information concerning BGP-dampening feature.

This example illustrates how to show BGP-dampening information of routes advertised by eBGP peer in AS 50:

```

DmSwitch(config-router-bgp)#show ipv6 bgp
BGP Routing with Router ID: 100.100.100.12
Admin status: up, Operational status: up
Local AS number: 100
Displaying IPv6 routes:
  Status codes: s suppressed, d damped, h history, * valid, > best
  Origin codes: i IGP, e EGP, ? incomplete

```

Network	Next Hop	Metric	LocPrf
*> 2001:db8::6464:640d/128	2001:db8::ac0a:5a02	0	10
*> 2001:db8::ac0a:5000/120	2001:db8::ac0a:5a02	0	10
* 2001:db8::ac0a:5a00/120	2001:db8::ac0a:5a02	0	10
*> 2001:db8::ac0a:c800/120	2001:db8::ac0a:5a02	0	10
*> 2001:db8::ac0a:c900/120	2001:db8::ac0a:5a02	0	10
*> 2001:db8::ac0a:ca00/120	2001:db8::ac0a:5a02	0	10
* 2001:db8::ac0a:fa00/120	2001:db8::ac0a:5a02	0	10
* d 2001:d8::ac0a:6400/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::6464:6428/128	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:5000/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:6400/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:6500/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:6600/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:6700/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:6800/120	2001:db8::ac0a:6401	0	10
* d 2001:db8::ac0a:d200/120	2001:db8::ac0a:6401	0	10

Total number of prefixes 14

Below, only dampened paths are shown:

```

DmSwitch(config-router-bgp)#show ipv6 bgp dampened-paths
BGP Routing with Router ID: 100.100.100.12
Admin status: up, Operational status: up
Local AS number: 100

```

Displaying IPv6 routes:

Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i IGP, e EGP, ? incomplete

Network	Next Hop	Time Left	Path
* d 2001:d8::ac0a:6400/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::6464:6428/128	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:5000/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:6400/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:6500/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:6600/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:6700/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:6800/120	2001:db8::ac0a:6401	00:12:01	50 i
* d 2001:db8::ac0a:d200/120	2001:db8::ac0a:6401	00:12:01	50 i

Total number of prefixes 9

How to show the configured BGP-dampening parameters:

DmSwitch(config-router-bgp)#show ipv6 bgp dampening parameters
BGP Dampening Configuration

Half-life : 300 secs (default)
Reuse : 50 (default)
Suppress : 200
Max-suppress-time : 900 secs (default)
Route-map names : damp_ipv6, damp.

Below, example of BGP-dampening flap-statistics:

DmSwitch(config-router-bgp)#show ipv6 bgp dampening flap-statistics
BGP Routing with Router ID: 100.100.100.12
Admin status: up, Operational status: up
Local AS number: 100
Displaying IPv6 routes:
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i IGP, e EGP, ? incomplete

Network	Next Hop	Penalty	Flap Cnt	Tim
* d 2001:d8::ac0a:6400/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::6464:6428/128	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:5000/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:6400/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:6500/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:6600/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:6700/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:6800/120	2001:db8::ac0a:6401	274	3	00:
* d 2001:db8::ac0a:d200/120	2001:db8::ac0a:6401	274	3	00:

Total number of prefixes 9

Related Commands

Command	Description
<code>router bgp</code>	Enables and accesses the BGP configuration.

show ip prefix-list

show ip prefix-list [*prefix-list name*]

Description

Shows configured prefix-lists.

Syntax

Parameter	Description
<i>prefix-list name</i>	(Optional) Shows information only regarding the given prefix-list.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
12.2	The command shows labeled-prefix information in prefix-lists.

Usage Guidelines

Entering this command without parameters all prefix-lists will be showed.

Example

This example illustrates how to show all configured prefix-lists.

```
DmSwitch#show ip prefix-list
-----
ip prefix-list unlabeled_prefix_list:
  seq 10 permit 10.10.10.0/24
-----
ip prefix-list labeled_prefix_list:
  seq 10 permit 10.1.23.0/30 labeled-prefix
  seq 20 permit 10.1.34.0/30 labeled-prefix
  seq 30 permit 10.1.45.0/30 labeled-prefix
-----
ip prefix-list another_prefix_list:
```

```
seq 20 permit 10.20.30.0/24 le 28
DmSwitch#
```

Related Commands

Command	Description
ip prefix-list	Configure a prefix list.

show ip default-gateway

show ip default-gateway

Description

Shows the configured default gateway.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the configured default gateway.

```
DmSwitch#show ip default-gateway
Default gateway: 10.11.12.13
DmSwitch#
```

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
ip default-gateway	Configures the default gateway for DmSwitch.

show ipv6 default-gateway

show ipv6 default-gateway

Description

Shows the configured IPv6 default gateway.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the configured IPv6 default gateway.

```
DmSwitch#show ipv6 default-gateway
Default gateway: 2001:db8::1
DmSwitch#
```

Related Commands

Command	Description
ipv6 address	Sets an IPv6 address for the selected VLAN.
ipv6 default-gateway	Configures the IPv6 default gateway for DmSwitch.

show ip dhcp relay

show ip dhcp relay

Description

Shows the DHCP relay settings.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.1	This command was introduced.
13.2	This command was modified.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCP relay settings.

```
DmSwitch#show ip dhcp relay

Global DHCP settings:
  DHCP relay:           Enabled
  DHCP option 82:       Enabled

DHCP server address:    192.168.0.254

DHCP relay enabled:     Vlan2 to Vlan5

Trusted interfaces:     Vlan2
                       Vlan4 to Vlan5

DmSwitch#
```


Related Commands

Command	Description
<code>ip dhcp relay</code>	Enables DHCP relay globally.
<code>ip dhcp relay</code>	Enables DHCP relay on the selected Vlan.
<code>ip dhcp relay information option</code>	Enables DHCP Agent Information Option (option 82).
<code>ip dhcp relay information trusted</code>	Mark a Vlan as a trusted interface.
<code>ip helper-address</code>	Add an address to the list of DHCP servers global.
<code>ip helper-address</code>	Add an address to the VLAN list of DHCP servers in VLAN.

show ip dhcp server

show ip dhcp server [leases]

Description

Shows the DHCP server global settings and status.

Syntax

Parameter	Description
leases	Shows DHCP server leases database.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCP server settings.

```
DmSwitch#show ip dhcp server
```

```
Server enabled: Yes
```

```
Excluded-addresses table:
```

```
Start address    End address
-----
10.0.0.200
```

```
Fixed-addresses table:
```

```
Hostname          IPv4          Hardware-Address
-----
```

```
pc_hostname                10.0.0.100        00:50:B6:0A:3F:48
DmSwitch#
```

This example illustrates how to show the DHCP server leases database.

```
DmSwitch#show ip dhcp server leases

IP address      Hardware address      Lease expiration
-----
10.0.1.3        00:13:3b:19:0c:10     Jan 01 1970 05:50 AM

DmSwitch#
```

Related Commands

Command	Description
ip dhcp server enable	Enables the DHCP server configuration mode.
excluded-address	Enables the DHCP server globally.
fixed-address	Exclude addresses from DHCP pools.
ip dhcp pool	Define host/ip mappings for DHCP pools.
network	Enables the DHCP pool configuration mode.
default-router	Configure the prefix/mask for the DHCP pool.
dns-server	Configure default routers for the DHCP pool.
netbios-name-server	Configure DNS servers for the DHCP pool.
netbios-node-type	Configure NetBios name servers for the DHCP pool.
domain-name	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
lease	Configure the domain name option (RFC 2132) for the DHCP pool.
deny-unknown-clients	Configure the maximum lease time for this DHCP pool.
show ip dhcp server	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp pool	Shows the DHCP server settings and status.
clear ip dhcp server	Shows the DHCP pool settings.
	Clear DHCP server leases database.

show ip dhcp pool

show ip dhcp pool [*name*]

Description

Shows the DHCP pool settings.

Syntax

Parameter	Description
<i>name</i>	Shows configuration for a specific pool.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCP pools settings.

```
DmSwitch#show ip dhcp pool

Pools table:

Pool name          Network
-----
local              10.0.0.0/24
relay              10.0.1.0/24
teste
DmSwitch#
```

This example illustrates how to show the DHCP pools settings for a specific pool.

```
DmSwitch#show ip dhcp pool local
relay
  Network: 10.0.1.0/24
  DNS Servers: 8.8.8.8
  Default Routers: 10.0.1.1
  NetBIOS Name Servers: 192.168.0.1
  NetBIOS Node Type: H-node: Hybrid - WINS, then broadcast
  Domain Name: relay.datacom.net
  Lease Time: 00d 00h 01m
  Unknown Clients: Allow

DmSwitch#
```

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

show ipv6 dhcp relay

show ipv6 dhcp relay

Description

It shows the details about DHCPv6 relay configurations.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows the command exit.

```
DmSwitch#show ipv6 dhcp relay
```

```
Global DHCPv6 relay:      Enabled
```

```
DHCPv6 relay enabled:    VLAN 1
```

IPv6 Helper Address	Egress VLAN
2000::1	1
ff05::1:3	1

Related Commands

Command	Description
ipv6 dhcp relay	It enables the global DHCPv6 relay.
ipv6 helper-address	It adds unicast or multicast IPv6 address into the list of DHCPv6 servers global.
ipv6 dhcp relay	It enables the DHCPv6 relay agent on a VLAN.
show ipv6 dhcp relay	It shows the details about DHCPv6 relay configurations.

show ipv6 dhcp server

show ipv6 dhcp server

Description

Shows the DHCPv6 server global settings and status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCPv6 server settings.

```
DmSwitch#show ipv6 dhcp server
```

```
Server enabled: Yes
```

```
DmSwitch#
```

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.

Command	Description
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

show ipv6 dhcp pool

```
show ipv6 dhcp pool [ name ]
```

Description

Shows the DHCPv6 pool settings.

Syntax

Parameter	Description
<i>name</i>	Shows configuration for a specific pool.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCPv6 pools settings.

```
DmSwitch#show ipv6 dhcp pool
```

```
Pools table:
```

Pool name	Network
pool1	2000::/64
pool2	2001::/64
pool3	2002::/64

```
DmSwitch#
```

This example illustrates how to show the DHCPv6 pools settings for a specific pool.

```
DmSwitch#show ipv6 dhcp pool pool1
pool1
  Network: 2000::/64
  DNS Servers: 2000::1, 2000::2
  SIP Addresses: 2000::3, 2000::4
  SIP Domain Names: a.sip.com, b.sip.com
  Domain Search: datacom.net

DmSwitch#
```

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

show ip dhcp snooping

`show ip dhcp snooping`

Description

Shows the DHCP Snooping settings.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCP settings.

```
DmSwitch#show ip dhcp snooping

DHCP Snooping Information
-----

Global DHCP Snooping:      Enabled
Verify MAC address:       Enabled
VLAN(s) enabled:          15, 16, 17, 18, 19
                           20, 21, 22, 23, 24
                           25, 26, 27, 28, 29
                           30

DHCP Snooping L3 interface configuration:

Unit 1
----

Interface    Trusted
-----

```

```

1/1      no
1/2      no
1/3      no
1/4      no
1/5      no
1/6      no
1/7      no
1/8      no
1/9      no
1/10     yes
1/11     yes
1/12     yes
1/13     yes
1/14     yes
1/15     yes
1/16     yes
1/17     yes
1/18     yes
1/19     yes
1/20     yes
1/21     yes
1/22     yes
1/23     yes
1/24     yes
Port-Ch 1 no

```

```
DmSwitch#
```

Related Commands

Command	Description
show ip dhcp snooping statistics	Shows DHCP Snooping statistics.
ip dhcp snooping	Enables DHCP Snooping globally.
ip dhcp snooping	Enables DHCP Snooping at VLAN.
ip dhcp snooping trust	Configures port as trusted for DHCP Snooping.
ip dhcp snooping verify mac-address	Enables configuration to verify mac-address on a DHCP Snooping message.

show ip dhcp snooping database

show ip dhcp snooping database

Description

Shows the DHCP Snooping Database entries.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the DHCP Snooping Database entries.

```
DmSwitch#show ip dhcp snooping database
```

```
Dhcp Snooping Config:
Flash Memory filename: /mnt/flash/DHCPsnoopDB
Cyclic flash saving timer: 10 secs
Temporary File filename: /var/run/sync/DHCPsnoopDB
Cyclic file timer: 10 secs
```

Vlan	Ip Address	Interface	Mac Address	Lease Time	Remainig
3000	10.0.2.1	ETH 2/10	00:22:33:44:55:66	600	594
3001	10.1.2.1	ETH 2/11	10:22:33:44:55:66	600	594
3002	10.2.2.1	ETH 2/12	20:22:33:44:55:66	600	594
3003	10.3.2.1	ETH 2/13	30:22:33:44:55:66	600	594
3004	10.4.2.1	ETH 2/14	40:22:33:44:55:66	600	594
3005	10.5.2.1	ETH 2/15	50:22:33:44:55:66	600	594
3006	10.6.2.1	ETH 2/16	60:22:33:44:55:66	600	594
3007	10.7.2.1	ETH 2/17	70:22:33:44:55:66	600	594
3008	10.8.2.1	ETH 2/18	80:22:33:44:55:66	600	594

```
3009 10.9.2.1          PCH 2      90:22:33:44:55:66      600      595

Database has 10 entries.
DmSwitch#
```

Related Commands

Command	Description
ip dhcp snooping vlan binding	Creates a DHCP Snooping Database entry
ip dhcp snooping cyclic-save-timer	Configures a time value to save DHCP Snooping Database to a temporary file or to flash memory
clear ip dhcp snooping	Resets DHCP Snooping counters and database entries.

show ip dhcp snooping statistics

show ip dhcp snooping statistics

Description

Shows DHCP Snooping statistics informations.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display DHCP snooping statistics.

```
DmSwitch#show ip dhcp snooping statistics
```

```
DHCP Snooping Statistics
----
```

```
Total packets received:    0
Total packets forwarded:    0
Total packets dropped:      0
```

```
Statistics by L3 interface:
```

Port	Forwarded	Dropped	Received
2/1	0	0	0
2/2	0	0	0
2/3	0	0	0
2/4	0	0	0
2/5	0	0	0
2/6	0	0	0


```

2/7      0      0      0
2/8      0      0      0
2/9      0      0      0
2/10     0      0      0
2/11     0      0      0
2/12     0      0      0
2/13     0      0      0
2/14     0      0      0
2/15     0      0      0
2/16     0      0      0
2/17     0      0      0
2/18     0      0      0
2/19     0      0      0
2/20     0      0      0
2/21     0      0      0
2/22     0      0      0
2/23     0      0      0
2/24     0      0      0
2/25     0      0      0
2/26     0      0      0
3/1      0      0      0
3/2      0      0      0
3/3      0      0      0
3/4      0      0      0
3/5      0      0      0
3/6      0      0      0
3/7      0      0      0
3/8      0      0      0
3/9      0      0      0
3/10     0      0      0
3/11     0      0      0
3/12     0      0      0
3/13     0      0      0
3/14     0      0      0
3/15     0      0      0
3/16     0      0      0
3/17     0      0      0
3/18     0      0      0
3/19     0      0      0
3/20     0      0      0
3/21     0      0      0
3/22     0      0      0
3/23     0      0      0
3/24     0      0      0
Port-Ch 1 0      0      0
Port-Ch 2 0      0      0
=====

```

DmSwitch#

Related Commands

Command	Description
show ip dhcp snooping	Shows DHCP Snooping informations.
ip dhcp snooping	Enables DHCP Snooping globally.
ip dhcp snooping	Enables DHCP Snooping at VLAN.
ip dhcp snooping trust	Configures port as trusted for DHCP Snooping.

Command

**ip dhcp snooping verify
mac-address
clear ip dhcp snooping**

Description

Enables configuration to verify mac-address on a DHCP Snooping message.

Resets DHCP Snooping counters and database entries.

show ip dns-servers

show ip dns-servers

Description

Shows the configured DNS servers.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the configured DNS servers.

```
DmSwitch#show ip dns-servers
DNS servers: 10.11.12.14
DmSwitch#
```

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
ip dns-server	Configures the DNS servers used by DmSwitch
show ip	Shows the IP configuration.

show ip domain-name

show ip domain-name

Description

Shows the configured domain name.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the configured default gateway.

```
DmSwitch#show ip domain-name
Domain name: datacom.telematica
DmSwitch#
```

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
ip domain-name	Configures the domain name for DmSwitch.
show ip	Shows the IP configuration.
show running-config	Shows the current operating configuration.

show ip hardware ecmp-table

```
show ip hardware ecmp-table
```

Description

Shows the hardware ECMP group table.

Syntax

No parameter accepted.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.4	This command was introduced.

Usage Guidelines

The hardware ECMP group table is used by DmSwitch to show which ECMP groups exist, how many routes are using them, hash and all next-hops status.

Example

This example illustrates how to show the hardware ECMP group table.

[illegible]

Related Commands

No related command.

show ip hardware egr-table

show ip hardware egr-table

Description

Shows L3 Egress created on Hardware.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.0	First release. Command introduced.
13.4	Moved from show mpls hierarchy to show hierarchy.

Usage Guidelines

Not available.

Example

This example shows the command results for **show ip hardware egr-table**

```
DmSwitch#show ip hardware egr-table
```

```
+-----+-----+-----+-----+-----+-----+-----+
| Egr OID | Type | Intf | U/Po  | Vlan | Label | Instances | State |
+-----+-----+-----+-----+-----+-----+-----+
| 104130 | HOST | 0    | 4/8   | 4007 | 0      | 0         | Active|
| 104129 | MPLS | 0    | 0/T2  | 4000 | 0      | 0         | Active|
| 104128 | MPLS | 0    | 4/8   | 4007 | 0      | 0         | Stale |
+-----+-----+-----+-----+-----+-----+-----+
```

```
DmSwitch#
```


Related Commands

Command	Description
<code>show ip hardware intf-table</code>	Shows L3 Interfaces created on Hardware.
<code>show mac-address-table</code>	Shows the MAC address table.
<code>show running-config</code>	Shows the current operating configuration.

show ip hardware egr-info

show ip hardware egr-info [detail]

Description

Show L3 Egress Informations created on Hardware.

Syntax

Parameter	Description
detail	Show L3 Egress detailed informations.

Default

The Egress informations not detailed.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.2	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows the command results for **show ip hardware egr-info**

```
DmSwitch#show ip hardware egr-info
```

```
Egress in use:      30
Egress available:   4066
Total of resources: 4096
```

+-----+ EGRESS TYPE +-----+ Host MPLS ECMP IPTun +-----+ 2 28 0 0 +-----+ EGRESS PROTOCOL +-----+				
---	--	--	--	--

LDP	RSVP	BGP
6	13	0

DmSwitch#

This example shows the command results for **show ip hardware egr-info detail**

DmSwitch#show ip hardware egr-info detail

Egress in use: 30
 Egress available: 4066
 Total of resources: 4096

EGRESS TYPE			
Host	MPLS	ECMP	IP Tun
2	28	0	0

EGRESS PROTOCOL			
LDP	RSVP	BGP	
6	13	0	

Egress type and route detailed:

Egr OID	Type	Sub-Type	Protocol
104126	MPLS	NONE	LDP
104125	MPLS	NONE	LDP
104124	MPLS	NONE	UNKNW
104123	MPLS	Binding	UNKNW
104122	MPLS	NONE	UNKNW
104121	MPLS	NONE	RSVP
104120	MPLS	NONE	RSVP
104119	MPLS	NONE	RSVP
104118	MPLS	NONE	RSVP
104117	MPLS	NONE	RSVP
104116	MPLS	NONE	RSVP
104115	MPLS	NONE	RSVP
104114	MPLS	NONE	LDP
104113	MPLS	NONE	LDP
104112	MPLS	NONE	LDP
104111	MPLS	NONE	UNKNW
104110	MPLS	NONE	LDP
104109	MPLS	NONE	UNKNW
104108	MPLS	Binding	UNKNW
104107	MPLS	NONE	UNKNW
104106	MPLS	Binding	UNKNW
104105	MPLS	NONE	UNKNW
104104	MPLS	NONE	RSVP
104103	MPLS	NONE	RSVP
104102	MPLS	NONE	RSVP
104101	MPLS	NONE	RSVP
104100	MPLS	NONE	RSVP
104099	MPLS	NONE	RSVP
104098	HOST	NONE	UNKNW
104097	HOST	NONE	UNKNW

DmSwitch#

Related Commands

Command	Description
<code>show ip hardware egr-table</code>	Shows L3 Egress created on Hardware.
<code>show ip hardware intf-table</code>	Shows L3 Interfaces created on Hardware.
<code>show mac-address-table</code>	Shows the MAC address table.
<code>show running-config</code>	Shows the current operating configuration.

show ip hardware host-table

```
show ip hardware host-table [ interface { ethernet [ unit-number/ ] port-number |  
port-channel channel-group-number } | ip-address ip-address | mac-address mac-address |  
summary | vlan vlan-id ]
```

Description

Shows the hardware host table.

Syntax

Parameter	Description
interface	(Optional) Filter by interface.
ethernet <i>[unit-number/] port-number</i>	Shows the hardware host table of a specified unit and port. (Range: 1-1/1-28)
port-channel <i>channel-group-number</i>	Shows the hardware host table of a specified port-channel. (Range: 1-128)
ip-address <i>ip-address</i>	(Optional) Filter by host IP.
mac-address <i>mac-address</i>	(Optional) Filter by MAC address.
summary	(Optional) Summarize Host table results.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Rangs: 1-4094)

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
6.6	All sub commands were introduced, excepting summary .
7.6	The option summary was introduced.
13.0	Added 'Static' column to the command output table.
13.6.4	Improve command output in 'Example'.

Usage Guidelines

The hardware host table is used by DmSwitch to maps directly connected hosts IP addresses to MAC/VLAN/Port, since the DmSwitch makes routing by hardware.

Entering this command without parameters, the entire hardware host table will be shown.

Example

This example illustrates how to show the hardware host table.

```
DmSwitch#show ip hardware host-table
IP address      MAC              VLAN  Interface  Static  Hit
-----
10.11.12.13     00:E0:63:C4:C4:28 1      Eth 2/6    N       N
172.16.0.1      00:04:DF:19:24:EB 10     CPU        N       Y
172.16.0.2      (incomplete)      -      -          -       -
172.16.0.255    (black-hole)      -      -          -       -
200.200.200.5   00:04:DF:19:24:EB -      lo 0       N       Y

Total for this criterion: 5

Total: 5          Free: 32763

DmSwitch#
```

Related Commands

No related command.

show ipv6 hardware host-table

```
show ipv6 hardware host-table [ interface { ethernet [ unit-number/ ] port-number  
| port-channel channel-group-number } | ipv6-address ipv6-address | mac-address mac-  
address | summary | vlan vlan-id ]
```

Description

Shows the IPv6 hardware host table.

Syntax

Parameter	Description
interface	(Optional) Filter by interface.
ethernet <i>[unit-number/] port-number</i>	Shows the IPv6 hardware host table of a specified unit and port. (Range: 1-1/1-28)
port-channel <i>channel-group-number</i>	Shows the hardware host table of a specified port-channel. (Range: 1-128)
ipv6-address <i>ipv6-address</i>	(Optional) Filter by host IPv6.
mac-address <i>mac-address</i>	(Optional) Filter by MAC address.
summary	(Optional) Summarize Host table results.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Rangs: 1-4094)

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The IPv6 hardware host table is used by DmSwitch to maps directly connected hosts IPv6 addresses to MAC/VLAN/Port, since the DmSwitch makes routing by hardware.

Entering this command without parameters, the entire IPv6 hardware host table will be shown.

Example

This example illustrates how to show the IPv6 hardware host table.

```
DmSwitch#show ipv6 hardware host-table
```

```
Unit 1
```

IP address	MAC	VLAN	Interface	Hit
2001:DB8::1	00:04:DF:13:D1:1D	680	CPU	Y
2001:DB8::2	00:E0:63:C4:C4:28	680	CPU	Y

```
Total for this criterion: 2
```

```
Total: 2          Free: 32764
```

```
DmSwitch#
```

Related Commands

No related command.

show ip hardware intf-table

```
show ip hardware intf-table | detail
```

Description

Shows L3 Interfaces created on Hardware.

Inserting **detail** at the end of the command will show information associated to interface.

Syntax

Parameter	Description
detail	Shows detailed information of all L3 interface configured on HW.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.0	First release. Command introduced.
13.4	Moved from show mpls hierarchy to show hierarchy.

Usage Guidelines

Not available.

Example

These examples show the command results for **show ip hardware intf-table** and **show ip hardware intf-table detail**.

```
DmSwitch#show ip hardware intf-table
```

Intf	Info	Type	State	Vlan	Users
1	0x00000239	vlan	Active	0	0
2	0x0000023A	vlan	Active	0	0
3	0x00000001	vlan	Active	0	0
6	0x00000014	mpls	Active	0	0

DmSwitch#

DmSwitch#show ip hardware intf-table detail

Intf	Info	Type	State	Vlan	Users	Label1	Label2	Action
4	0x00000012	vlan	Stale	571	0	0	0	---
5	0x00000013	mpls	Active	564	2	0	0	---
5	0x00000013	mpls	Active	569	0	0	0	FWD
6	0x00000014	mpls	Active	0	0	104	0	PSH

DmSwitch#

Related Commands

Command	Description
show ip hardware egr-table	Shows L3 Egress created on Hardware.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

show ip hardware lpm-table

```
show ip hardware lpm-table [ interface { ethernet [ unit-number/ ] port-number |  
port-channel channel-group-number } | ip-address ip-address | mac-address mac-address |  
summary | vlan vlan-id | vrf vrf-name ] [ | tftp ip-address filename ]
```

Description

Shows the hardware longest prefix match table.

Syntax

Parameter	Description
interface	(Optional) Filter by interface.
ethernet <i>[unit-number/] port-number</i>	Shows the hardware lpm table of a specified unit and port. (Range: 1-1/1-28)
port-channel <i>channel-group-number</i>	Shows the hardware lpm table of a specified port-channel. (Range: 1-128)
ip-address <i>ip-address</i>	(Optional) Filter by host IP.
mac-address <i>mac-address</i>	(Optional) Filter by MAC address.
summary	(Optional) Summarize lpm table results.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Range: 1-4094)
vrf <i>vrf-name</i>	(Optional) Filter by VRF.
tftp <i>ip-address filename</i>	(Optional) Redirects the output to the tftp server on <i>ip-address</i> with filename <i>filename</i> .

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
6.6	All sub commands were introduced, excepting summary .
7.6	The option summary was introduced.
10.0	The options vrf and tftp were introduced and the command output was changed.

Release	Modification
12.2	Command output was changed. Hit column was removed from default output is only shown when ip-address parameter is specified

Usage Guidelines

The hardware longest prefix match table is used by DmSwitch to maps subnets to gateway MAC/VLAN/Port, since the DmSwitch makes routing by hardware.

Entering this command without parameters, the entire hardware LPM table will be shown.

Example

This example illustrates how to show the hardware longest prefix match table.

```
DmSwitch#show ip hardware lpm-table
```

```
Unit 1
```

Network subnet	Next Hop MAC	VLAN	Unit	Port	PortCh	Local
192.168.101.0/24	08:00:27:48:76:17	480	1	6	-	N
172.16.48.0/29	-	480	-	-	-	Y
2.3.4.5/32	08:00:27:48:76:17	480	1	6	-	N

```
Total for this criterion: 3
```

```
Total: 3          Free: 524285
```

```
DmSwitch#
```

Example illustrating how to send the show's output through tftp.

```
DmSwitch#show ip hardware lpm-table | tftp 10.1.3.51 lpm.txt
DmSwitch#
```

Related Commands

Command	Description
show ip route	Shows the IP routing table.

show ipv6 hardware lpm-table

```
show ipv6 hardware lpm-table [ interface { ethernet [ unit-number/ ] port-number  
| port-channel channel-group-number } | ipv6-address ipv6-address | mac-address mac-  
address | summary | vlan vlan-id | vrf vrf-name ] [ | tftp ip-address filename ]
```

Description

Shows the IPv6 hardware longest prefix match table.

Syntax

Parameter	Description
interface	(Optional) Filter by interface.
ethernet <i>[unit-number/] port-number</i>	Shows the IPv6 hardware lpm table of a specified unit and port. (Range: 1-1/1-28)
port-channel <i>channel-group-number</i>	Shows the IPv6 hardware lpm table of a specified port-channel. (Range: 1-128)
ipv6-address <i>ipv6-address</i>	(Optional) Filter by host IP.
mac-address <i>mac-address</i>	(Optional) Filter by MAC address.
summary	(Optional) Summarize IPv6 lpm table results.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Range: 1-4094)
vrf <i>vrf-name</i>	(Optional) Filter by VRF.
tftp <i>ip-address filename</i>	(Optional) Redirects the output to the tftp server on <i>ip-address</i> with filename <i>filename</i> .

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.
12.2	Command output was changed. Hit column was removed from default output is only shown when ipv6-address parameter is specified

Usage Guidelines

The IPv6 hardware longest prefix match table is used by DmSwitch to maps subnets to gateway MAC/VLAN/Port, since the DmSwitch makes routing by hardware.

Entering this command without parameters, the entire IPv6 hardware LPM table will be shown.

Example

This example illustrates how to show the IPv6 hardware longest prefix match table.

```
DmSwitch#show ipv6 hardware lpm-table
```

```
Unit 1
```

Network subnet	Next Hop MAC	VLAN	Unit	Port	PortCh	Local
2001:DB8:1000::/36	-	680	-	-	-	Y
2001:DB8:2000::/36	-	690	-	-	-	Y

```
Total for this criterion: 2
```

```
Total: 2          Free: 524284
```

```
DmSwitch#
```

Example illustrating how to send the show's output through tftp.

```
DmSwitch#show ipv6 hardware lpm-table | tftp 10.1.3.84 lpm.txt
DmSwitch#
```

Related Commands

Command	Description
show ipv6 route	Shows the IPv6 routing table.

show ip http

show ip http

Description

Shows the HTTP server information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the HTTP and secure HTTP servers status (enabled or disabled), the configured access port for the both servers and the maximum connections allowed for their clients.

Example

This example illustrates how to show the HTTP server information.

```
DmSwitch#show ip http
HTTP:
  HTTP status:  Enable
  HTTP port:    80

secure HTTP:
  HTTPS status:  Enable
  HTTPS port:    443

HTTP/HTTPS connections limit: 8

DmSwitch#
```

Related Commands

Command	Description
<code>ip http</code>	Configures the internal HTTP server for external access.

show ip igmp snooping

```
show ip igmp snooping [ mroute ]
```

Description

Shows the IGMP snooping configuration.

Syntax

Parameter	Description
mroute	(Optional) Click here to see the "mroute" parameter description.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Entering this command without parameters, will be shown the IGMP snooping status (enabled or disabled), the configured time parameters, query count, IGMP version and IGMP IP address.

Example

This example illustrates how to show the HTTP server information.

```
DmSwitch#show ip igmp snooping
Service status:           Enabled
Querier status:           Enabled
Query count:              3
Query interval:           60 sec
Query max response time:  10 sec
Last member query interval: 1 sec
Router port expire time:  300 sec
IGMP snooping version:    2
IGMP querier IP address:  (not set)
Flood unknown traffic:    Enabled
```

```
SSM-Map: (not set)
DmSwitch#
```

Related Commands

Command	Description
ip igmp	Configures the IGMP snooping.
ip igmp snooping vlan	Configures static multicast entries in the mac address table.
show ip igmp snooping mroute	Shows the static entries in mac address table of the multicast routers.

show ipv6 mld snooping

```
show ipv6 mld snooping [ mroute ]
```

Description

Shows the MLD snooping configuration.

Syntax

Parameter	Description
mroute	(Optional) Click here to see the "mroute" parameter description.

Default

No default is defined.

Command Modes

Privileged EXEC.

Usage Guidelines

Entering this command without parameters, will be shown the MLD snooping status (enabled or disabled), the configured time parameters, query count, MLD version and MLD IP address.

Example

This example illustrates how to show the HTTP server information.

```
DmSwitch#show ipv6 mld snooping
Service status:           Enabled
Querier status:           Enabled
Query count:               2
Query interval:            125 sec
Query max response time:   10 sec
Router port expire time:   300 sec
MLD snooping version:      3
MLD querier IP address:    (not set)

DmSwitch#
```

Related Commands

Command	Description
ipv6 mld snooping vlan	Configures static multicast entries in the mac address table.

Command	Description
<code>show ipv6 mld snooping mroute</code>	Shows the static entries in mac address table of the multicast routers.

show ip igmp snooping mroute

```
show ip igmp snooping mroute [ vlan index ]
```

Description

Shows the static entries in mac address table of the multicast routers.

Syntax

Parameter	Description
<i>vlan index</i>	(Optional) Specifies a VLAN index. (Range: 1-4094)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the VLAN index and the port number that is configured to connect a multicast router.

Entering this command without parameters, all VLAN informations will be shown.

Example

This example illustrates how to show the static entries in mac address table of the multicast routers.

```
DmSwitch#show ip igmp snooping mroute
VLAN M'cast Router Ports Type
-----
1          Eth1/ 1 Static
DmSwitch#
```

Related Commands

Command	Description
<code>ip igmp</code>	Configures the IGMP snooping.
<code>ip igmp snooping vlan</code>	Configures static multicast entries in the mac address table.
<code>show ip igmp snooping</code>	Shows the IGMP snooping configuration.

show ipv6 mld snooping mroute

show ipv6 mld snooping mroute [*vlan index*]

Description

Shows the static entries in mac address table of the multicast routers.

Syntax

Parameter	Description
vlan index	(Optional) Specifies a VLAN index. (Range: 1-4094)

Default

No default is defined.

Command Modes

Privileged EXEC.

Usage Guidelines

This command shows the VLAN index and the port number that is configured to connect a multicast router.

Entering this command without parameters, all VLAN informations will be shown.

Example

This example illustrates how to show the static entries in mac address table of the multicast routers.

```
DmSwitch#show ipv6 mld snooping mroute
VLAN M'cast Router Ports Type
-----
    1                Eth1/ 1 Static
DmSwitch#
```

Related Commands

Command	Description
ipv6 mld snooping vlan	Configures static multicast entries in the mac address table.
show ipv6 mld snooping	Shows the MLD snooping configuration.

show ip interface

show ip interface

Description

Shows the interface information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the IP address configured for each VLAN.

Example

This example illustrates how to show the interface information.

```
DmSwitch#show ip interface
VLAN 1  10.11.12.21/24
VLAN 2  10.11.13.21/24

DmSwitch#
```

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.

show ipv6 interface

show ipv6 interface

Description

Shows IPv6 interface information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command shows the IPv6 address configured for each VLAN.

Example

This example illustrates how to show the interface information.

```
DmSwitch#show ipv6 interface
VLAN 1          Scope Global  2001:DB8:1::204:dfff:fe13:d11d
VLAN 1          Scope Link   fe80::204:df00:113:3263/64
VLAN 1          Scope Link   fe80::200:5eff:fe00:101/64
VLAN 2          Scope Global  2001:DB8:2::204:dfff:fe13:d11d
VLAN 2          Scope Link   fe80::204:df00:213:3263/64
VLAN 2          Scope Link   fe80::204:dfff:fe13:3263/64

DmSwitch#
```

Related Commands

Command	Description
ipv6 address	Sets an IPv6 address for the selected VLAN.

show ip multicast-routing

```
show ip multicast-routing { table [ group ip-address [ ... ] | source ip-address [ ... ] |  
type { all [ ... ] | reserved [ ... ] | user [ ... ] } | vlan vlan-id [ ... ] | units }
```

Description

Shows the multicast routing configuration.

Syntax

Parameter	Description
table	Shows multicast forwarding table.
units	Shows the multicast enabled per unit.
group <i>ip-address</i>	(Optional) Filter by group type.
source <i>ip-address</i>	(Optional) Filter by source address.
type <i>ip-address</i>	(Optional) Filter by group type.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Range: 1-4094)
all	Specifies all groups.
reserved	Specifies groups reserved for administrative applications.
user	Specifies user traffic groups.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the multicast-routing status on the unit 1. (to DmSwitch 3000)

```
DmSwitch#show ip multicast-routing units
Unit 1:                Enabled

DmSwitch#
```

Related Commands

No related command.

show ipv6 multicast-routing

```
show ipv6 multicast-routing { table [ group ipv6-address [ ... ] | source ipv6-address [ ... ] | type { all [ ... ] | reserved [ ... ] | user [ ... ] } | vlan vlan-id [ ... ] | units }
```

Description

Shows the IPv6 multicast routing configuration.

Syntax

Parameter	Description
table	Shows IPv6 multicast forwarding table.
units	Shows the multicast enabled per unit.
group <i>ipv6-address</i>	(Optional) Filter by group type.
source <i>ipv6-address</i>	(Optional) Filter by source address.
type <i>ipv6-address</i>	(Optional) Filter by group type.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Range: 1-4094)
all	Specifies all groups.
reserved	Specifies groups reserved for administrative applications.
user	Specifies user traffic groups.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Usage Guidelines

Not available.

Example

This example illustrates how to show the IPv6 multicast-routing table. (to DM4000)

```
DmSwitch#show ipv6 multicast-routing table
VLAN 720, Group: 2001:DB8::1, Source: *
      MLD Static: 1/17
DmSwitch#
```

Related Commands

No related command.

show ip ospf

```
show ip ospf [ border-routers ]
```

```
show ip ospf [ database [ max-age | self-originate ] ]
```

```
show ip ospf [ database [ asbr-summary | external | network | nssa-external  
| router | summary ] [ adv-router adv-router-ip-address | self-originate |  
link-state-ip-address [ adv-router adv-router-ip-address | self-originate ] ] ]
```

```
show ip ospf [ neighbor [ detail ] ]
```

```
show ip ospf [ route ]
```

```
show ip ospf [ virtual-links ]
```

```
show ip ospf [ vlan vlan-id ]
```

Description

Shows the OSPF process parameters.

Syntax

Parameter	Description
border-routers	(Optional) Border information for the area.
database	(Optional) Database summary.
asbr-summary	(Optional) ASBR summary link states.
external	(Optional) External link states.
network	(Optional) Network link states.
nssa-external	(Optional) NSSA external link state.
router	(Optional) Router link states.
summary	(Optional) Network summary link states.
adv-router <i>adv-router-ip-address</i>	(Optional) Advertising Router link states.
<i>link-state-ip-address</i>	(Optional) Link State ID.
max-age	(Optional) LSAs in MaxAge list.
self-originate	(Optional) Self-originated link states.
neighbor detail	(Optional) List neighbors (with or without details).
route	(Optional) Shows the OSPF routing table.
virtual-links	(Optional) Shows virtual links information.
vlan <i>vlan-index</i>	(Optional) Advertising Router link states.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.
9.4	The virtual-links parameter was added.
8.0	The max-age parameter was deprecated.

Usage Guidelines

Entering this command without parameters, the basic OSPF information will be shown.

Example

This example illustrates how to show the basic OSPF information.

```
DmSwitch#show ip ospf
  OSPF Routing with Router ID: 192.168.0.25
  Admin status: up, Operational status: up
  TOS routing support is disabled
  RFC1583 Compatibility is disabled
  Opaque Capability is enabled
  Traffic Engineering support is disabled
  Equal Cost Multi-Path (ECMP) support is disabled
  Maximum Admin Distance at router is disabled
  Maximum Metric at router is disabled
  Route Admin Distances: Internal 30, External 110
  External LSA reflood timer is 1800 secs
  This router is an AS Border Router
  Redistributing External Routes from:
    connected with metric 20
  SPF recalculation triggers:
    Maximum delay is 5000 msec
    LS updates threshold to start recalculation is infinite
    LS updates threshold to restart recalculation is infinite
    Inter-Area/AS-extern LS pending updates threshold to full recalculation is 50
    Intra-Area LS pending updates threshold to full recalculation is immediate
  Non-Stop Forwarding (NSF) Information:
    NSF planned is enabled
    NSF unplanned is disabled
    NSF start-up status: disabled / not-started
    NSF restart-interval limit: 120 secs
    NSF remaining time: 0 secs
```



```
NSF helper support is: enabled
NSF helper maximum restart-interval: 140 secs
Number of external LSA (type-5)      5. Checksum Sum 0x000307ab
Number of ext-opaque LSA (type-11)   0. Checksum Sum 0x00000000
Number of areas in this router is 1 (1 normal, 0 stub, 0 nssa)
Area BACKBONE - 0 - (0.0.0.0)
  It is a NORMAL area
  Area has no authentication
  LSA reflood timer is 1800 secs
  SPF algorithm executed 3 times
  Number of reachable Area Border Router 0
  Number of reachable AS Border Router 1
  Number of LSA 3. Checksum Sum 0x0001a76b
    Router LSA (type-1)      2. Checksum Sum 0x0000e82f
    Network LSA (type-2)    1. Checksum Sum 0x0000bf3c
    Summary LSA (type-3)    0. Checksum Sum 0x00000000
    ASBR-S LSA (type-4)     0. Checksum Sum 0x00000000
    NSSA LSA (type-7)       0. Checksum Sum 0x00000000
    Opaque LSA (type-10)    0. Checksum Sum 0x00000000

DmSwitch#
```

Related Commands

Command	Description
router ospf	Enables and accesses the OSPF configuration.

show ipv6 ospfv3

```
show ipv6 ospfv3 [ database [ database-summary | external | inter-area-prefix  
| inter-area-router | intra-area-prefix | link | network | nssa | router ] [  
adv-router A.B.C.D | self-originate | link-state-ipv4-address [ adv-router | A.B.C.D |  
self-originate ] ] ]
```

```
show ipv6 ospfv3 [ neighbor [ detail ] ]
```

```
show ipv6 ospfv3 [ vlan vlan-id ]
```

Description

Shows the OSPFv3 process parameters.

Syntax

Parameter	Description
database	(Optional) Dump all database.
database-summary	(Optional) Summary database link states.
external	(Optional) External link states (Type-5).
inter-area-prefix	(Optional) Inter-Area Prefix link states (Type-3).
inter-area-router	(Optional) Inter-Area Router link states (Type-4).
intra-area-prefix	(Optional) Intra-Area Prefix link states (Type-9).
link	(Optional) Link link states (Type-8).
network	(Optional) Network link states (Type-2).
nssa	(Optional) NSSA link states (Type-7).
router	(Optional) Router link states (Type-1).
adv-router <i>A.B.C.D</i>	(Optional) Advertising Router link states.
<i>link-state-ipv4-address</i>	(Optional) Link State ID.
self-originate	(Optional) Self-originated link states.
neighbor detail	(Optional) List neighbors (with or without details).
vlan <i>vlan-index</i>	(Optional) Advertising Router link states.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, the basic OSPFv3 information will be shown.

Example

This example illustrates how to show the basic OSPFv3 information.

```
DmSwitch#show ipv6 ospfv3
OSPFv3 Routing with Router ID: 100.100.100.203
Admin status: up, Operational status: up
Traffic Engineering support is disabled
Equal Cost Multi-Path (ECMP) support is disabled
Route Admin Distances: Internal 30, External 110
External LSA reflood timer is 1800 secs
This router is an AS Border Router
Redistributing External Routes from:
  connected with metric 20
  static with metric 20
SPF recalculation triggers:
  Maximum delay is 5000 msec
  LS updates threshold to start recalculation is infinite
  LS updates threshold to restart recalculation is infinite
  Inter-Area/AS-extern LS pending updates threshold to full recalculation is 50
  Intra-Area LS pending updates threshold to full recalculation is immediate
Non-Stop Forwarding (NSF) Information:
  NSF planned is enabled
  NSF unplanned is enabled
  NSF start-up status: disabled / not-started
  NSF restart-interval limit: 120 secs
  NSF remaining time: 0 secs
  NSF helper support is: enabled
  NSF helper maximum restart-interval: 140 secs
Number of external LSA (type-0x4005) 0.
Number of AS-Scope LSA 0. Checksum Sum 0x00000000
Number of areas in this router is 1 (1 normal, 0 stub, 0 nssa)
Area BACKBONE - 0 - (0.0.0.0)
  It is a NORMAL area
  LSA reflood timer is 1800 secs
  SPF algorithm executed 1 times
  Number of reachable Area Border Router 0
  Number of reachable AS Border Router 1
  Number of LSA 1. Checksum Sum 0x00000433
    Router LSA (type-0x2001) 1. Checksum Sum 0x00000433
    Network LSA (type-0x2002) 0. Checksum Sum 0x00000000
    Inter-Area-Prefix LSA (type-0x2003) 0. Checksum Sum 0x00000000
    Inter-Area-Router LSA (type-0x2004) 0. Checksum Sum 0x00000000
    Group Membership LSA (type-0x2006) 0. Checksum Sum 0x00000000
```

```
Type7          LSA (type-0x2007)  0. Checksum Sum 0x00000000
Intra-Area-Prefix LSA (type-0x2009) 0. Checksum Sum 0x00000000
Intra-Area-TE    LSA (type-0xA00A)  0. Checksum Sum 0x00000000

DmSwitch#
```

Related Commands

Command	Description
<code>router ospfv3</code>	Enables and accesses the OSPFv3 configuration.

show ip path-mtu-discovery cache

show ip path-mtu-discovery cache [*ip-address*]

Description

Displays the Path MTU Discovery table with route cache information.

Syntax

Parameter	Description
<i>ip-address</i>	(Optional) Shows only Path MTU Discovery cache entries with given destination IP address.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

This command shows Path MTU Discovery information.

Examples

This example illustrates how to show information about Path MTU Discovery.

```
DmSwitch#show ip path-mtu-discovery cache
Vlan Destination      From                Via                MTU
-----
684  172.16.69.2        172.16.68.42       172.16.68.41      1300
692  224.0.0.5          172.16.95.17       172.16.68.41      1500
DmSwitch#
```

Related Commands

Command	Description
<code>clear ip path-mtu-discovery cache</code>	Clear IP Path MTU Discovery cache.
<code>show ipv6 path-mtu-discovery cache</code>	Shows the IPv6 Path MTU Discovery cache entries.
<code>clear ipv6 path-mtu-discovery cache</code>	Clear IPv6 Path MTU Discovery cache.

show ipv6 path-mtu-discovery cache

show ipv6 path-mtu-discovery cache [*ipv6-address*]

Description

Displays the Path MTU Discovery table with route cache information.

Syntax

Parameter	Description
<i>ipv6-address</i>	(Optional) Shows only Path MTU Discovery cache entries with given destination IPv6 address.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

This command shows Path MTU Discovery information.

Examples

This example illustrates how to show information about Path MTU Discovery.

```
DmSwitch#show ipv6 path-mtu-discovery cache
Vlan Destination                               Via                                           MTU
-----
581  ff02::1                                   ff02::1                                   1500
580  ff02::1                                   ff02::1                                   1500
581  ff02::5                                   ff02::5                                   1500
581  ff02::d                                   ff02::d                                   1500
580  ff02::d                                   ff02::d                                   1500
DmSwitch#
```

Related Commands

Command	Description
<code>clear ipv6 path-mtu-discovery cache</code>	Clear IPv6 Path MTU Discovery cache.
<code>show ip path-mtu-discovery cache</code>	Shows the IP Path MTU Discovery cache entries.
<code>clear ip path-mtu-discovery cache</code>	Clear IP Path MTU Discovery cache.

show ip pim bsr-candidate

show ip pim bsr-candidate

Description

Shows the candidate for Bootstrap Router (BSR) and its respective parameters, such as priorities, timeout values, state and LocalAddress.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the information related to the candidate for Bootstrap Router, its respective priority for the BSR election, local address, state (Elected or not) and timeout values. It also shows the Elected BSR, its address, priority and Expiry Time.

Example

This example illustrates how to show PIM BSR-Candidate information.

```
DmSwitch(config)#show ip pim bsr-candidate
```

```
Elected BSR      Pri Expiry Time
-----
10.42.3.151      1    1646

Cand-BSR          Pri LocalAddress  Pri State      Timeout
-----
10.42.3.151      1 10.42.3.151    1 Elected      1628

DmSwitch(config)#
```

Related Commands

Command	Description
<code>ip pim bootstrap</code> <code>bsr-candidate</code>	Sets BSR Candidate parameters.

show ipv6 pim bsr-candidate

show ipv6 pim bsr-candidate

Description

Shows the candidate for Bootstrap Router (BSR) and its respective parameters, such as priorities, timeout values, state and local IPv6 address.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the information related to the candidate for Bootstrap Router, its respective priority for the BSR election, local address, state (Elected or not) and timeout values. It also shows the Elected BSR, its address, priority and Expiry Time.

Example

This example illustrates how to show PIM BSR-Candidate information.

```
DmSwitch(config)#show ipv6 pim bsr-candidate
Elected BSR          Pri Expiry Time
-----
2001:db8::1          1    2666
Cand-BSR              Pri LocalAddress          Pri State          Timeout
-----
2001:db8::1          1 2001:db8::1          1 Elected          2666

DmSwitch(config)#
```

Related Commands

Command	Description
<code>ipv6 pim bootstrap bsr-candidate</code>	Sets BSR Candidate parameters.

show ip pim config

show ip pim config

Description

Shows global PIM (Protocol Independent Multicast) configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the status for global PIM, PIM SPT switchover, PIM Bootstrap, RP-address, BSR and RP Candidates, and VLAN interfaces with PIM enabled.

Example

This example illustrates how to show PIM configuration.

```
DmSwitch(config)#show ip pim config
PIM Status: enabled
PIM SPT switchover: enabled
PIM Bootstrap: enabled

PIM Enabled on VLAN 420

BSR-Candidate: VLAN 420

DmSwitch(config)#
```

Related Commands

Command	Description
<code>ip pim</code>	Enables global PIM protocol.
<code>ip pim rp-address</code>	Configures static RP-Address for PIM protocol.
<code>ip pim spt-switch</code>	Sets immediate SPT switchover.
<code>ip pim bootstrap</code>	Sets Bootstrap feature.
<code>ip pim bootstrap bsr-candidate</code>	Sets BSR Candidate parameters.
<code>ip pim bootstrap rp-candidate</code>	Sets RP Candidate parameters.
<code>ip pim</code>	Enables PIM protocol on a VLAN interface.

show ipv6 pim config

show ipv6 pim config

Description

Shows global IPv6 PIM (Protocol Independent Multicast) configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the status for global PIM, PIM SPT switchover, PIM Bootstrap, RP-address, BSR and RP Candidates, and VLAN interfaces with PIM enabled.

Example

This example illustrates how to show PIM configuration.

```
DmSwitch(config)#show ipv6 pim config
PIM IPv6 Status: enabled
PIM SPT switchover: enabled
PIM Bootstrap: enabled

PIM Enabled on VLAN 720

PIM Enabled on VLAN 721

Static RP: 2001:db8::1
          Group-Prefix: ff00::/8

BSR-Candidate: VLAN 721

RP-Candidate: VLAN 720
              Group-Prefix: ff07::/16
              Priority: 12
```

```
Holdtime: 65  
DmSwitch(config)#
```

Related Commands

Command	Description
ipv6 pim	Enables global PIM protocol.
ipv6 pim rp-address	Configures static RP-Address for IPv6 PIM protocol.
ipv6 pim spt-switch	Sets immediate SPT switchover.
ipv6 pim bootstrap	Sets Bootstrap feature.
ipv6 pim bootstrap bsr-candidate	Sets BSR Candidate parameters.
ipv6 pim bootstrap rp-candidate	Sets RP Candidate parameters.
ipv6 pim	Enables PIM protocol on a VLAN interface.

show ip pim interfaces

show ip pim interfaces

Description

Shows PIM (Protocol Independent Multicast) interfaces parameters, such as Designated Router (DR) address, neighbours count, VLANs with PIM enabled and their priority for DR election.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the information related to VLAN interfaces with PIM enabled. It will show their PIM State (DR or not DR), quantity of neighbours, Designated Router address, and priority for DR election.

Example

This example illustrates how to show PIM interfaces information.

```
DmSwitch(config)#show ip pim interfaces
```

VLAN	PIM State	Neighbors	DR Address	Priority
420	DR	0	10.42.0.151	1

```
DmSwitch(config)#
```

Related Commands

Command	Description
ip pim	Enables PIM protocol on a VLAN interface.

show ipv6 pim interfaces

show ipv6 pim interfaces

Description

Shows IPv6 PIM (Protocol Independent Multicast) interfaces parameters, such as Designated Router (DR) address, neighbours count, VLANs with PIM enabled and their priority for DR election.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the information related to VLAN interfaces with PIM for IPv6 enabled. It will show their PIM State (DR or not DR), quantity of neighbours, Designated Router address, and priority for DR election.

Example

This example illustrates how to show PIM interfaces information.

```
DmSwitch(config)#show ipv6 pim interfaces
```

VLAN	PIM State	Neighbors	DR Address	Priority
720	DR	0	fe80::204:df02:d013:fcde	1
721	DR	0	fe80::204:df02:d113:fcde	1

```
DmSwitch(config)#
```

Related Commands

Command	Description
---------	-------------

Command	Description
ipv6 pim	Enables PIM protocol on a VLAN interface.

show ip pim join

```
show ip pim join [ group ip-address | source ip-address | summary | vlan vlan-id ]
```

Description

Shows PIM Join status for the Group and Source address entries, and their correspondent neighbor, RP (Rendezvous Point) address, interface information and assert status.

Syntax

Parameter	Description
group <i>ip-address</i>	(Optional) Filter by a multicast group IP address.
source <i>ip-address</i>	(Optional) Filter by source IP address.
summary	(Optional) Summarize Host table results.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Rangs: 1-4094)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.
12.2	Added filter parameters.

Usage Guidelines

This command shows the Join Status information (joined/not joined) for the Upstream Neighbors and VLAN Interfaces, with additional information of RP-Address for the distribution tree, PIM Neighbor address, indicative Flags for Shortest-Path Tree (SPT) and Designated Router (DR), and Assert value (Winner/Loser) for the VLAN Interface.

Example

This example illustrates how to show PIM join information.

```
DmSwitch(config)#show ip pim join
```

```

Group Address   Source Address  RP Address      Neighbor         Vlan  Flags
-----
224.10.10.1     10.42.2.88     0.0.0.0         10.42.0.155     420   SPT DR
Join State: not joined
Join Timer: 0

Interfaces:
  Vlan    Local Membership  Join/Prune State  Timer  Assert
-----
  420     Joined           Joined            0      Winner

DmSwitch(config)#

```

Related Commands

Command	Description
ip pim	Enables global PIM protocol.
ip pim	Enables PIM protocol on a VLAN interface.

show ipv6 pim join

show ipv6 pim join [**group** *ipv6-address* | **source** *ipv6-address* | **summary** | **vlan** *vlan-id*]

Description

Shows IPv6 PIM Join status for the Group and Source address entries, and their correspondent neighbor, RP (Rendezvous Point) address, interface information and assert status.

Syntax

Parameter	Description
group <i>ipv6-address</i>	(Optional) Filter by a multicast group IPv6 address.
source <i>ipv6-address</i>	(Optional) Filter by a source IPv6 address.
summary	(Optional) Summarize Host table results.
vlan <i>vlan-id</i>	(Optional) Filter by VLAN. (Rangs: 1-4094)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the Join Status information (joined/not joined) for the Upstream Neighbors and VLAN Interfaces, with additional information of RP-Address for the distribution tree, PIM Neighbor address, indicative Flags for Shortest-Path Tree (SPT) and Designated Router (DR), and Assert value (Winner/Loser) for the VLAN Interface.

Example

This example illustrates how to show PIM join information.

```
DmSwitch(config)#show ipv6 pim join
```

Group Address	Source Address	RP Address	Neighbor	Vlan	Flags
-----	-----	-----	-----	-----	-----

```
ff01:1000::          ::          2001:db8::          ::          720
Join State: not joined
Join Timer: 0

Interfaces:
  Vlan    Local Membership  Join/Prune State  Timer  Assert
-----  -
  720    Joined             Joined            0      Winner
DmSwitch(config)#
```

Related Commands

Command	Description
ipv6 pim	Enables global PIM protocol.
ipv6 pim	Enables PIM protocol on a VLAN interface.

show ip pim mfc

`show ip pim mfc`

Description

Shows the PIM multicast forwarding entries, the multicast group and source addresses, and their incoming and outgoing VLANs.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the information related to the PIM multicast forwarding cache (MFC), which are the group and source entries for the multicast packets, and their respective incoming and outgoing VLAN interfaces.

Example

This example illustrates how to show PIM MFC information.

```
DmSwitch(config)#show ip pim mfc

Group          Source
-----
224.10.10.1    10.42.0.7
    Incoming VLAN: 420
    Outgoing VLANs: 422

DmSwitch(config)#
```

Related Commands

Command	Description
<code>ip pim</code>	Enables global PIM protocol.
<code>ip pim</code>	Enables PIM protocol on a VLAN interface.

show ipv6 pim mfc

show ipv6 pim mfc

Description

Shows the IPv6 PIM multicast forwarding entries, the multicast group and source addresses, and their incoming and outgoing VLANs.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the information related to the IPv6 PIM multicast forwarding cache (MFC), which are the group and source entries for the multicast packets, and their respective incoming and outgoing VLAN interfaces.

Example

This example illustrates how to show IPv6 PIM MFC information.

```
DmSwitch(config)#show ipv6 pim mfc

Group                               Source
-----
ff00::5                            2001:db8::1
    Incoming VLAN: 420
    Outgoing VLANs: 422

DmSwitch(config)#
```

Related Commands

Command	Description
<code>ipv6 pim</code>	Enables global PIM protocol.
<code>ipv6 pim</code>	Enables PIM protocol on a VLAN interface.

show ip pim neighbors

show ip pim neighbors

Description

Shows all PIM (Protocol Independent Multicast) neighbors the router has knowledge, their addresses, DR (Designated Router) priorities, uptime and timeout values

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the information related to the PIM neighbors the router has knowledge, their VLAN and IP addresses, priorities for the DR election, how long they have been up (uptime) and timeout values.

Example

This example illustrates how to show PIM neighbors information.

```
DmSwitch(config)#show ip pim neighbors
```

VLAN	Neighbor Address	DR-Priority	Uptime	Timeout
420	10.42.0.155	1	5824	102

```
DmSwitch(config)#
```

Related Commands

Command	Description
ip pim	Enables PIM protocol on a VLAN interface.

show ipv6 pim neighbors

show ipv6 pim neighbors

Description

Shows all IPv6 PIM (Protocol Independent Multicast) neighbors the router has knowledge, their addresses, DR (Designated Router) priorities, uptime and timeout values

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the information related to the IPv6 PIM neighbors the router has knowledge, their VLAN and IPv6 addresses, priorities for the DR election, how long they have been up (uptime) and timeout values.

Example

This example illustrates how to show PIM neighbors information.

```
DmSwitch(config)#show ipv6 pim neighbors
```

VLAN	Neighbor Address	DR-Priority	Uptime	Timeout
420	2001:DB8::1	1	2665	112

```
DmSwitch(config)#
```

Related Commands

Command	Description
ipv6 pim	Enables PIM protocol on a VLAN interface.

show ip pim rp-candidate

show ip pim rp-candidate

Description

Shows the candidates for Rendezvous Point (RP) and their respective parameters, such as group-prefix, priority and timeout values.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the information related to the candidates for Rendezvous Point, their respective priorities for the RP election, group-prefix and timeout values.

Example

This example illustrates how to show PIM RP-candidate information.

```
DmSwitch(config)#show ip pim rp-candidate
```

RP Address	GroupPrefix	Priority	Timeout
10.42.8.151	224.0.0.0/4	78	13302

Candidate-RP	GroupPrefixIdx	Priority	CandRpAdvTimeout
10.42.8.151	1	78	4282

```
DmSwitch(config)#
```

Related Commands

Command	Description
<code>ip pim bootstrap</code> <code>rp-candidate</code>	Sets RP Candidate parameters.

show ipv6 pim rp-candidate

```
show ipv6 pim rp-candidate
```

Description

Shows the IPv6 candidates for Rendezvous Point (RP) and their respective parameters, such as group-prefix, priority and timeout values.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the information related to the candidates for IPv6 Rendezvous Point (RP), their respective priorities for the RP election, group-prefix and timeout values.

Example

This example illustrates how to show IPv6 PIM RP-candidate information.

```
DmSwitch(config)#show ipv6 pim rp-candidate
```

RP Address	GroupPrefix	Priority	Timeout
2001:db8::1	ff07::/16	192	11349
Candidate-RP	GroupPrefixIdx	Priority	CandRpAdvTimeout
2001:db8::1	1	192	2349

```
DmSwitch(config)#
```

Related Commands

Command	Description
<code>ipv6 pim bootstrap rp-candidate</code>	Sets RP Candidate parameters.

show ip pim rps

show ip pim rps

Description

Shows configured PIM Rendezvous Points (RP) and their respective priorities, timeout values and group-prefixes.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command shows the information related to the configured Rendezvous Points on the router. It shows the type of them (static, BSR (Bootstrap Router) or EBSR (elected BSR)), priorities for the RP election, timeout values and group-prefix addresses.

Example

This example illustrates how to show PIM RPs information.

```
DmSwitch(config)#show ip pim rps
```

RP	Type	Pri	Timeout	GroupPrefix
10.42.5.142	static			224.0.0.0/4
10.42.5.142	static			232.0.0.0/8
10.42.8.151	bsr	192	5110	
10.42.8.151	ebsr	192	14104	224.0.0.0/4

```
DmSwitch(config)#
```

Related Commands

Command	Description
<code>ip pim rp-address</code>	Configures static RP-Address for PIM protocol.
<code>ip pim bootstrap</code>	Sets RP Candidate parameters.
<code>rp-candidate</code>	

show ipv6 pim rps

```
show ipv6 pim rps
```

Description

Shows configured IPv6 PIM Rendezvous Points (RP) and their respective priorities, timeout values and group-prefixes.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command shows the information related to the configured IPv6 Rendezvous Points on the router. It shows the type of them (static, BSR (Bootstrap Router) or EBSR (elected BSR)), priorities for the RP election, timeout values and group-prefix addresses.

Example

This example illustrates how to show IPv6 PIM RPs information.

```
DmSwitch(config)#show ipv6 pim rps
```

RP	Type	Pri	Timeout	GroupPrefix
2001:db8::1	static			ff00::/8
2001:db8::1	static			ff3e::/32
2001:db8::2	bsr	192	177	
2001:db8::2	ebsr	192	9177	ff07::/24

```
DmSwitch(config)#
```

Related Commands

Command	Description
<code>ipv6 pim rp-address</code>	Configures static RP-Address for IPv6 PIM protocol.
<code>ipv6 pim bootstrap</code>	Sets RP Candidate parameters.
<code>rp-candidate</code>	

show ip rip

show ip rip

Description

Shows the RIP process parameters.

Syntax

No parameter accepted.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the RIP information.

```
DmSwitch#show ip rip
```

```
Routing Protocol RIPv2
```

```
  Sending updates every 30 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Admin.Status: up      Oper.Status: up
```

Vlan	IfAddr	SentUp	BadPck	BadRoutes	AuthType	Metric	Passive
100	10.10.10.1	0	0	0	disabled	0	yes
200	20.20.20.1	0	0	0	disabled	0	yes

```
DmSwitch#
```

Related Commands

Command	Description
<code>clear ip rip process</code>	Clear RIP routing data.
<code>default-metric</code>	Defines the default metric of RIP protocol.
<code>distance</code>	Defines the administrative distance of RIP protocol.
<code>network</code>	Associates a network with a RIP routing process.
<code>passive-interface</code>	Suppresses RIP routing updates on specified VLAN interfaces.
<code>redistribute</code>	Redistributes routes with a metric of RIP protocol.
<code>router rip</code>	Enables and accesses the RIP configuration.
<code>show ip rip neighbor</code>	Shows RIP neighbors
<code>show running-config</code>	Shows the current operating configuration.
<code>timers basic</code>	Defines the basic timers of RIP protocol.

show ip rip neighbor

```
show ip rip neighbor
```

Description

Shows RIP neighbors.

Syntax

No parameter accepted.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.4.2	This command was introduced.

Usage Guidelines

This command will show the neighbors detected by RIP. It is important to note that RIP will only detect a neighbor if it receives a RIP message from that neighbor. This means that even if there is a usable RIP adjacency formed, it will not show up as a RIP neighbor until this router receives any RIP messages from that adjacency.

Example

This example illustrates how to show the RIP neighbors.

```
DmSwitch#show ip rip neighbor
Routing Protocol RIP Neighbor

Neighbor          Domain LastUp BadPck BadRoutes Version Bfd
-----
10.10.10.2         0      226    0      0          2      0

DmSwitch#
```

Related Commands

Command	Description
<code>clear ip rip process</code>	Clear RIP routing data.
<code>default-metric</code>	Defines the default metric of RIP protocol.
<code>distance</code>	Defines the administrative distance of RIP protocol.
<code>network</code>	Associates a network with a RIP routing process.
<code>passive-interface</code>	Suppresses RIP routing updates on specified VLAN interfaces.
<code>redistribute</code>	Redistributes routes with a metric of RIP protocol.
<code>router rip</code>	Enables and accesses the RIP configuration.
<code>show ip rip</code>	Shows the RIP process parameters.
<code>show running-config</code>	Shows the current operating configuration.
<code>timers basic</code>	Defines the basic timers of RIP protocol.

show ipv6 ripng

```
show ipv6 ripng [ database | neighbors ]
```

Description

Shows the RIPng process parameters.

Syntax

Parameter	Description
database	(Optional) Display RIPng routing table entries information.
neighbors	(Optional) Display RIPng neighbors information.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the RIPng information.

```
DmSwitch#show ipv6 ripng
```

```
Routing Protocol RIPng
```

```
Administrative status: UP
```

```
Operational status: UP
```

```

Equal Cost Multi-Path (ECMP) support is disabled
Sending updates every 30 seconds
Timeout after 180 seconds
Garbage collect after 120 seconds
DmSwitch#

```

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

show ipv6 ripng neighbors

show ipv6 ripng neighbors

Description

Shows RIPng neighbors.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command will show the neighbors detected by RIPng. It is important to note that RIPng will only detect a neighbor if it receives a RIPng message from that neighbor. This means that even if there is a usable RIPng adjacency formed, it will not show up as a RIPng neighbor until this router receives any RIPng messages from that adjacency.

Example

This example illustrates how to show the RIPng neighbors.

```
DmSwitch#show ipv6 ripng neighbors
Routing Protocol RIPng Neighbor
```

Neighbor	LastUp	BadPck	BadRoutes	Version	BFD
-----	-----	-----	-----	-----	-----
fe80::204:dfff:fe17:5d8f	7919	0	0	1	0

```
DmSwitch#
```

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

show ipv6 ripng database

show ipv6 ripng database

Description

Shows RIPng database.

Default

No default is defined.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command will show information about the interfaces with RIPng enabled.

Example

This example illustrates how to show the RIPng database.

```
DmSwitch#show ipv6 ripng database
Routing Protocol RIPng Database
```

Vlan	Addr	SentUp	BadPck	BadRoutes	Metric	Passive
100	2001:db8:100::/64	0	0	0	0	no

```
DmSwitch#
```

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.

Command	Description
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

show ip route

show ip route [*parameter*] | [*parameter*] ...

Description

Shows the IP routing table.

Syntax

Parameter	Description
active	Shows active routes.
bgp	Shows the BGP routes.
connect	Shows the connected routes.
destination { <i>ip address/mask</i> }	Shows the routes associated with the given ip address and mask.
destination { <i>ip address</i> }	Shows the routes associated with the given ip address.
gateway { <i>ip address</i> }	Shows the routes associated with the given gateway address.
ospf	Shows the OSPF routes.
out-iface-vlan { <i>vlan id</i> }	Shows the routes associated with the given vlan.
rip	Shows the RIP routes.
summary	Shows the number of routes installed.
static	Shows the number of routes installed.
vrf { <i>table name</i> }	Show VRF table for given name.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows all routes and using the *parameters* is possible to filter the routes results.

Example

This example illustrates how to show the IP routing table.

```
DmSwitch#show ip route
```

Codes: AD - Administrative Distance

Destination/Mask	Gateway	Protocol	AD/Cost	Output Interface	Status
0.0.0.0/0	172.16.1.254	static	0/0	mgmt-eth	Active
100.100.100.1/32	0.0.0.0	connect	0/0	-	Active
172.16.30.0/29	172.16.30.1	connect	0/0	VLAN 300	Active
172.16.30.1/32	0.0.0.0	connect	0/0	-	Active

DmSwitch#

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
ip route	Adds a static route to the routing table.
ip routing	Enables the IP routing.
show ip routing	Shows the IP routing table.

show ip route pbr

show ip route pbr [**seq** *sequence*]

Description

Shows the PBR sequence entries.

Syntax

Parameter	Description
<i>sequence</i>	PBR sequence number.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

This command shows the PBR sequence entries.

Example

Ex.1 - This example illustrates how to show all PBR sequence entries

```
DmSwitch#show ip route pbr
PBR SEQ 1 : enabled
  Action:   next-hop      172.16.95.9
            match src-interface ethernet range 1/1 1/5
            source-ip     172.16.96.34/29
            destination-ip 172.16.97.57/29
  HW status: installed
PBR SEQ 2 : enabled
  Action:   l3-routing
            match src-interface ethernet range 1/1 1/48
            source-ip     172.16.96.12/29
            destination-ip 192.168.0.1/24
  HW status: installed
```

DmSwitch#

Ex.2 - This example illustrates how to show a specific PBR sequence entry

```
DmSwitch#show ip route pbr seq 1
PBR SEQ 1 : enabled
  Action:      next-hop      172.16.95.9
               match src-interface ethernet range 1/1 1/5
               source-ip      172.16.96.34/29
               destination-ip 172.16.97.57/29
  HW status:   installed

DmSwitch#
```

Related Commands

Command	Description
ip route pbr	Enables the IP Route PBR configuration mode.
action	Set action rule for PBR sequence.
description	Set description for PBR sequence.
match dest-ip	Set destination IP address for PBR sequence.
match src-interface	Set source interface for PBR sequence.
match src-ip	Set source IP address for PBR sequence.

show ipv6 route

show ipv6 route

Description

Shows the IPv6 routing table.

Syntax

No parameter accepted.

Parameter	Description
active	Shows active routes.
connect	Shows the connected routes.
destination { <i>ipv6 address/mask</i> }	Shows the routes associated with the given ipv6 address and mask.
destination { <i>ipv6 address</i> }	Shows the routes associated with the given ipv6 address.
gateway { <i>ipv6 address</i> }	Shows the routes associated with the given gateway address.
out-iface-vlan { <i>vlan id</i> }	Shows the routes associated with the given vlan.
summary	Shows the number of routes installed.
static	Shows the number of routes installed.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command shows all IPv6 routes and using the *parameters* is possible to filter the routes results.

Example

This example illustrates how to show the IPv6 routing table.

```
DmSwitch#show ipv6 route
```

Codes: AD - Administrative Distance

Destination/Mask	Gateway	Protocol	AD/Cost	Output Interface	Status
-----	-----	-----	-----	-----	-----
12a0::/64	0db1::204:dfff:fe13	connect	0/0	VLAN 690	Active
0c1a::204:dfff/128	::	connect	0/0	-	Active
af5b::/64	fa42::204:dfff:fe13	connect	0/0	VLAN 680	Active
ad14::204:dfff/128	::	connect	0/0	-	Active
::/64	::/64	static	0/0	-	Inactive

```
DmSwitch#
```


show ip route vrf

show ip route vrf *vrf-name*

Description

Shows the Routing Information Base (RIB) associated to the specified VRF instance.

Syntax

Parameter	Description
<i>vrf-name</i>	Name assigned to a VRF.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
10.0	Changed example output to fit this release.

Usage Guidelines

This command shows the RIB associated to the VRF instance, including information about how the route was learned. Both IPv4 and VPNv4 routes are displayed together.

Example

This example illustrates how to show the RIB of a VRF instance.

```
DmSwitch#show ip route vrf vpn1
```

Codes: AD - Administrative Distance

Destination/Mask	Gateway	Protocol	AD/Cost	Output Interface	Status
-----	-----	-----	-----	-----	-----
100.200.101.0/24	2.3.4.5	bgp	200/0	DmSwitch_Tnn12	Active
172.16.49.0/29	172.16.49.1	connect	0/0	VLAN 490	Active
172.16.49.1/32	0.0.0.0	connect	0/0	-	Active

```
DmSwitch(config)#
```

Related Commands

Command	Description
<code>show ip vrf</code>	Shows VRF general information.
<code>show ip hardware vrf-table</code>	Shows the FIB of the specified VRF.

show ip routing

`show ip routing [multipath]`

Description

Shows the routing status.

Syntax

Parameter	Description
<code>multipath</code>	(Optional) Show Multipath configuration.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
7.6	The option <code>multipath</code> was introduced.

Usage Guidelines

Entering this command without parameters, all IP routing will be showed.

Example

This example illustrates how to show the routing status.

```
DmSwitch#show ip routing
IP routing is enabled

Multipath is disabled

DmSwitch#
```

Related Commands

Command	Description
<code>ip route</code>	Adds a static route to the routing table.
<code>ip routing</code>	Enables the IP routing.
<code>show ip route</code>	Shows the IP routing table.

show ip snmp-server

```
show ip snmp-server [ traps ]
```

Description

Shows the SNMP server information.

Syntax

Parameter	Description
traps	(Optional) Click here to see the "traps" parameter description.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the SNMP server status (enabled or disabled), the communities and users configured, the traps recipient hosts and the version of SNMP protocol used for the communication.

Entering this command without parameters, SNMP server information will be shown.

Example

This example illustrates how to show the SNMP server information.

```
DmSwitch#show ip snmp-server
SNMP status: Enable
```

```
Local SNMP engineID: 80000E7D030004DF006A79
```

```
SNMP Community:
  public (Read-Only)
```

```
SNMPv3 User:
  USER          ACCESS      AUTHENTICATION  PRIVACY
  manager       Read/Write   MD5             AES

SNMPv(1|2c) Trap Manager:
  IP            COMMUNITY    VERSION
  10.1.1.10     management  2c

SNMPv3 Trap Manager:
  IP            USER        AUTHENTICATION  PRIVACY
  10.1.1.11     manager    MD5             AES

DmSwitch#
```

Related Commands

Command	Description
ip snmp-server	Configures the internal SNMP server.
ip snmp-server traps	Enables sending of SNMP traps.

show ip snmp-server traps

show ip snmp-server traps

Description

Shows the SNMP traps status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the SNMP traps status.

```
DmSwitch#show ip snmp-server traps
TRAP                                STATUS
alarm-status-change                 enable
authentication                       enable
cold-warm-start                     enable
config-change                       enable
config-save                         enable
critical-event-detected              enable
critical-event-recovered             enable
duplicated-ip                       enable
fan-status-change                   enable
forbidden-access                    enable
link-flap-detected                  enable
link-flap-no-more-detected          enable
link-up-down                        enable
login-fail                          enable
login-success                       enable
loopback-detected                   enable
loopback-no-more-detected           enable
```

```
power-status-change      enable
sfp-presence             enable
stack-attach             enable
stack-detach             enable
traps-lost               enable
unidir-link-detected     enable
unidir-link-recovered    enable
```

DmSwitch#

Related Commands

Command	Description
ip snmp-server	Configures the internal SNMP server.

show ip ssh

show ip ssh

Description

Shows the SSH server information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
15.0	Information about Legacy support was introduced.
15.0	DSA and RSA fingerprint algorithm changed from MD5 to SHA256 and format from hexadecimal to Base64.

Usage Guidelines

This command shows the SSH server status (enabled or disabled), its timeout, the generated host key pair and the limit client connections.

Example

This example illustrates how to show the SSH server information.

```
DmSwitch#show ip ssh
SSH Enabled
  Legacy support:      Disabled
  Timeout:             120
  Fingerprints:
    DSA: SHA256: sTWKvv/4AG/EgE0xAA1Eneyce/ktqJtGgLUblQsJN1A
    RSA: SHA256: X2SpI5f1VvFN0DV3plwaaMBVIawB6seQHzc4u0+l0bo
  SSH connections limit: 8

DmSwitch#
```

Related Commands

Command	Description
<code>ip ssh</code>	Configures the internal SSH server for external access.

show ip telnet

show ip telnet

Description

Shows the Telnet server information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the Telnet server status (enabled or disabled) and the maximum connections allowed for Telnet clients.

Example

This example illustrates how to show the Telnet server information.

```
DmSwitch#show ip telnet
Telnet status:          Enable
Telnet connections limit: 8

DmSwitch#
```

Related Commands

Command	Description
ip telnet	Configures the internal Telnet server for external access.

show ip tftp

show ip tftp

Description

Shows the TFTP client information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command shows the TFTP client options.

Example

This example illustrates how to show the TFTP client information.

```
DmSwitch#show ip tftp
TFTP client source interface: VLAN 1

DmSwitch#
```

Related Commands

Command	Description
ip tftp	Configures the internal TFTP client options.

show ip vrf

show ip vrf [*vrf-name*]

Description

Shows VRF general information.

Syntax

Parameter	Description
<i>vrf-name</i>	Name assigned to VRF

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

This command shows the general information about the specified VRF. In the absence of *vrf-name*, all VRFs are displayed.

Example

This example illustrates how to show the information about a VRF.

```
DmSwitch(config)#show ip vrf vrf1
VRF:                vrf1
Route Distinguisher: 65123:1
Route Target
Both:                65123:3
Export:              (none)
Import:              (none)
MPLS label:         500000

DmSwitch(config)#
```

Related Commands

Command	Description
<code>ip vrf</code>	Enables the VRF configuration mode.
<code>ip vrf forwarding</code>	Configures the selected VLAN to use the specified VRF instance.
<code>rd</code>	Specifies the route distinguisher for a VRF instance.
<code>import-map</code>	Associates an import route map with the VRF instance.
<code>route-target</code>	Creates a route-target extended community for a VRF instance.
<code>show ip route vrf</code>	Shows the RIB of the specified VRF.
<code>show ip vrf</code>	Shows VRF general information.
<code>show vlan</code>	Shows the Virtual LAN settings.

show ip-tunnel

show ip-tunnel [**id index** | **range IDs**]

Description

Shows general informations about IP Tunnel entries.

Syntax

Parameter	Description
id index	(Optional) Filter table by IP Tunnel ID. Value between 1 and 64.
range IDs	(Optional) Filter table by a range of IDs. (Range: 1-64)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command shows IP Tunnel entries configurations and informations about tunnel status.

Example

This example illustrates how to show IP Tunnel table.

```
DmSwitch(config)#show ip-tunnel
```

IP-Tunnel ID	Type	Source	Destination	Adm/Oper
1	ipv6ip	lo 0	200.200.200.2	up/down
3	ipv6ip	VLAN 951	200.200.200.2	up/down
4	ipv6ip	lo 1	200.200.200.2	up/down
5	-	-	-	down/down
62	-	-	-	down/down
64	ipv6ip	lo 0	200.200.200.3	up/down

Table entries: 6

DmSwitch(config)#

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show isis

```
show isis { database [ detail ] | neighbors [ detail ] }
```

Description

Displays the isis information.

Syntax

Parameter	Description
database [detail]	Displays IS-IS Database Information.
neighbors [detail]	Displays IS-IS Neighbors List.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

In order to use this command is necessary to enter one of the command parameters.

Examples

This example illustrates how to show the IS-IS database information

```
DmSwitch#show isis database
```

```
Area al:
IS-IS Level 1 Link State Database
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
-----
DM4001-33.00-00      0x00000067  0xD038        1006          0/0/0
DM4001-33.00-01      0x0000006B  0x8E81        0414          0/0/0
DM4001-33.00-02      0x00000068  0x0410        0720          0/0/0
DM4001-33.01-00      0x00000068  0x8D50        0603          0/0/0
DM4001-14.00-00      0x00000067  0xC83F        0855          0/0/0
DM4001-14.00-01      0x00000065  0x3AED        0681          0/0/0
```

```

DM4001-14.00-02      0x00000065  0xF71F      0532      0/0/0
router-cisco.00-00   0x00000237  0x5FD8      0880      0/0/0

```

IS-IS Level 2 Link State Database

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
DM4001-33.00-00	0x00000067	0xD038	1059	0/0/0
DM4001-33.00-01	0x0000006C	0x14E4	0701	0/0/0
DM4001-33.00-02	0x00000067	0x060F	0831	0/0/0
DM4001-14.00-00	0x00000067	0xC83F	0779	0/0/0
DM4001-14.00-01	0x00000069	0x5AC7	1134	0/0/0
DM4001-14.00-02	0x00000067	0xF321	1150	0/0/0
router-cisco.00-00	0x00000232	0xD169	0669	0/0/0
router-cisco.01-00	0x0000022B	0xC359	0994	0/0/0

DmSwitch#show isis database detail

Area al:

IS-IS Level 1 Link State Database

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
DM4001-33.00-00	0x00000067	0xD038	0998	0/0/0
Length: 5				
NLPID: 0xCC				
Area Address(es): 49.0001				
DM4001-33.00-01	0x0000006B	0x8E81	0406	0/0/0
Ip Address: 10.1.12.1				
Metric: 20 IS DM4001-33.01				
Metric: 20 IP 10.1.12.0 255.255.255.0				
DM4001-33.00-02	0x00000068	0x0410	0712	0/0/0
Hostname: DM4001-33				
DM4001-33.01-00	0x00000068	0x8D50	0595	0/0/0
Metric: 0 IS DM4001-33.00				
Metric: 0 IS DM4001-33.00				
Metric: 0 IS DM4001-33.00				
DM4001-14.00-00	0x00000067	0xC83F	0847	0/0/0
Length: 5				
NLPID: 0xCC				
Area Address(es): 49.0001				
DM4001-14.00-01	0x00000065	0x3AED	0673	0/0/0
Ip Address: 10.1.12.2				
Metric: 10 IS DM4001-14.01				
Metric: 10 IP 10.1.12.0 255.255.255.0				
DM4001-14.00-02	0x00000065	0xF71F	0524	0/0/0
Hostname: DM4001-14				
router-cisco.00-00	0x00000237	0x5FD8	0872	0/0/0
Area Address(es): 49.0001				
NLPID: 0xCC				
Hostname: router-cisco				
Ip Address: 10.1.12.3				
Metric: 10 IP 10.1.12.0 255.255.255.0				
Metric: 10 IS router-cisco.01				

IS-IS Level 2 Link State Database

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
DM4001-33.00-00	0x00000067	0xD038	1051	0/0/0
Length: 5				
NLPID: 0xCC				
Area Address(es): 49.0001				
DM4001-33.00-01	0x0000006C	0x14E4	0693	0/0/0
Ip Address: 10.1.12.1				
Metric: 30 IS DM4001-33.01				
Metric: 30 IP 10.1.12.0 255.255.255.0				
DM4001-33.00-02	0x00000067	0x060F	0823	0/0/0

```

      Hostname: DM4001-33
DM4001-14.00-00      0x00000067      0xC83F      0771      0/0/0
      Length: 5
      NLPID: 0xCC
      Area Address(es): 49.0001
DM4001-14.00-01      0x00000069      0x5AC7      1126      0/0/0
      Ip Address: 10.1.12.2
      Metric: 10      IS DM4001-14.01
      Metric: 10      IP 10.1.12.0 255.255.255.0
DM4001-14.00-02      0x00000067      0xF321      1142      0/0/0
      Hostname: DM4001-14
router-cisco.00-00      0x00000232      0xD169      0661      0/0/0
      Area Address(es): 49.0001
      NLPID: 0xCC
      Hostname: router-cisco
      Ip Address: 10.1.12.3
      Metric: 10      IS router-cisco.01
      Metric: 10      IP 10.1.12.0 255.255.255.0
router-cisco.01-00      0x0000022B      0xC359      0986      0/0/0
      Metric: 0      IS router-cisco.00

```

This example illustrates how to show the information concerning the IS-IS neighbors. The "Circuit Id" field shows the DIS (Designated Intermediate System) for the interface and adjacency type (L1 or L2).

```
DmSwitch#show isis neighbors
```

```

Area al:
System ID      Type      Interface      Ip Address      State      Holdtime      Circuit Id
-----
0000.0000.0003 L1      251      10.1.12.3      UP      25      0000.0000.0001.01
0000.0000.0003 L2      251      10.1.12.3      UP      8      0000.0000.0003.01
0000.0000.0002 L1      251      10.1.12.2      UP      28      0000.0000.0001.01
0000.0000.0002 L2      251      10.1.12.2      UP      29      0000.0000.0003.01

```

```
DmSwitch#show isis neighbors detail
```

```

Area al:
System ID      Type      Interface      Ip Address      State      Holdtime      Circuit Id
-----
0000.0000.0003 L1      251      10.1.12.3      UP      28      0000.0000.0001.01
Area Address(es): 49.0001
SNPA: ca00.72d2.001d
State Changed: 13:01:05
LAN Priority: 80
Interface Name: vlan 251
Graceful Restart: capable/not restarting
0000.0000.0003 L2      251      10.1.12.3      UP      8      0000.0000.0003.01
Area Address(es): 49.0001
SNPA: ca00.72d2.001d
State Changed: 13:03:03
LAN Priority: 80
Interface Name: vlan 251
Graceful Restart: capable/not restarting
0000.0000.0002 L1      251      10.1.12.2      UP      28      0000.0000.0001.01
Area Address(es): 49.0001
SNPA: 0004.df15.c359
State Changed: 00:53:17
LAN Priority: 80
Interface Name: vlan 251
Graceful Restart: capable/not restarting
0000.0000.0002 L2      251      10.1.12.2      UP      28      0000.0000.0003.01
Area Address(es): 49.0001

```

```

SNPA: 0004.df15.c359
State Changed: 00:53:17
LAN Priority: 80
Interface Name: vlan 251
Graceful Restart: capable/not restarting

```

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
isis metric	Configure the IS-IS metric in a VLAN
isis metric-wide	Configure the IS-IS wide metric in a VLAN
isis passive-interface	Configure interface as a passive IS-IS interface
lsp-gen-interval	Configure the maximum LSP generation interval for an IS-IS instance.
max-lsp-int	
lsp-gen-interval	Configure the minimum LSP generation interval for an IS-IS instance.
min-lsp-int	
metric-style	Configure the IS-IS metric style
router isis	Enables and accesses the IS-IS configuration.
summary-address	Configure summary-address for an IS-IS instance
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

show ipfix

show ipfix

Description

Shows IPFIX configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Example

This example illustrates how to show the IPFIX settings.

```
DmSwitch#show ipfix
```

```
Host configuration:
```

```
Host 1:
  Address:      172.16.0.1
  Port:         4739
Host 2:
  Address:      172.16.0.2
  Port:         4740
```

```
Flow configuration:
```

```
Flow:
  Sample rate (packet/s): 1
```

```
Interfaces enabled:
  Eth 2/1
  Eth 5/48
```

```
DmSwitch#
```

Related Commands

Command	Description
<code>ipfix host</code>	Configures an IPFIX collector.
<code>ipfix flow-trigger</code>	Configures IPFIX flow monitoring parameters.
<code>ipfix</code>	Enables IPFIX on an Ethernet Interface.

show l2protocol-tunnel

```
show l2protocol-tunnel [ interface { ethernet [ unit-number/ ] port-number |  
port-channel channel-group-number } ]
```

Description

Shows Layer 2 Protocols Tunneling information.

Syntax

Parameter	Description
interface	(Optional) Shows the information of a specific interface.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Shows information of a specific unit and port.
port-channel <i>channel-group-number</i>	Shows information of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Entering this command without parameters, the Layer 2 Protocols Tunneling information for all interfaces will be shown.

Example

This example illustrates how to show the tunneling configurations of a specific Ethernet port.

```
DmSwitch#show l2protocol-tunnel interface ethernet 1  
Eth 1/1  
  CDP packets tunneling: Disabled  
  STP packets tunneling: Enabled  
  VTP packets tunneling: Disabled  
  PVST packets tunneling: Disabled
```

```
UDLD packets tunneling: Disabled
PAgP packets tunneling: Disabled
LACP packets tunneling: Disabled
LLDP packets tunneling: Disabled
```

```
DmSwitch#
```

Related Commands

Command	Description
l2protocol-tunnel (Global configuration)	Configures a Layer 2 protocols tunneling.
l2protocol-tunnel (Interface configuration)	Configures Layer 2 protocols tunneling for the Ethernet interface.

show lacp counters

show lacp counters

Description

Shows the LACP traffic counters.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Changed output layout. Information are shown grouped by port-channel regardless of aggregation status.

Usage Guidelines

This command shows the transmitted and received LACPDUs, the transmitted and received marker and marker response, and the number of packets for which errors were detected.

Example

This example illustrates how to show the LACP traffic counters.

```
DmSwitch#show lacp counters
```

PortCh		Eth	LACPDUs		Marker		Marker Response		LACPDUs	
			Sent	Recv	Sent	Recv	Sent	Recv	Pkts	Err
3		1/1	8	9	0	0	0	0	0	
		1/2	8	9	0	0	0	0	0	

```
DmSwitch#
```

Related Commands

Command	Description
---------	-------------

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lacp	Enables use of LACP in port-channel.
show lacp internal	Shows the LACP internal information.
show lacp <i>port-channel</i>	Shows the LACP information by port-channel.
show lacp neighbors	Shows the LACP neighbors information.
show lacp sysid	Shows the system identifier used by LACP.

show lacp *port-channel*

show lacp *port-channel* { counters | internal | neighbors }

Description

Shows LACP information for the specified port-channel.

Output modifiers are available for this command.

Syntax

Parameter	Description
<i>port-channel</i>	Specifies the port-channel. (Range: 1-128)
counters	Shows the traffic counters.
internal	Shows the internal information.
neighbors	Shows the neighbors information.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Changed command syntax. Changed optional filtering from aggregator ID to port-channel index.

Usage Guidelines

Not available.

Example

This example illustrates how to show LACP counters only for a specific port-channel.

```
DmSwitch#show lacp 3 counters
          LACPDU      Marker      Marker Response      LACPDU
PortCh   | Eth   Sent   Recv   Sent   Recv   Sent   Recv   Pkts Err
-----
```

```
-----  
3      | 1/1  8    9    0    0    0    0  
      | 1/2  8    9    0    0    0    0  
  
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lacp	Enables use of LACP in port-channel.
show lacp counters	Shows the LACP traffic counters.
show lacp internal	Shows the LACP internal information.
show lacp neighbors	Shows the LACP neighbors information.
show lacp sysid	Shows the system identifier used by LACP.

show lacp internal

show lacp internal

Description

Shows the LACP internal information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Changed output layout. Information are shown grouped by port-channel regardless of aggregation status.

Usage Guidelines

This command shows the flags, priority, keys and the ports states for each port member of port-channels with LACP enabled in the DmSwitch.

Example

This example illustrates how to show the LACP internal information.

```
DmSwitch#show lacp internal
Flags: S-Device is requesting Slow LACPDUs F-Device is requesting Fast LACPDUs
       A-Device is in Active Mode           P-Device is in Passive Mode

Port state: A-LACP_Activity   T-LACP_Timeout  G-Aggregation  E-Expired
            S-Synchronization D-Distributing C-Collecting F-Defaulted

  PortCh  |  Eth    Flags  LACP port  Admin   Oper   Port
           |         |            Priority  Key      Key    State
-----|-----|-----|-----|-----|-----|-----
    3     |  1/1    SA     32768      0x0200  0x0203  AGSCD
           |  1/2    SA     32768      0x0200  0x0203  AGSCD

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lacp	Enables use of LACP in port-channel.
show lacp counters	Shows the LACP traffic counters.
show lacp <i>port-channel</i>	Shows the LACP information by port-channel.
show lacp neighbors	Shows the LACP neighbors information.
show lacp sysid	Shows the system identifier used by LACP.

show lacp neighbors

show lacp neighbors

Description

Shows the LACP neighbors information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Changed output layout. Information are shown grouped by port-channel regardless of aggregation status.

Usage Guidelines

This command shows the flags, priority, keys, the neighbor ports states and system identifier for port members of port-channels with LACP enabled.

Example

This example illustrates how to show the LACP neighbors.

```
DmSwitch#show lacp neighbors
Flags: S-Device is requesting Slow LACPDUs F-Device is requesting Fast LACPDUs
       A-Device is in Active Mode           P-Device is in Passive Mode
```

```
Port state: A-LACP_Activity   T-LACP_Timeout   G-Aggregation   E-Expired
             S-Synchronization D-Distributing C-Collecting   F-Defaulted
```

PortCh	Eth	Partner ID	Flags	LACP port Priority	Oper Key	Port Number	Port State
3	1/1	32768,00:04:DF:1B:6C:3D	SA	32768	0x0003	1	AGSCD
	1/2	32768,00:04:DF:1B:6C:3D	SA	32768	0x0003	2	AGSCD

```
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lacp	Enables use of LACP in port-channel.
show lacp counters	Shows the LACP traffic counters.
show lacp <i>port-channel</i>	Shows the LACP information by port-channel.
show lacp internal	Shows the LACP internal information.
show lacp sysid	Shows the system identifier used by LACP.

show lacp sysid

show lacp sysid

Description

Shows the system identifier used by LACP.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the system identifier used by LACP.

```
DmSwitch#show lacp sysid
32768,00:04:DF:61:25:4A

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lacp	Enables use of LACP in port-channel.
show lacp counters	Shows the LACP traffic counters.
show lacp port-channel	Shows the LACP information by port-channel.
show lacp internal	Shows the LACP internal information.

Command	Description
<code>show lacp neighbors</code>	Shows the LACP neighbors information.

show link-flap

show link-flap

Description

Shows link-flap information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the link-flap information.

```
DmSwitch#show link-flap
```

Port	Enable	Configuration			Detection		Unblock Timeout	Link Flap
		Flaps	Interv	Unblock	Flaps	Interv		
1/ 1	YES	10	20	30	0	----	-----	NO
1/ 2	YES	10	20	30	0	----	-----	NO
1/ 3	YES	10	20	30	0	----	-----	NO
1/ 4	YES	10	20	30	0	----	-----	NO
1/ 5	YES	10	20	30	0	----	-----	NO
1/ 6	YES	10	20	30	0	----	-----	NO
1/ 7	YES	10	20	30	0	----	-----	NO
1/ 8	YES	10	20	30	0	----	-----	NO
1/ 9	YES	10	20	30	0	----	-----	NO
1/10	YES	10	20	30	0	----	-----	NO
1/11	YES	10	20	30	0	----	-----	NO
1/12	YES	10	20	30	0	----	-----	NO
1/13	YES	10	20	30	0	----	-----	NO
1/14	YES	10	20	30	0	----	-----	NO
1/15	YES	10	20	30	0	----	-----	NO

1/16	YES	10	20	30	0	----	-----	NO
1/17	YES	10	20	30	0	----	-----	NO
1/18	YES	10	20	30	0	----	-----	NO
1/19	YES	10	20	30	0	----	-----	NO
1/20	YES	10	20	30	0	----	-----	NO
1/21	YES	10	20	30	0	----	-----	NO
1/22	YES	10	20	30	0	----	-----	NO
1/23	YES	10	20	30	0	----	-----	NO
1/24	YES	10	20	30	0	----	-----	NO
1/25	YES	10	40	30	0	----	-----	NO
1/26	YES	10	40	30	0	----	-----	NO
1/27	YES	10	40	30	0	----	-----	NO
1/28	YES	10	40	30	0	----	-----	NO

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
link-flap	Configures Link-Flap Detection for Ethernet interface

show link-state-tracking

show link-state-tracking [*groupID*]

Description

Shows Link-State Tracking status of all groups.

Syntax

Parameter	Description
<i>groupID</i>	Displays configuration and status information of a single group (groupID).

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Entering this command without parameters, all link-state groups status will be shown.

Example

This example illustrates how to show status and configuration of a single link-state tracking group.

```
DmSwitch#show link-state-tracking 1
```

```
DmSwitch#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

Command	Description
<code>link-state-tracking</code>	Creates and configures a Link-State Tracking Group.

show lldp

```
show lldp [ counters | neighbor ]
```

Description

Shows LLDP configuration information.

Output modifiers are available for this command.

Syntax

Parameter	Description
counters	(Optional) Click here to see the "counters" parameter description.
neighbor	(Optional) Click here to see the "neighbor" parameter description.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.
12.0	The optional command counters was introduced and the show output was modified.

Usage Guidelines

Entering this command without parameters, the LLDP configuration for all interfaces will be shown.

Example

This example illustrates how to show the LLDP configuration information.

```
DmSwitch#show lldp
```

```
Global configuration:
State                : enable
Transmit interval (sec):      30
```

```

Hold value:                4
Transmit delay (sec):      2
Notification interval (sec): 5
Reinit delay (sec):        2

```

Interface configuration:

Port	Admin Status	SNMP Notif.	Transmitted TLVs	Port	Admin Status	SNMP Notif.	Transmitted TLVs
mgmt	TX/RX	Disabled	PNDPCM	1/ 1	TX/RX	Disabled	PNDPCM
1/ 2	TX/RX	Disabled	PNDPCM	1/ 3	TX/RX	Disabled	PNDPCM
1/ 4	TX/RX	Disabled	PNDPCM	1/ 5	TX/RX	Disabled	-----
1/ 6	TX/RX	Disabled	-----	1/ 7	TX/RX	Disabled	-----
1/ 8	TX/RX	Disabled	-----	1/ 9	TX/RX	Disabled	-----
1/10	TX/RX	Disabled	-----	1/11	TX/RX	Disabled	-----
1/12	TX/RX	Disabled	-----	1/13	TX/RX	Disabled	-----
1/14	TX/RX	Disabled	-----	1/15	TX/RX	Disabled	-----
1/16	TX/RX	Disabled	-----	1/17	TX/RX	Disabled	-----
1/18	TX/RX	Disabled	-----	1/19	TX/RX	Disabled	-----
1/20	TX/RX	Disabled	-----	1/21	TX/RX	Disabled	-----
1/22	TX/RX	Disabled	-----	1/23	TX/RX	Disabled	-----
1/24	TX/RX	Disabled	-----	1/25	TX/RX	Disabled	-----
1/26	TX/RX	Disabled	PNDPCM				

Flags: (P) Port Description, (N) System Name, (D) System Description
(C) System Capabilities, (M) Mgmt Addr

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, (0.25 * transmit-interval), to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is transmit-interval * transmit-hold.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp counters	Shows LLDP counters information.

Command	Description
<code>show lldp neighbor</code>	Shows LLDP neighbor information.
<code>clear lldp</code>	Clears LLDP data.

show lldp counters

```
show lldp counters [ global | interface { ethernet [ unit-number ] port | mgmt-eth |  
port-channel port-channel-number } ]
```

Description

Shows LLDP counters information.

Syntax

Parameter	Description
global	Shows counters global information.
interface	Shows counters information of a specific interface.
ethernet	Shows counters information of a specific unit and port.
<i>unit-number</i>	Unit number.
<i>port-number</i>	Port number.
mgmt-eth	Shows counters information of the management ethernet.
port-channel	Shows counters information of a specific port-channel.
<i>port-channel-number</i>	Port channel number.

Default

No default is defined.

Commands Modes

User EXEC

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, the counters information for all interfaces will be shown.

Example

This example illustrates how to show the LLDP counters information of a specific port.

```
DmSwitch#show lldp counters interface ethernet 14  
Ethernet 1/14 counters:
```

```

Input frames:          158
Output frames:         158
Discarded frames:      0
Input frames with error: 0
Discarded TLVs:        0
Unrecognised TLVs:     0
Aged out neighbors:    39

```

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, (0.25 * transmit-interval), to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is transmit-interval * transmit-hold.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

show lldp neighbor

```
show lldp neighbor [ detail | interface { ethernet [ unit-number/ ] port-number |  
mgmt-eth | port-channel port-channel-number/ } ]
```

Description

Shows LLDP neighbor information.

Output modifiers are available for this command.

Syntax

Parameter	Description
output modifiers	Options to filter text output: after, begin, exclude and include
detail	(Optional) Shows all LLDP neighbors information detailedly.
interface	(Optional) Shows LLDP neighbor information of a specific interface.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Shows LLDP neighbor information of a specific unit and port.
mgmt-eth	Shows LLDP neighbor information of the management ethernet.
port-channel <i>port-channel-number</i>	Shows LLDP neighbor information of a specific port-channel.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.
12.0	The optionals detail and interface were added. The show output was modified.

Usage Guidelines

Entering this command without parameters, the neighbor information for all interfaces will be shown.

Example

This example illustrates how to show the LLDP neighbor information of a specific port.

```
DmSwitch#show lldp neighbor ethernet 5

*****
LLDP Eth 1/5      Total neighbors = 1

Neighbor:
Chassis ID (subtype 4):  00:04:DF:01:25:56
Port ID (subtype 5):     Port1
Time to live:            120
Port description:        ethernet 1/2
System name:             DM4000
System description:      DATACOM, DM4001, ETH24GX+2x10GX H Series, Version
11.2-dev
System capabilities:      Bridge*, Router,  (*Enabled capabilities)
Management Address:      Subtype 802 (6), Address 00:04:DF:01:25:56
Interface subtype ifIndex (2), number 1001
OID: 1.3.6.1.4.1.1.156.125.1.2.64

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, (0.25 * transmit-interval), to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is transmit-interval * transmit-hold.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.

show log

```
show log { flash | ram } [ all ] [ command | internal [ command ] ] [ tail | tail number_lines ]
```

Description

Shows log messages.

Output modifiers are available for this command.

Syntax

Parameter	Description
flash	Shows the 4000 last events stored in flash memory.
ram	Shows the 4000 last events stored in RAM memory.
all	(Optional) Shows all events stored.
command	(Optional) Shows events with the commands history. (The show commands aren't displayed)
internal	(Optional) Shows log messages with internal events. This option requires authentication.
tail	(Optional) Shows only the 10 last events.
tail number_lines	(Optional) Shows only the number_lines last events.(Range: 0-65535)

Default

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.0	The optional internal was introduced.
13.4	The optional all was introduced and the command "show log" displayed by default only the last 4000 lines of log.

Usage Guidelines

Not available.

Example

This example illustrates how to show the last logged events in flash memory.

```
DmSwitch#show log flash tail
Jan  5 23:00:48 swa : Interface ethernet 1/27 changed state to up
Jan  5 23:00:48 swa : Interface ethernet 1/27 changed state to down
Jan  5 23:00:50 swa : Interface ethernet 1/27 changed state to up
Jan  5 23:00:50 swa : Interface ethernet 1/27 changed state to down
Jan  1 00:01:00 DmSwitch : Unit 1: Power source 1 ok.
Jan  1 00:01:00 DmSwitch : Unit 1: Power source 1 ok.
Jan  1 00:01:00 DmSwitch : Unit 1: Power source 1 ok.
Jan  1 00:19:34 DmSwitch : CPU usage > 90%
Jan  1 00:27:52 DmSwitch : CPU usage < 90%
Jan  1 00:01:00 DmSwitch : Unit 1: Power source 1 ok.
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
clear logging	Deletes log messages.
logging facility	Sets the facility type for remote logging.
logging history	Configures the level of local events.
logging host	Configures a remote syslog server.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
logging on	Enables the logging of events.
logging sendmail	Enables and configures the sending of logs via e-mail.
logging trap	Configures the level of events that will be sent to remote syslog.
show logging	Shows logging configuration.

show logging

```
show logging { commands | debug | flash | ram | sendmail | terminal | trap }
```

Description

Shows logging configuration.

Syntax

Parameter	Description
commands	Shows the settings for storing command events.
debug	Shows the settings for debug messages logging.
flash	Shows the settings for storing events in flash memory.
ram	Shows the settings for storing events in RAM memory.
sendmail	Shows the settings for sending events through SMTP.
terminal	Shows the settings for displaying events on terminal.
trap	Shows the settings for remote logging.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
9.4	A new option (terminal) for this command was introduced.
11.2	A new option (commands) for this command was introduced.

Usage Guidelines

This command shows the logging settings for: storing events in flash or RAM, display them directly in the terminal, send by e-mail or to a remote host.

Example

This example illustrates how to show the settings of logging events in flash memory.

```
DmSwitch#show logging flash
```



```
          Syslog logging: Enabled
    History logging in flash: error (3)
DmSwitch#
```

Related Commands

Command	Description
clear logging	Deletes log messages.
logging facility	Sets the facility type for remote logging.
logging history	Configures the level of local events.
logging host	Configures a remote syslog server.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
logging on	Enables the logging of events.
logging sendmail	Enables and configures the sending of logs via e-mail.
logging trap	Configures the level of events that will be sent to remote syslog.
show log	Shows log messages.

show loopback-detection

`show loopback-detection`

Description

Shows loopback detection information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the loopback-detection information.

```
DmSwitch#show loopback-detection
```

Port	Enabled	Unblock-Time	Timeout	Blocked	Loopback
1/ 1	YES	30	--	NO	NO
1/ 2	YES	30	--	NO	NO
1/ 3	YES	30	--	NO	NO
1/ 4	YES	30	--	NO	NO
1/ 5	YES	30	--	NO	NO
1/ 6	YES	30	--	NO	NO
1/ 7	YES	30	--	NO	NO
1/ 8	YES	30	--	NO	NO
1/ 9	YES	30	--	NO	NO
1/10	YES	30	--	NO	NO
1/11	YES	30	--	NO	NO
1/12	YES	30	--	NO	NO
1/13	YES	30	--	NO	NO
1/14	YES	30	--	NO	NO
1/15	YES	30	--	NO	NO
1/16	YES	30	--	NO	NO

1/17	YES	30	--	NO	NO
1/18	YES	30	--	NO	NO
1/19	YES	30	--	NO	NO
1/20	YES	30	--	NO	NO
1/21	YES	30	--	NO	NO
1/22	YES	30	--	NO	NO
1/23	YES	30	--	NO	NO
1/24	YES	30	--	NO	NO
1/25	YES	30	--	NO	NO
1/26	YES	30	--	NO	NO
1/27	YES	30	--	NO	NO
1/28	YES	30	--	NO	NO

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
loopback-detection	Configures Loopback Detection for Ethernet interface

show mac-address-table

```
show mac-address-table [ address mac-address | hardware | interface { ethernet [ unit-number/ ] port-number | port-channel channel-group-number } | tftp ip-address filename | summary | unit unit-number | vlan index | multicast | vpn vpn-id ]
```

Description

Shows the MAC address table.

Syntax

Parameter	Description
address <i>mac-address</i>	(Optional) Shows the table filtering by an address.
hardware	(Optional) Shows hardware MAC address table.
interface	(Optional) Shows the table filtering by a specific interface.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Shows the table filtering by a specific unit and port.
multicast	(Optional) Shows only multicast entries.
port-channel <i>channel-group-number</i>	Shows the table filtering by a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
unit <i>unit-number</i>	(Optional) Shows the table filtering by a specific unit.
vlan <i>index</i>	(Optional) Shows the table filtering by a VLAN ID. (Range: 1-4094)
summary	(Optional) Show the number of entries by given filtering criteria
tftp <i>ip-address filename</i>	(Optional) Send output to TFTP server. This command may take several minutes in case of MAC address table fully loaded.
vpn <i>vpn-id</i>	(Optional) Shows the table filtering by a VPN identifier.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
10.0	The vpn filtering was introduced.

Release	Modification
13.0	Summary was introduced.
13.4	Added support for multicast entries.
13.4	The option hardware was introduced. The default behaviour was changed to display only MAC addresses learned in frontal ports. Please use the new option to show a complete version of MAC address table, considering all entries from hardware.

Usage Guidelines

Multicast addresses are also displayed on the table. Each output port from a multicast entry is shown in a separate line.

Usage Guidelines for stacking or chassis

This command will display only MAC addresses learned in frontal ports. To display a complete version of MAC address table, considering all internal entries that are currently in the hardware, please use the **hardware** option.

Static MAC addresses for Port-channels are shown and counted for all units.

Example

This example illustrates how to show the MAC address table filtered by a VLAN index.

```
DmSwitch#show mac-address-table vlan 1
Total MAC Addresses for this criterion: 8
```

Unit	Block	Interface	MAC Address	VLAN	VPN	Type
1	1-26	Eth 1/ 1	00-13-20-1F-94-85	1	-	Learned
1	1-26	Eth 1/ 1	01-02-03-04-05-06	1	-	Static
1	1-26	Eth 1/12	00-0C-F1-AC-92-87	1	-	Learned
1	1-26	Eth 1/12	00-0C-F1-AC-92-F0	1	-	Learned
1	1-26	Eth 1/12	00-12-A9-E4-1E-A5	1	-	Learned
1	1-26	Eth 1/12	00-15-F2-59-B1-07	1	-	Learned
1	1-26	Eth 1/12	00-15-F2-BC-D4-EE	1	-	Learned
1	1-26	Eth 1/12	00-E0-63-C4-C4-28	1	-	Learned

```
DmSwitch#
```

This example illustrates how to show the MAC address table.

```
DmSwitch#show mac-address-table
This command may take a while...
Total MAC Addresses for this criterion: 16
```

Unit	Block	Interface	MAC Address	VLAN	VPN	Type
2	1-24	Eth 2/ 2	00:03:03:03:03:02	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:03	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:04	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:01	1	-	Learned
3	1-26	Eth 3/ 2	00:02:02:02:02:03	1	-	Learned
3	1-26	Eth 3/ 2	00:02:02:02:02:04	1	-	Learned

```

3 1-26 Eth 3/ 2 00:02:02:02:02:01 1 - Learned
3 1-26 Eth 3/ 2 00:02:02:02:02:02 1 - Learned

```

MAC entries reserved for system internal use, not listed above: 8
DmSwitch#

This example illustrates how to show same table with the hardware option.

```

DmSwitch#show mac-address-table hardware
This command may take a while...
Total MAC Addresses for this criterion: 24

```

Unit	Block	Interface	MAC Address	VLAN	VPN	Type
2	1-24	Eth 3/ 2	00:02:02:02:02:02	1	-	Learned
2	1-24	Eth 3/ 2	00:02:02:02:02:03	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:02	1	-	Learned
2	1-24	Eth 3/ 2	00:02:02:02:02:04	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:03	1	-	Learned
2	1-24	Eth 3/ 2	00:02:02:02:02:01	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:04	1	-	Learned
2	1-24	Eth 2/ 2	00:03:03:03:03:01	1	-	Learned
3	1-26	Eth 3/ 2	00:02:02:02:02:03	1	-	Learned
3	1-26	Eth 3/ 2	00:02:02:02:02:04	1	-	Learned
3	1-26	Eth 3/ 2	00:02:02:02:02:01	1	-	Learned
3	1-26	Eth 3/ 2	00:02:02:02:02:02	1	-	Learned
3	1-26	Eth 2/ 2	00:03:03:03:03:02	1	-	Learned
3	1-26	Eth 2/ 2	00:03:03:03:03:03	1	-	Learned
3	1-26	Eth 2/ 2	00:03:03:03:03:04	1	-	Learned
3	1-26	Eth 2/ 2	00:03:03:03:03:01	1	-	Learned

MAC entries reserved for system internal use, not listed above: 8
DmSwitch#

Related Commands

Command	Description
show mac-address-table aging-time	Shows the MAC address table aging time configuration.
show mac-address-table sort	Shows sorted MAC address table.
show mac-address-table summary	Shows summary MAC address table.
show mac-address-table usage	Shows usage of MAC address table.
mac-address-table static	Adds a static address to MAC address table.

show mac-address-table aging-time

show mac-address-table aging-time

Description

Shows the MAC address table aging time configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the aging time configuration.

```
DmSwitch#show mac-address-table aging-time
Aging mode: global.
Global aging time: 300 sec.
DmSwitch#
```

Related Commands

Command	Description
mac-address-table aging-time (Global configuration)	Sets the aging time for MAC address table entries.
show mac-address-table	Shows the MAC address table.

Command	Description
<code>show mac-address-table sort</code>	Shows sorted MAC address table.
<code>show mac-address-table summary</code>	Shows summary MAC address table.
<code>show mac-address-table usage</code>	Shows usage of MAC address table.

show mac-address-table sort

show mac-address-table sort

Description

Shows sorted MAC address table.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the sorted MAC address table.

```
DmSwitch#show mac-address-table sort
This command may take a while...
Total MAC Addresses for this criterion: 3

Unit Block Interface MAC Address      VLAN Type
-----
  1      Eth  1/ 1 00:01:02:03:04:01    1 Static
  1      Eth  1/ 1 00:01:02:03:04:05    1 Static
  1      Eth  1/ 1 00:01:02:03:04:06    1 Static

DmSwitch#
```

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table.
show mac-address-table aging-time	Shows the MAC address table aging time configuration.
show mac-address-table summary	Shows summary MAC address table.
show mac-address-table usage	Shows usage of MAC address table.
mac-address-table static	Adds a static address to MAC address table.

show mac-address-table summary

show mac-address-table summary

Description

Shows summary MAC address table.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the summarized MAC address table.

```
DmSwitch#show mac-address-table summary
```

```
This command may take a while...
Total MAC Addresses for this criterion: 3
```

```
DmSwitch#
```

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table.
show mac-address-table aging-time	Shows the MAC address table aging time configuration.

Command	Description
<code>show mac-address-table sort</code>	Shows sorted MAC address table.
<code>show mac-address-table usage</code>	Shows usage of MAC address table.
<code>mac-address-table static</code>	Adds a static address to MAC address table.

show mac-address-table usage

`show mac-address-table usage`

Description

Shows usage of hardware resources of MAC address table for each unit of the system.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command may take some time to display the requested information, depending on the number units and amount of entries of each unit.

For hardware models without external L2 memory, this command will only display resources of internal memory. For hardware models with internal and external memories, both are considered by this command.

Please note that total number of available entries depends on the hardware model and configuration of external memory partitioning.

For hardware models with internal and enabled external memories, internal memory is used for system entries, static entries and specific feature entries.

This command consider hardware resources, so the total number of entries differs from **show mac-address-table** in chassis or stack configuration. To verify all entries in hardware, use command **show mac-address-table hardware**.

Example

This example illustrates how to show the usage of MAC address table.

```
DmSwitch#show mac-address-table usage
This command may take a while...
```

```

          MAC Address Table
Unit  Block  Total    Used    (%)
-----
   1    1-48  32768   13057   39
```

```
DmSwitch#
```

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table.
show mac-address-table aging-time	Shows the MAC address table aging time configuration.
show mac-address-table sort	Shows sorted MAC address table.
show mac-address-table summary	Shows summary MAC address table.
memory external	Configures external memory partitioning.
mac-address-table static	Adds a static address to MAC address table.

show management

```
show management { all-client | http-client | snmp-client | telnet-client |  
ssh-client }
```

Description

Shows the management IP filters.

Output modifiers are available for this command.

Syntax

Parameter	Description
all-client	Shows the clients IP addresses to HTTP, SNMP, SSH and Telnet internal servers.
http-client	Shows the clients IP addresses to HTTP internal server.
snmp-client	Shows the clients IP addresses to SNMP internal server.
telnet-client	Shows the clients IP addresses to SSH internal server.
ssh-client	Shows the clients IP addresses to Telnet internal server.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show all clients IP addresses.

```
DmSwitch#show management all-client  
Management IP filter:
```

```
Telnet client:
  10.11.12.22/32
  10.11.13.22/32

HTTP client:
  10.11.12.22/32
  10.11.13.22/32

SNMP client:
  10.11.12.22/32
  10.11.13.22/32

SSH client:
  10.11.12.22/32
  10.11.13.22/32

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
management	Filters client IP address that tries to access internal servers.

show managers

show managers

Description

Shows the connected managers using terminals.
Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the connected managers.

```
DmSwitch#show managers
User on CLI      Uptime
admin            3 d, 3 h, 21 m, 59 s
test_user        7 h, 55 m, 27 s
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
username	Creates users and configures access to the DmSwitch.

show memory

```
show memory { external | internal | usage }
```

Description

Shows memory configuration. This command prints the number of entries and the partitioning percentage available for MAC and Route tables.

Syntax

Parameter	Description
external [s]	Shows external memory configuration.
internal	Shows internal memory configuration.
usage	Memory usage information.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
6.0	This command was introduced.
11.2	The show memory [internal usage] command was introduced.

Usage Guidelines

This command may take some time to display the requested information, depending on the number units and amount of entries of each unit. For hardware models without external L2/L3 memory, this command will only display resources of internal memory. For hardware models with internal and external memories, both are considered by this command. Please note that total number of available entries depends on the hardware model and configuration of external memory partitioning .

Example

This example illustrates how to show the external memory information.

```
DmSwitch#show memory external
MAC Table      Route Table Entries      Partitioning (%)
```

Unit	Block	Entries	Total	IPv4	IPv6**	Total	MAC	Route	IPv4	IPv6
1	1-12	0	262144	-	-	100	0	100	-	-

(**) IPv6 routes occupies more table entries than IPv4 and L2
DmSwitch#

This example illustrates how to show the internal memory information.

DmSwitch#show memory internal

Unit	Block	MAC Address	Route Table		Configurable	
		Table	Total	IPv4		IPv6
1	1-24	32768	16384+	16384	8192	No

(+) Maximum number of entries. L3 memory is shared by IPv4 and IPv6 routes.

DmSwitch#

Related Commands

Command	Description
show cpu memory	Shows the processor memory utilization.

show meter

```
show meter [ sort remark | ingress { id meter-id | all } | egress { id meter-id | all } ]
```

Description

Shows meters configuration.

Syntax

Parameter	Description
sort remark	(Optional) Shows ingress stage meter sort by remark
ingress id <i>meter-id</i>	(Optional) Shows ingress stage meter with a specific id
ingress all	(Optional) Shows all ingress stage meter
egress id <i>meter-id</i>	(Optional) Shows egress stage meter with a specific id
egress all	(Optional) Shows all egress stage meter

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
11.6	<i>ingress</i> <i>egress</i> parameter was added.

Usage Guidelines

Entering this command without parameters, all meter configuration will be shown.

Example

This example illustrates how to show the meters configuration

```
DmSwitch#show meter ingress all
Meter 1:
  Filter(s):
  Mode:      Flow
  Rate-limit: 64 kbit/s
  Burst:     4 kbyte
```

```
Stage:          Ingress
DmSwitch#
```

Related Commands

Command	Description
meter	Configures a meter to be used by a filter
filter	Creates or configures a traffic filter

show monitor

show monitor

Description

Shows traffic monitoring configuration.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
10.0	RSPAN was introduced.
13.0	Filtered sources were introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the traffic monitoring configuration.

```
DmSwitch#show monitor
```

```
Traffic Monitor
```

```
-----  
Destination port:  Eth 1/24  
Remote SPAN:      Using VLAN 100
```

```
Sources:
```

ID	Interface	Mode	Match
-	Eth 1/2-1/4	Rx/Tx	
1	Eth 1/5	Rx/Tx	VLAN 3
2	Eth 1/6-1/7	Rx	802.1p 5 VLAN 100

```
DmSwitch#
```

Related Commands

Command	Description
<code>output modifiers</code>	Options to filter text output: after, begin, exclude and include
<code>monitor</code>	Configures the traffic monitoring.
<code>monitor source</code>	Sets the interface as a monitoring source.

show mpls forwarding-table ^[1] ^[3] ^[6]

```
show mpls forwarding-table [ wrap-fields ]
```

```
show mpls forwarding-table [ wrap-fields ] protocol { ldp | rsvp }
```

```
show mpls forwarding-table [ wrap-fields ] interface { tunnel { tunnel-id | any } |  
vlan { vlan-id | any } }
```

```
show mpls forwarding-table [ wrap-fields ] action { forward | php | pop | push |  
swap }
```

```
show mpls forwarding-table [ wrap-fields ] prefix { address | address/prefix length |  
any }
```

```
show mpls forwarding-table [ wrap-fields ] tunnel { tunnel name | any }
```

```
show mpls forwarding-table [ wrap-fields ] vrf { vrf name | any }
```

```
show mpls forwarding-table [ wrap-fields ] graceful-restart
```

Description

Displays the MPLS forwarding table.

Syntax

Parameter	Description
wrap-fields	(optional) Wrap fields longer than the column length in several lines. This option may be used with all other parameters.
protocol { ldp rsvp bgp ^[1] ^[3] ^[5] }	(optional) Show entries using the given protocol.
interface tunnel { tunnel-id any }	(optional) Show entries using the given tunnel as output interface. Unless any is given, <i>tunnel-id</i> must be a numeric tunnel identifier.
interface vlan { vlan-id any }	(optional) Show entries using the given VLAN as output interface. Unless any is given, <i>vlan-id</i> must be a numeric VLAN identifier.
action { forward php pop push swap }	(optional) Show entries which executes the given MPLS label action.
prefix { address address/prefix length any }	(optional) Show entries matching the given address or prefix. Unless any is given, <i>address</i> must be an IPv4 address optionally followed by a prefix length.

Parameter**tunnel** { *tunnel name* | **any** }**vrf** { *vrf name* | **any** }**graceful-restart****Description**

(optional) Show entries using the given tunnel as input interface. Unless **any** is given, *tunnel name* must be the exact tunnel name.

(optional) Show entries using the given VRF prefix as input interface. Unless **any** is given, *vrf name* must be the exact VRF name.

(optional) Shows stale entries during or immediately following a graceful restart.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.2	This command was introduced.
12.2	The protocol parameter was introduced.

Usage Guidelines

This command shows a list of all entries present in the MPLS forwarding table, with its associated protocols, actions, labels, interfaces, statuses and roles.

Example

This example illustrates how to show the full MPLS forwarding table and how to filter by MPLS action and prefix.

```
DmSwitch#show mpls forwarding-table
```

```
Number of entries: 14 (8 ILMs and 6 FTNs)
```

```
Action Codes: FWD - Forward, PHP - Penultimate Hop Popping,
               POP - Pop and L3 Lookup, PSH - Push Label, SWP - Label Swap
```

```
Role Codes: D - Detour Tunnel, LR - Local Repair
```

```
Status Codes: A - Active, I - Inactive, P - Pending, S - Stale
```

```
-----+-----+-----+-----+-----+-----+
Prefix, Tunnel ID | Act | Incoming      | Outgoing      | Outgoing      | Status
or Lookup Table  | ion | Label/        | Label/        | Interface      | & Role
              |    | Protocol      | Protocol      |                |
-----+-----+-----+-----+-----+-----+-----+

```

```

200.200.200.3/32      SWP  21/LDP      16/BGP      VLAN 507    A
200.200.200.2/32      SWP  20/LDP      19/BGP      VLAN 507    A
200.200.200.1/32      PHP  19/LDP      ImpNull/LDP  VLAN 516    A
200.200.200.1/32      PHP  18/BGP      ImpNull/LDP  VLAN 516    A
172.16.95.10/31       POP  17/BGP        -           -           A
200.200.200.4/32      POP  16/BGP        -           -           A
200.200.200.1/32      FWD  -           ImpNull/LDP  VLAN 516    A
200.200.200.2/32      PSH  -           19/BGP      VLAN 507    A
172.16.95.8/31        PSH  -           18/BGP      VLAN 507    A
172.16.95.16/31       PSH  -           17/BGP      VLAN 507    A
200.200.200.3/32      PSH  -           16/BGP      VLAN 507    A

```

DmSwitch#

DmSwitch#show mpls forwarding-table action php

Number of entries: 2 (2 ILMs)

Action Codes: FWD - Forward, PHP - Penultimate Hop Popping,
 POP - Pop and L3 Lookup, PSH - Push Label, SWP - Label Swap,
 DIS - Discard

Role Codes: D - Detour Tunnel, LR - Local Repair

Status Codes: A - Active, I - Inactive, P - Pending, S - Stale

```

-----+-----+-----+-----+-----+-----
Prefix, Tunnel ID | Act | Incoming | Outgoing | Outgoing | Status
or Lookup Table  | ion | Label/   | Label/   | Interface | & Role
                |    | Protocol | Protocol |           |
-----+-----+-----+-----+-----+-----
200.200.200.1/32  PHP  19/LDP    ImpNull/LDP  VLAN 516    A
200.200.200.1/32  PHP  18/BGP    ImpNull/LDP  VLAN 516    A
-----+-----+-----+-----+-----+-----

```

DmSwitch#show mpls forwarding-table prefix 200.200.200.1

Number of entries: 3 (2 ILMs and 1 FTN)

Action Codes: FWD - Forward, PHP - Penultimate Hop Popping,
 POP - Pop and L3 Lookup, PSH - Push Label, SWP - Label Swap,
 DIS - Discard

Role Codes: D - Detour Tunnel, LR - Local Repair

Status Codes: A - Active, I - Inactive, P - Pending, S - Stale

```

-----+-----+-----+-----+-----+-----
Prefix, Tunnel ID | Act | Incoming | Outgoing | Outgoing | Status
or Lookup Table  | ion | Label/   | Label/   | Interface | & Role
                |    | Protocol | Protocol |           |
-----+-----+-----+-----+-----+-----
200.200.200.1/32  PHP  19/LDP    ImpNull/LDP  VLAN 516    A
200.200.200.1/32  PHP  18/BGP    ImpNull/LDP  VLAN 516    A
200.200.200.1/32  FWD  -         ImpNull/LDP  VLAN 516    A
-----+-----+-----+-----+-----+-----

```

Command	Description
---------	-------------

Related Commands

Command	Description
<code>show ip route</code>	Shows the IP routing table.
<code>show ip bgp labels</code>	Shows the BGP routing table entries.
<code>show mpls ftn</code>	Shows all FECs that are sharing one NHLFE.

show mpls exp-map egress ^[1] ^[3] ^[6]

`show mpls exp-map egress`

Description

Shows MPLS COS priority to EXP mapping table for egress packets.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Shows the translation table from internal priority to MPLS EXP.

Example

This example illustrates how to show the mpls-exp mapping information.

```
DmSwitch#show mpls exp-map egress
Priority - EXP
0 - 0
1 - 1
2 - 2
3 - 3
4 - 4
5 - 5
6 - 6
7 - 7
```

Related Commands

Command	Description
mpls exp-map egress	Configures the table mapping for COS priority to EXP egress packets.
mpls exp-map ingress	Configures the table mapping for EXP to COS priority ingress packets.
show mpls exp-map ingress	Shows MPLS EXP to COS priority mapping table for ingress packets.

show mpls exp-map ingress ^[1] ^[3] ^[6]

`show mpls exp-map ingress`

Description

Shows MPLS EXP to COS priority mapping table for ingress packets.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Shows the translation table from MPLS EXP to internal priority.

Example

This example illustrates how to show the mpls-exp mapping information.

```
DmSwitch#show mpls exp-map ingress
EXP - Priority
0   -   0
1   -   1
2   -   2
3   -   3
4   -   4
5   -   5
6   -   6
7   -   7
```

Related Commands

Command	Description
mpls exp-map egress	Configures the table mapping for COS priority to EXP egress packets.
mpls exp-map ingress	Configures the table mapping for EXP to COS priority ingress packets.
show mpls exp-map egress	Shows MPLS COS priority to EXP mapping table for egress packets.

show mpls ftn ^[1] ^[3] ^[6]

show mpls ftn

Description

Shows all FECs that are sharing one NHLFE (Next Hop Label Forwarding Entry).

Syntax

No parameter accepted.

Default

No default is defined.

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

One entry in LFIB (Label Forwarding Information Base), that represent a FEC-to-NHLFE (FTN) mapping, can be shared by multiple FECs. The command **show mpls ftn** shows all FECs, sharing one NHLFE, that could be installed on MPLS LFIB.

Example

This example illustrates how to shows FECs that are sharing one NHLFE.

```
DmSwitch#show mpls ftn
```

Status Codes: A - Active, P - Pending, S - Stale

Prefix, Tunnel ID or Lookup Table	Prot ocol	Label	Unit/ Port	Outgoing Interface	Next-hop	Sta tus
100.100.100.4/32	LDP	21	1/11	VLAN 841	172.16.84.9	A
100.100.100.2/32 100.100.100.3/32	LDP	ImpNull	1/11	VLAN 841	172.16.84.9	A

Table entries: 3

```
DmSwitch#
```


Related Commands

Command	Description
<code>show mpls forwarding table</code>	List the forwarding table
<code>show mpls ldp database</code>	List LSP database

show mpls l2vpn [1] [3] [6]

```
show mpls l2vpn [counters [vpn id] | detail | summary | vpn id [detail] | range  
First id Last id [detail]]
```

Description

Shows L2VPN (VPWS/VPLS) information.

Syntax

Parameter	Description
counters [1] [3] [5]	Show L2VPN counters.
detail	Show L2VPN detailed information.
summary	Show L2VPN summarized information.
vpn id	The VPN identifier.
range	Show a range of L2VPN configurations.

Default

When **vpn id** is not specified, all L2VPN entries are shown.

Command Modes

Privileged EXEC.

Command History

Release	Modification
9.0	These commands were introduced.
10.0	These commands were modified and improved.
11.0	Added Graceful Restart recovery status.
12.2	Added the VPN name in show mpls l2vpn counters.
12.4	Added the Backup PW information and new hardware status.
14.2	Added L2VPN counters on DM4100 Enduro.

Usage Guidelines

To use this command, the equipment must support the MPLS feature.

On DM4100 Enduro, statistics must be enabled on a VPN in order to check its L2VPN counters (due to hardware restrictions, only RX counters are available).

Example

This example shows a table with all L2VPN entries.

```
DmSwitch(config)#show mpls l2vpn
```

VPN ID		Access Int			Uplink Interfaces (PW's)					

	Type	VC type/VID		pw_id	dest address		status	l_label		r_label

2	VPWS	vlan	3		2	100.100.100.2		Up		16 16

3	VPWS	vlan	4		3	100.100.100.2		Up		17 17

4	VPWS	vlan	5		4	100.100.100.2		Up		18 18

This example shows L2VPN detailed information for VPN ID #2.

```
DmSwitch(config)#show mpls l2vpn vpn 2 detail
```

```
-----
VPN ID 2: VPWS enabled Name: CWB-RT-3
VC type: Ethernet VLAN; VLAN ID: 3, Access Intf status: Up

Destination address: 100.100.100.2, PW id: 2
PW status: Up, VC status: Up
Remote Access Intf status: Up
Create time: Thu Jan 1 00:00:18 1970
Total Up time: 0 days 5 hours 44 minutes 43 seconds
Up time: 0 days 5 hours 44 minutes 43 seconds
Last status change time: Thu Jan 1 00:12:31 1970
Signalling protocol: LDP (Up)
MPLS VC labels: local 16, remote 16
MTU: local 9198, remote 9198
Backup Role: None Actual State: Unavailable
```

This example shows L2VPN summarized information, and graceful restart recovery status.

```
DmSwitch(config)#show mpls l2vpn summary
```

```
Total number of PWs:
-----
Unknown: 0
Up: 3
Down: 0
Dormant: 0
LowerLayerDown: 0
Admin Down: 0
Access Pend: 0
Tunnel Pend: 0

L2VPN Graceful Restart:
-----
Recovery Status: inactive
```

This example shows L2VPN counters when uplink is not protected.

```
DmSwitch(config)#show mpls l2vpn counters
```

Warning: Tx values can be overcounted if monitor is enabled at the interface.

VPN	Type	Interface	Type	Peer	RX Pkts	TX Pkts
Name VPN_1_DATACOM_2012						
1		Eth 1/2	access	--	0	0
	VPWS	Eth 1/1	uplink	100.100.100.1	0	0
Name -						
2		Eth 1/2	access	--	0	0
	VPLS	Eth 1/1	uplink	100.100.100.1	0	0
		Eth 1/1	uplink	100.100.100.2	0	0

This example shows L2VPN counters when uplink is protected. Note in both L2VPN entries that port **Eth 1/3** is the backup port. Only **TX packets** are available for backup port.

```
DmSwitch(config)#show mpls l2vpn counters
```

Warning: Tx values can be overcounted if monitor is enabled at the interface.

VPN	Type	Interface	Type	Peer	RX Pkts	TX Pkts
Name VPN_1_DATACOM_2012						
1		Eth 1/2	access	--	0	0
	VPWS	Eth 1/1	uplink	100.100.100.1	0	0
		Eth 1/3				0
Name -						
2		Eth 1/2	access	--	0	0
	VPLS	Eth 1/1	uplink	100.100.100.1	0	0
		Eth 1/3				0
		Eth 1/1	uplink	100.100.100.2	0	0
		Eth 1/3				0

This example shows L2VPN counters on DM4100 Enduro (statistics have been previously enabled only on VPN 1).

```
DmSwitch(config)#show mpls l2vpn counters
```

Warning: Tx values can be overcounted if monitor is enabled at the interface.

VPN	Type	Interface	Type	Peer	RX Pkts	TX Pkts
-----	------	-----------	------	------	---------	---------

		Name	VPN_1_DATACOM_2012				
	1						
			Eth 1/2		access		--
						0	
			VPWS				
			Eth 1/1		uplink		100.100.100.1
						0	
							Not Avail.
		Name	-				
	2						
			Eth 1/2		access		--
						Disabled	
							Not Avail.
			VPWS				
			Eth 1/1		uplink		100.100.100.1
						Disabled	
							Not Avail.
			Eth 1/1		uplink		100.100.100.2
						Disabled	
							Not Avail.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
mpls vpws	Configure Virtual Private Wire Service.
mpls vpls	Configure Virtual Private LAN Service.
vpn	Create, disable or enable a Virtual Private Wire Service VPN.
vpn	Create, disable or enable a Virtual Private LAN Service VPN.
statistics	Enables statistics on the VPLS VPN.
statistics	Enables statistics on the VPWS VPN.
xconnect vlan	Creates an access VLAN interface for the VPWS VPN.
xconnect vlan	Creates an access VLAN interface for the VPLS VPN.
neighbor	Configures a VPWS with the specified neighbor.
neighbor	Configures a VPLS with the specified neighbor.
mpls ldp graceful-restart	Activate/configure LDP Graceful Restart.

show mpls l2vpn hardware

```
show mpls l2vpn hardware vpn [id | all | range [ First id Last id ] ]
```

Description

Show detailed information for VPN allowing comparisons between software and hardware status side by side.

Syntax

Parameter	Description
vpn <i>id</i>	Show hardware information for specified VPN identifier
all	Show all configured L2VPN hardware information.
range	Show a range of L2VPN hardware information.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.6	This command was introduced.
12.0	Included state that show the synchronization between units.
14.0	This command was made visible to cli users.

Usage Guidelines

The **show mpls l2vpn hardware vpn** command presents information about the status of an MPLS L2VPN in control and data plane. The table presents informations from the protocol stack, responsible for MPLS protocols; from the configuration database, present in the local database and from hardware, side by side. Therefore, it is possible to compare all levels of configuration necessary for a MPLS L2VPN.

The structure of the show have three levels, that can be found in the columns fields:

Field	Description
<i>CP Status:</i>	Presents information about control plane level.
<i>DB Status::</i>	Presents information about local configuration database.

Field	Description
<i>HW Status::</i>	Presents hardware informations.

The **show mpls l2vpn hardware vpn** lines presents the following informations:

VPN: Display the VPN status informations, that should be present at all configuration levels

Field	Description
<i>VPN</i>	Shows the type of VPN (VPLS or VPWS) and the status
<i>MAC limit</i>	Display the <i>mac limit</i> value configured in the VPN

Access port: Display the access interface information at different levels, containing the follow informations in database and hardware levels

Field	Description
<i>Id</i>	Shows the type of access interface, which can be the following types

The following table presents the possible types of access interface:

Type	Description
<i>Ltn</i>	Local Tunnel internal loop;
<i>PWE3</i>	CESOP PWE3 over MPLS
<i>PTP</i>	CESOP PTP clock synchronization over MPLS
<i>Eth</i>	Ethernet interface
<i>PCh</i>	Port-Channel interface

Note: The *Access port* information are not reported for the control plane, thus the audit does not provide *CP Status* information.

Uplink port: Display the *Uplink port* information at different levels. Containing the follow informations.

Field	Description
<i>ID</i>	Shows the type of uplink interface, listed in the next table
<i>local label</i> and <i>remote label</i>	Display the labels negotiated by the control plane. They must contain the same value in all configuration levels.
<i>Split-Horizon</i>	Display if the Split-Horizon feature is enabled. This feature is present in MPLS VPLS type.
<i>Egress tnl</i>	Egress ID of MPLS tunnel used by this vpn.
<i>Egress vpn</i>	Egress ID of L2VPN uplink port.

The following table presents the possible types of Uplink interface:

Type	Description
<i>Eth</i>	Ethernet interface;
<i>PCh</i>	Port-Channel interface.

Both *VPN*, *Access port* and *Uplink port* have the same status classification:

Status	Description
<i>Created</i>	Created and properly configured.
<i>Pending</i>	Port has been allocated in database but is not present on hardware.
<i>Not Sync</i>	The system that compare information between units to check if is synchronized, return fail.
<i>FAILED</i>	Failure state, observed in a hardware configuration failures.
<i>Init FAILED</i>	Port is created but has problem in VLAN translate and/or Multicast flags.
<i>MAC Limit FAILED</i>	MAC limit configuration error.
<i>Stand-By</i>	Port is from Back-PW and is in stand-by state.
<i>Not Created</i>	Represents a Back-PW ports in hardware level or a invalid value sent to the bcmd configuration logic.

Examples

This example shows a normal **show mpls l2vpn hardware vpn** for a MPLS VPWS VPN

```
show mpls l2vpn hardware vpn 3
```

```
Codes: * Do not care.
       - Do not exist.
```

```

+-----+
| VPN ID 3 |
+-----+
| VPN Components | CP Status | DB Status | HW Status |
+-----+
| VPN (VPWS ) | Created | Created | Created |
| - ID | * | 3 | 0x00002002 |
+-----+
| Access port | * | Created | Created |
| - ID | * | Eth 1/1 | Eth 1/1 |
| - VLAN | * | 142 | 142 |
| | | | |
+-----+
| Uplink port | Created | Created | Created |
| - ID | * | Pch 1 | Pch 1 |
| - local label | 125 | 125 | 125 |
| - remote label | 54 | 54 | 54 |
| - egress | * | 104111 | 104111 |
| | | | |
+-----+

```

This example shows a normal **show mpls l2vpn hardware vpn** for a MPLS VPLS VPN with three uplink ports.


```
show mpls l2vpn hardware vpn 2
```

```
Codes: * Do not care.
       - Do not exist.
```

+-----+				
VPN ID 2				
+-----+				
VPN Components CP Status DB Status HW Status				
+-----+				
VPN (VPLS) Created Created Created				
- ID * 2 0x00003000				
- MAC limit * 1024 1024				
+-----+				
Access port * Created Created				
- ID * Eth 1/5 Eth 1/5				
- VLAN * 142 142				
+-----+				
Uplink port Created Created Created				
- ID * Pch 1 Pch 1				
- local label 89 89 89				
- remote label 127 127 127				
- egress * 104116 104116				
- Split-Horizon * YES YES				
Uplink port Created Created Created				
- ID * Pch 1 Pch 1				
- local label 54 54 54				
- remote label 125 125 125				
- egress * 104118 104118				
- Split-Horizon * YES YES				
Uplink port Created Created Created				
- ID * Eth 1/3 Eth 1/3				
- local label 19 19 19				
- remote label 125 125 125				
- egress * 104120 104120				
- Split-Horizon * YES YES				
+-----+				

This example shows a **show mpls l2vpn hardware vpn** for a MPLS VPWS VPN with Backup-PW enabled. When this feature is enabled, the backup-PW presents *Stand-By* state at the *CP Status* and *DB Status* levels. But the *HW Status* presents the *Not Created* state. Because, only active PW's have hardware configurations.

```
show mpls l2vpn hardware vpn 29
```

```
Codes: * Do not care.
       - Do not exist.
```

+-----+				
VPN ID 29				
+-----+				
VPN Components CP Status DB Status HW Status				
+-----+				
VPN (VPWS) Created Created Created				
- ID * 29 0x00002006				
+-----+				
Access port * Created Created				
- ID * Eth 2/20 Eth 2/20				
- VLAN * 562 562				
+-----+				
Uplink port Created Created Created				

- ID	*	Eth 2/6	Eth 2/6	
- local label	23	23	23	
- remote label	19	19	19	
- egress	*	104102	104102	
Uplink port	Stand-By	Stand-By	Not Created	
- ID	*	Eth 2/1	-	
- local label	24	24	-	
- remote label	21	21	-	
- egress	*	104100	0	
+-----+-----+-----+-----+				

Related Commands

No related command.

show mpls audit l2vpn [1] [3] [6]

```
show mpls audit l2vpn
```

Description

Shows the status of MPLS L2VPN scheduled to audit.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command shows all MPLS L2VPN scheduled to audit, the associate lsp FEC and handle id and wait time status.

The MPLS audit L2VPN provides scheduling of periodic audits to correct possible hardware inconsistencies presents on installed MPLS L2VPNs. This audits are carried out based on the values of *guard-time* and *interval-time*, which control the initial delay after event ocurrence and the interval between audits respectively.

Example

This example illustrates how to show the MPLS L2VPN scheduled to audit.

```
DmSwitch#show mpls audit l2
Scheduled VPN audits
-----|
| Handle      | FEC          | wait (s) | VPN  |
| 0x01AA0003 | 0xC8C8C804 | 0000     |      |
|              |              |           | 3201 |
|              |              |           | 3202 |
|              |              |           | 3203 |
|              |              |           | 3204 |
|              |              |           | 3205 |
|-----|
```

```
Total: 1
DmSwitch#
```

Related Commands

Command	Description
mpls audit l2vpn	Specifies the mpls audit l2vpn parameters.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.

show mpls vpls mac-address-limit ^[1] ^[3] ^[6]

```
show mpls vpls mac-address-limit [vpn id]
```

Description

Shows the configured mac-address limit of VPLS VPN's.

Syntax

Parameter	Description
vpn id	The VPN identifier.

Default

When **vpn id** is not specified, mac-address limit of all VPLS VPN's are shown.

Command Modes

Global configuration.

Command History

Release	Modification
11.6	This command was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS/VPLS feature.

This command shows the global (default) mac-address limit and the limits configured for each VPLS VPN's, indicating if it is a local configured value or the global value.

Example

This example shows the table with all mac-address limits.

```
DmSwitch#show mpls vpls mac-address-limit
```

```
mpls vpls mac-address limit global 512
```

```
VPN      Limit  Type
-----
7        350  Local
8        512  Global
9        512  Global
```

DmSwitch#

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mac-address-table	Shows the MAC address table.

show mpls ldp database ^[1] ^[3] ^[6]

```
show mpls ldp database { reason-codes } [ ipaddress ]
```

Description

List LSP database.

Syntax

Parameter	Description
<i>ipaddress</i>	(optional) Information about specific FEC.
reason-codes	Show a list of available reason codes and their explanation.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
10.0	New parameter to filter by FEC. Indicator of not selected entries.
10.0	Added netmask in the Network Prefix row.
13.4	Added reason codes and reason messages to explain why a FEC is Not Selected.

Usage Guidelines

This command shows an ordered list of all labels present in LDP database, including non-installed labels. Also, it shows the number of total entries in the database and the number of FEC's. Entries marked with NS are not installed (not used to forward packets).

Every label mapping received from a peer LSR is retained regardless of whether the LSR is the next hop for the advertised mapping or not. Only the label received from the current next hop will be installed.

Inserting the FEC (*ipaddress*) parameter will display only the labels associated with the respective FEC.

Example

This example illustrates how to show the full LDP's database and how to filter by FEC.

```
DmSwitch#show mpls ldp database
```

```
Number of Entries: 13
```

```
Number of FECs....: 4
```

```
NS/XXX = Not Selected/Reason Code
```

```
For a detailed description of the reason codes,  
see 'show mpls ldp database reason-codes'
```

Network Prefix	UpStream LSR-ID	Label	DownStream LSR-ID	Label
100.100.100.1/32	100.100.100.2	16	--	--
100.100.100.1/32	--	--	100.100.100.1	3
NS/10A 100.100.100.1/32	--	--	100.100.100.2	301392
100.100.100.2/32	100.100.100.1	19	--	--
NS/12B 100.100.100.2/32	--	--	100.100.100.1	300160
100.100.100.2/32	--	--	100.100.100.2	3
100.100.100.3/32	100.100.100.2	17	--	--
100.100.100.3/32	--	--	100.100.100.1	299792
NS/10A 100.100.100.3/32	--	--	100.100.100.2	301408
100.100.100.11/32	100.100.100.1	3	--	--
100.100.100.11/32	100.100.100.2	3	--	--
NS/10A 100.100.100.11/32	--	--	100.100.100.1	300144
NS/12B 100.100.100.11/32	--	--	100.100.100.2	301376

```
DmSwitch#
```

```
DmSwitch#show mpls ldp database 100.100.100.1
```

```
Number of Entries: 3 out of 13
```

```
Number of FECs....: 1 out of 4
```

```
NS/XXX = Not Selected/Reason Code
```

```
For a detailed description of the reason codes,  
see 'show mpls ldp database reason-codes'
```

Network Prefix	UpStream LSR-ID	Label	DownStream LSR-ID	Label
100.100.100.1/32	100.100.100.2	16	--	--
100.100.100.1/32	--	--	100.100.100.1	3
NS/10A 100.100.100.1/32	--	--	100.100.100.2	301392

```
DmSwitch#
```

This example illustrates how to show the translated error codes.

```
DmSwitch#show mpls ldp database reason-codes
```

```
List of reason codes for the Not-Selected (NS) FEC's in LDP database
```

```
000: Contact your customer support.
```

```
001: Contact your customer support.
```

```
002: Contact your customer support.
```

```
003: User deactivated this LSP.
```

```
021: Reroute of the LSP.
```

```
022: LSP output interface is down.
```

```
023: Contact your customer support.
```

```
024: Error while attempting to route.
```

```
025: LSP was pre-empted.
```


047: Feature was disable on control plane.
 048: Multiple LSPs are sharing the same set of resources.
 061: FEC has gone down.
 062: Properties of the FEC has changed (e.g. next hop has changed).
 063: Session to the peer has gone down.
 064: The C-bit is invalid.
 065: Recovery period has ended.
 066: This is a non-merging FEC and the upstream has been released.
 067: A loop has been detected.
 068: Invalid interface parameters.
 069: Local policy.
 06A: Label Withdraw message has been received.
 06B: Label Release message has been received.
 06C: Label Abort message has been received.
 06D: Peer has withdrawn the address of the next hop for the FEC.
 06E: There is no downstream session the ordered control mode is in use.
 06F: There was a local error programming the label.
 100: Contact your customer support.
 101: FEC is not in local Routing Table.
 102: The next hop for the FEC is different than the FEC.
 103: The next hop for the FEC is different than the FEC.
 104: Label Mapping is not from a route next hop.
 105: Session to the peer is down.
 106: Invalid interface index.
 107: Interface is down.
 108: Contact your customer support.
 109: This is a stale mapping.
 10A: This is not a stale mapping.
 10B: FEC is not UP.
 10C: There is outstanding requests for this FEC.
 10D: Internal error on Control Plane.
 10E: FEC did not came from a downstream session for the FEC.
 10F: Restart recovery time is not in progress.
 110: Internal error on Control Plane.
 111: Cannot restart this LSP using LDP restart procedures.
 112: FEC was uninstalled and was not worth retaining.
 113: FEC was uninstalled and was worth retaining.
 114: FEC via an unsolicited mapping and was not worth keeping
 115: FEC has two or more outsegments and ECMP is not enabled.
 116: FEC is down and the session is configured to be local liberal.
 117: FEC is down and the session is configured to be local liberal.
 118: FEC is down and the session is configured to be local liberal.
 119: FEC is down and the session is configured to be local liberal.
 11A: FEC is down and it supports querying.
 11B: FEC is down and it supports querying.
 11C: FEC is down and it supports querying.
 11D: FEC is down and session supports policies.
 11E: FEC is down and session supports policies.
 11F: FEC is down and session supports policies.
 120: Recovery is in progress.
 121: Recovery is in progress.
 122: Recovery is in progress.
 123: Recovery is in progress.
 124: FEC is being released by a policy decision.
 125: FEC is being retained by a policy decision.
 126: The label mapping was rejected locally.
 127: Internal error on Control Plane.
 128: Next hop has changed.
 129: The downstream mapping belongs to an orphan LSP for a
 non-LSP merging FEC.
 12A: Liberally-retaining this FEC until the peer withdraws it and
 resends it with C-bit 0.
 12B: It's not a VC FEC and all out labels have failed (possibly error when
 trying to install on hardware).
 12C: The label mapping was retained.

```
12D: The label mapping was retained.  
12E: The label mapping was retained.  
12F: The label mapping is from a route next hop.  
130: Contact your customer support.  
131: Contact your customer support.  
132: Contact your customer support.  
133: Contact your customer support.
```

Related Commands

Command	Description
show ip route	Shows the IP routing table.
show mpls ldp neighbor	Shows the status of LDP sessions.
show mpls ldp parameters	Shows current LDP parameters.
ldp enable	Enable LDP capability in selected VLAN.

show mpls ldp discovery ^[1] ^[3] ^[6]

```
show mpls ldp discovery [ detail ] [ ip-address ]
```

Description

Shows the status of LDP discovery process.

Syntax

Parameter	Description
<i>ip-address</i>	(optional) Shows information about specific LSR Id.
detail	(optional) Shows information about all LSR Id's.
detail <i>ip-address</i>	(optional) Shows information about specific LSR Id.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	New filter by LSR Id. Two display nodes: common and detailed.

Usage Guidelines

This command shows the list of active adjacencies discovered via basic and extended discovery mechanism.

"Local Peers" use basic discovery mechanism, sending Hello messages over UDP to an well known Multicast Group. They are directly connected to the router.

"Remote Peers" use extended discovery mechanism, sending Targeted Hello messages. They can be both directly and remotely connected to the router. Note that for this type of adjacency there is no associated interface since LDP hello messages are exchanged through the best L3 route.

Example

This example illustrates how to show the active LDP adjacencies in common and detailed format.

```
DmSwitch#show mpls ldp discovery
```

```
-----
|Adjacency ID          |Discovery Mechanism   |Hold Time           |
|-----|-----|-----|
|          100.100.100.2:0|          Basic|          15 s|
|          100.100.100.2:0|        Extended|          45 s|
|-----|-----|-----|
```

```
DmSwitch#
```

```
DmSwitch#show mpls ldp discovery detail
```

```
Adjacency: 100.100.100.2:0 - Basic Discovery Mechanism
Interface: VLAN 100
Adjacency discovery hello hold time: 15s
Local LDP ID: 100.100.100.1:0 discovery hello hold time: 15s
Negotiated discovery hello hold time: 15s
Negotiated time between hello messages: 5s
Remaining time: 12s
```

```
Adjacency: 100.100.100.2:0 - Extended Discovery Mechanism
Interface: L3
Adjacency discovery hello hold time: 45s
Local LDP ID: 100.100.100.1:0 discovery hello hold time: 45s
Negotiated discovery hello hold time: 45s
Negotiated time between hello messages: 15s
Remaining time: 33s
```

```
DmSwitch#
```

Related Commands

Command	Description
mpls ldp discovery	Specifies the global discovery hold timer for LDP sessions.
show mpls ldp neighbor	Shows the status of LDP sessions.
show mpls ldp parameters	Shows current LDP parameters.
show running-config	Shows the current operating configuration.

show mpls ldp graceful-restart ^[1] ^[3] ^[6]

```
show mpls ldp graceful-restart
```

Description

Shows LDP/L2VPN Graceful Restart recovery status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.0	This command was introduced.
12.2	Added status information about GR to L2VPN.

Usage Guidelines

This command informs the graceful restart configuration and whether the LDP/L2VPN control plane is in the process of graceful restart or not. If affirmative, it will return "in progress". Otherwise, "inactive" is returned.

Example

This example illustrates how to show the LDP graceful restart recovery status.

```
DmSwitch#show mpls ldp graceful-restart
```

```
Graceful Restart: enabled
Recovery status:
  LDP Recovery status: inactive
  L2VPN Recovery Status: inactive
```

Related Commands

Command	Description
---------	-------------

Command	Description
<code>mpls ldp graceful-restart</code>	Activate/configure LDP Graceful Restart.
<code>show mpls ldp parameters</code>	Shows current LDP parameters.

show mpls ldp igp sync ^[1] ^[3] ^[6]

```
show mpls ldp igp sync [ interface vlan [ all | vid ] ]
```

Description

Shows information for LDP-IGP Synchronization process.

Syntax

Parameter	Description
<i>vid</i>	Displays the LDP-IGP Synchronization information for the specified interface.
all	Displays the LDP-IGP Synchronization information for all interfaces.

Default

When **interface vlan** is not specified, all interfaces with LDP capabilities are shown.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The table below describes the significant fields shown.

Field	Description
Vlan	ID of the VLAN interface
LDP configured	Label Distribution Protocol is configured.
SYNC enabled	Either LDP-IGP Synchronization is enabled or disabled on that interface.
SYNC status	Synchronization was achieved or not.
IGP holddown time	The IGP holddown time.
Peer LDP Ident	IP Address of the peer.
IGP enabled	IGP that the feature is enabled for.

Example

This example shows a sample output from the **show mpls ldp igp sync**.

```
DmSwitch#show mpls ldp igp sync
Vlan 311
    LDP configured; SYNC enabled.
    SYNC status: IGP and LDP up and synced.
    IGP holddown time: infinite.
    Peer LDP Ident: 200.200.200.1
    IGP enabled: OSPF 1
Vlan 312
    LDP configured; SYNC enabled.
    SYNC status: IGP and LDP up and synced.
    IGP holddown time: infinite.
    Peer LDP Ident: 200.200.200.3
    IGP enabled: OSPF 1
```

This example shows a sample output from the **show mpls ldp igp sync interface vlan all**.

```
DmSwitch#show mpls ldp igp sync
Vlan 311
    LDP configured; SYNC enabled.
    SYNC status: IGP and LDP up and synced.
    IGP holddown time: infinite.
    Peer LDP Ident: 200.200.200.1
    IGP enabled: OSPF 1
Vlan 312
    LDP configured; SYNC enabled.
    SYNC status: IGP and LDP up and synced.
    IGP holddown time: infinite.
    Peer LDP Ident: 200.200.200.3
    IGP enabled: OSPF 1
Vlan 313
    LDP not configured; SYNC enabled.
    SYNC status: IGP and LDP not synced, no holddown.
    IGP holddown time: infinite.
    Peer LDP Ident: 200.200.200.4
    IGP enabled: OSPF 1
```

If LDP-IGP Synchronization is disabled on an interface, the output looks like the following.

```
DmSwitch#show mpls ldp igp sync
Vlan 313
    LDP configured; SYNC disabled.
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show mpls ldp neighbor ^[1] ^[3] ^[6]

```
show mpls ldp neighbor [ detail ] [ ip-address ]
```

Description

Shows either summarized or detailed information about LDP sessions. The full output of this command displays general status information about the established LDP sessions (status, role, uptime, remaining keepalive hold time, etc.), session negotiated timer values, and the addresses advertised by the neighbors through LDP Address Messages.

Syntax

Parameter	Description
<i>ip-address</i>	(optional) Shows summarized information about the LDP session established with the specified neighbor.
detail	(optional) Shows detailed information about all the LDP sessions.
detail <i>ip-address</i>	(optional) Shows detailed information about the LDP session established with the specified neighbor.

Default

N/A.

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	New filter by LSR Id. Two display modes: summarized and detailed.
13.4	Added list of addresses ("Remote addresses") advertised by a neighbor through LDP Address Messages.

Usage Guidelines

This command shows all active LDP sessions and the current status in summarized and detailed format.

The LSR Id determines whether it will play the active or passive role in session establishment by comparing addresses A1 (LSR1 address) and A2 (LSR2 address) as unsigned integers. If $A1 > A2$, LSR1 plays the active

role, otherwise it is passive (RFC 3036).

If LSR1 A1 is active, it attempts to establish the LDP TCP connection by connecting to the well-known LDP port at address A2. If LSR1 is passive, it waits for LSR2 to establish the LDP TCP connection to its well-known LDP port.

Example

This example illustrates how to show LDP session information in summarized and detailed format.

```
DmSwitch#show mpls ldp neighbor
```

```
-----
|Adjacency ID          |Status              |Local Role          |
|-----|-----|-----|
|          200.200.200.1:0|          Operational|          Active|
|          100.100.100.3:0|          Operational|          Passive|
|-----|-----|-----|
```

```
DmSwitch#show mpls ldp neighbor detail 200.200.200.1
```

```
Peer LDP Id: 200.200.200.1 local LDP Id: 200.200.200.2
  Local TCP connection role: Active
  Status: Operational
  Up time: 00:01:23
  Local configured KeepAlive (KA) hold time: 40s
  Peer's advertised KA hold time: 40s
  Negotiated KeepAlive (KA) hold time: 40s
  Negotiated time between KA messages: 7s
  KA hold time remaining for this session: 36s
  Maximum PDU length: 4096
  Remote addresses:
    Total: 10
    172.16.95.8      172.16.95.11      172.16.95.33      172.17.15.0
    172.17.15.2      172.17.15.4      172.17.15.6      172.17.15.8
    172.17.15.10     200.200.200.1
```

```
DmSwitch#
```

Related Commands

Command	Description
mpls ldp neighbor	Sets up an LDP targeted session with a specified neighbor.
show mpls ldp parameters	Shows current LDP parameters.
show mpls ldp discovery	Shows the status of LDP discovery process.
show running-config	Shows the current operating configuration.
ldp enable	Enable LDP capability in selected VLAN.

show mpls ldp parameters ^[1] ^[3] ^[6]

show mpls ldp parameters

Description

The output of this command displays the current control-plane configuration state of several LDP parameters such as: Session/adjacency general configuration, Graceful Restart (RFC3478), label distribution to targeted neighbors policy, address list of local LDP-enabled interfaces (the IP addresses that are advertised by this router to its neighbors through LDP Address Messages), and the list of LDP entities (link and targeted).

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
10.0	Changes in output layout.
11.0	Added LDP Graceful Restart parameters.
13.4	Added list of LDP-enabled interfaces ("Local addresses").
14.4	Added neighbor advertise-labels parameter.

Usage Guidelines

This command shows the current configured LDP parameters.

Example

This example illustrates how to show the current LDP parameters.

```
DmSwitch#show mpls ldp parameters

LSR_ID: 200.200.200.2
Protocol version: 1
Discovery hello holdtime: 15s
Discovery targeted hello holdtime: 45s
Session hold time : 40s
Allocation mode: Ordered
Encapsulation mode: PHP implicit-null
```

```

Distribution mode: Unsolicited
Retention mode: Liberal
Graceful Restart: disabled
  FT Reconnect timer: 240000 (msec)
  MPLS Forwarding State Holding timer: 240000 (msec)
  Neighbor Liveness timer: 240000 (msec)
  Maximum Recovery timer: 240000 (msec)
  Adjacency Down Hold timer: 60000 (msec)
Advertise Labels to Targeted Peers: yes
Local addresses:
  Total: 10
  172.16.95.9          172.16.95.16          172.17.15.1          172.17.15.3
  172.17.15.5          172.17.15.7          172.17.15.9          172.17.15.11
  172.17.15.13         200.200.200.2
Entities LDP link session:
  Local peer 200.200.200.2:0 Entity ID: 1
Entities LDP target session:
  Target peer 200.200.200.3:0 Entity ID: 2 Authentication: MD5 encryption
  Target peer 200.200.200.4:0 Entity ID: 3 Authentication: MD5 encryption
  Target peer 200.200.200.1:0 Entity ID: 4 Authentication: MD5 encryption

```

Related Commands

Command	Description
show mpls ldp discovery	Specifies the global discovery hold timer for LDP sessions.
mpls ldp holdtime	Specifies the global hold time for all LDP sessions.
show mpls ldp discovery	Shows the status of LDP discovery process.
show mpls ldp neighbor	Shows the status of LDP sessions.
show running-config	Shows the current operating configuration.
mpls ldp graceful-restart	Activate/configure LDP Graceful Restart.
ldp enable	Enable LDP capability in selected VLAN.

show mpls oam [1] [3] [6]

```
show mpls oam { db }
```

Description

Shows MPLS OAM information.

Syntax

Parameter	Description
db	Show all information on the MPLS OAM database.
db handle <i>handle-id</i>	(optional) Show only information about the specified handle.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the MPLS OAM database.

```
DmSwitch#show mpls oam db
Command:      ping
Type:         ldp
Handle:       1153103
PID:          -1
FEC:          200.200.200.2/32
filename:     /tmp/lrmo_1153103.xml
State:        complete
Started at:   Fri Jul 15 16:17:58 2011 UTC0
Last update:  Fri Jul 15 16:17:58 2011 UTC0
```

```
Command:      traceroute
Type:         ldp
Handle:       884917
PID:         -1
FEC:         200.200.200.3/32
filename:     /tmp/lrmo_884917.xml
State:       aborted
Started at:   Fri Jul 15 16:18:05 2011 UTC0
Last update:  Fri Jul 15 16:18:05 2011 UTC0
```

DmSwitch#

Example

This example illustrates how to show the MPLS OAM database entry specified by handle.

```
DmSwitch#show mpls oam db handle 1153103
Command:      ping
Type:         ldp
Handle:       1153103
PID:         -1
FEC:         200.200.200.2/32
filename:     /tmp/lrmo_1153103.xml
State:       complete
Started at:   Fri Jul 15 16:17:58 2011 UTC0
Last update:  Fri Jul 15 16:17:58 2011 UTC0
```

DmSwitch#

Related Commands

Command	Description
clear mpls-oam	Deletes entries from the MPLS OAM database.

show mpls rsvp [1] [3] [6]

show mpls rsvp counters messages [vlan *vlan_id*]

Description

Show counters of RSVP messages.

Syntax

Parameter	Description
<i>vlan_id</i>	Vlan identification

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example presents the command results for **show mpls rsvp counters messages**.

```
DmSwitch#show mpls rsvp counters messages
VLAN 560      Recv   Xmit
Path          102    79    Resv          186    90
PathError     0      0    ResvError     0      0
PathTear      0      0    ResvTear      0      0
Hello         330    330    ResvConfirm   1      1
Bundle        0      0    SRefresh      0      0
TotalMsgs     619    500

VLAN 561      Recv   Xmit
Path          195    123    Resv          151    81
PathError     0      0    ResvError     0      0
PathTear      0      0    ResvTear      0      0
Hello         330    330    ResvConfirm   2      3
```

Bundle	0	0	SRefresh	0	0
TotalMsgs	678	537			

Related Commands

Command	Description
<code>show mpls te traffic-eng tunnels</code>	Shows Traffic Engineering Tunnel Information

show mpls te traffic-eng tunnels ^[1] ^[3] ^[6]

```
show mpls te traffic-eng tunnels [{destination dst_ip_addr | detail |  
name tnl_name | role {all | head | headtail | tail | transit} | source  
src_ip_addr}]
```

Description

Shows either a brief or detailed information about all tunnels, including those that the router is the ingress, egress or transit label switched router (LSR).

Inserting **detail** at the end of the command will show all Tunnels (Ingress, Egress and Transit) in a detailed form.

Syntax

Parameter	Description
destination <i>dst_ip_addr</i>	Shows all tunnels that matches the destination IP address.
detail	Shows detailed information of all configured tunnels.
name <i>tnl_name</i>	Shows only the tunnels that matches the tunnel name.
role {all head headtail tail transit}	Shows only the tunnels that matches the provided role (head, headtail, tail, transit or all).
source <i>src_ip_addr</i>	Shows all tunnels that matches the source IP address.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows the command results for **show mpls te traffic-eng tunnels detail** and **show mpls te traffic-eng tunnels**.

```
DmSwitch#show mpls te traffic-eng tunnels detail

Name: DM4001_10_T10 [Instance 0]
Src: 100.100.1.10 Dst: 100.100.1.16
Status:
  Admin: up          Oper: up          Role: head      Dir: out
  Setup Prio: 0      Holding Prio: 0      LSP_ID: 0
  Affinity: 0x0 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Detour: none
Resources:
  Max rate: (value not available)
History:
  Tunnel:
    Time since created : 0 days, 0 hours, 31 minutes, 45 seconds
    Total up time      : 0 days, 0 hours, 0 minutes, 43 seconds
  InLabel: -
  OutLabel: VLAN 888, 0

DmSwitch#

DmSwitch#show mpls te traffic-eng tunnels
Tunnel-Name[Inst.]  Destination      Detour  Up-If    Down-If    Adm/Oper
-----
DM4001_10_T10      [ 0] 100.100.1.16  none           888 ,0      up/up

DmSwitch#
```

Related Commands

Command	Description
show mpls rsvp	Show counters of RSVP messages

show network-policy

show network-policy

Description

Shows Network Policy settings.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the Network Policy configuration.

```
DmSwitch#show network-policy
```

Profile	Application Type	VLAN	Layer 2 Priority	DSCP	MAC List
1	voice	native	0	0	-
2	voice	untagged	0	46	-
3	voice	200	7	0	auto
4	voice	dot1p	5	46	-
5	voice	dot1p	2	46	-
6	voice-sig	100	3	46	-
7	voice	1	5	46	-
8	voice	100	3	46	-

```
DmSwitch#
```

Related Commands

Command	Description
<code>network-policy</code>	Enters on Network Policy configuration mode.
<code>voice vlan</code>	Configure Voice VLAN feature.
<code>voice-signaling vlan</code>	Configure Voice-Signaling VLAN feature.
<code>show running-config</code>	Shows the current operating configuration.
<code>network-policy mac-list</code>	Configure Network Policy MAC List settings.

show network-policy mac-list

show network-policy mac-list

Description

Shows Network Policy MAC list settings.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the Network Policy configuration.

```
DmSwitch#show network-policy mac-list
```

Entry	MAC Address	Mask	Description
1	00:04:DF:00:00:00	FF:FF:FF:00:00:00	MyTelephone

```
DmSwitch#
```

Related Commands

Command	Description
network-policy	Enters on Network Policy configuration mode.
voice vlan	Configure Voice VLAN feature.

Command

voice-signaling vlan
show running-config

Description

Configure Voice-Signaling VLAN feature.
Shows the current operating configuration.

show oam

show oam

Description

Shows oam information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the OAM information.

```
DmSwitch#show oam
```

```
Events:          UL - Link Down/Unidirectional link  CE - Critical Event
                  TO - Link OAM timeout
                  NO - No event  -- - OAM disabled/Interface shutdown/Unknown(Remote)
```

```
Discovery:       UN - Unsatisfied/Unknown(Remote)  IN - Incomplete  CO - Complete
                  -- - Local OAM disabled/Local interface shutdown
```

```
Dest. Address:  ST - Standard IEEE OAMPDUs destination MAC address
                  AL - Alternative OAMPDUs destination MAC address
```

Port	Enabled	Local		Remote		Discovery		Destination Address
		Event	Event	Event	Event	Local	Remote	
1/ 1	YES	UL	--	UN	UN			ST
1/ 2	YES	UL	--	UN	UN			ST
1/ 3	YES	UL	--	UN	UN			ST
1/ 4	YES	UL	--	UN	UN			ST
1/ 5	YES	UL	--	UN	UN			ST

1/ 6	YES	UL	--	UN	UN	ST
1/ 7	YES	UL	--	UN	UN	ST
1/ 8	YES	UL	--	UN	UN	ST
1/ 9	YES	UL	--	UN	UN	ST
1/10	YES	UL	--	UN	UN	ST
1/11	YES	UL	--	UN	UN	ST
1/12	YES	UL	--	UN	UN	ST
1/13	YES	UL	--	UN	UN	ST
1/14	YES	UL	--	UN	UN	ST
1/15	YES	UL	--	UN	UN	ST
1/16	YES	UL	--	UN	UN	ST
1/17	YES	UL	--	UN	UN	ST
1/18	YES	UL	--	UN	UN	ST
1/19	YES	UL	--	UN	UN	ST
1/20	YES	UL	--	UN	UN	ST
1/21	YES	UL	--	UN	UN	ST
1/22	YES	UL	--	UN	UN	ST
1/23	YES	UL	--	UN	UN	ST
1/24	YES	UL	--	UN	UN	ST
1/25	YES	UL	--	UN	UN	ST
1/26	YES	UL	--	UN	UN	ST
1/27	YES	UL	--	UN	UN	ST
1/28	YES	UL	--	UN	UN	ST

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
oam	Enables or disables OAM for Ethernet interface

show openflow

show openflow [flows]

Description

Shows global OpenFlow information.

Syntax

Parameter	Description
flows	(Optional) Shows all flows installed in hardware.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
OF-1.0.4	This command was introduced.
OF-1.0.5	Changes in output layout.

Usage Guidelines

Not available.

Example

This example illustrates how to show OpenFlow configuration.

```
DmSwitch(config)#show openflow

OpenFlow is enabled.
Version: 1.0
Datapath ID: 00:00:00:04:df:1c:7a:1d

Controller:
  IP Address: 10.1.32.101
  Port: 6633
  Connection: tcp
  Status: Not Connected
```

```

Mode:
    reactive

Native Vlan:
    4000

Ports:
    1/1 1/2

Reserved Filter Group Priority:
    None

Strip of FCS (Frame Check Sequence) is enabled.

DmSwitch(config)#

```

Example

This example illustrates how to show OpenFlow flows installed in hardware.

```

DmSwitch(config)#show openflow flows

FLOW 1: Priority: 32767 Duration: 4.843s Number of Packets: 0
  MATCHES: Ether-type: 0x0800          IP proto: 1
           Ingress Port: 23             Src MAC: 00:01:02:03:04:05
           Dst MAC: 05:06:07:08:09:10   Src IP: 1.1.1.0/24
           Dst IP: 2.2.2.2              IP ToS Bits: 0
  ACTIONS: Output: Ingress Port
FLOW 2: Priority: 32767 Duration: 4.843s Number of Packets: 0
  MATCHES: Ether-type: 0x0800          IP proto: 1
           Ingress Port: 24             Src MAC: 05:06:07:08:09:10
           Dst MAC: 00:01:02:03:04:05   Src IP: 2.2.2.2
           Dst IP: 1.1.1.0/24           IP ToS Bits: 0
  ACTIONS: Output: 23

```

Related Commands

Command	Description
openflow	Enables global OpenFlow protocol.

show poe

show poe

Description

Shows the PoE configuration and status of all available interfaces.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
10.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the PoE configuration in use.

```
DmSwitch#show poe

Priority precedence
-----
static
high
low

Unit 1

System
-----
PSU power:          1000.0 W
System total power: 1000.0 W
Mainboard usage:    140.0 W
RPU Power Sharing:  disabled

PoE
---
```

PoE System Power

```

-----
Total:                860.0 W
Effective used power:  3.1 W

```

Configuration

```

-----

```

Configured Power

```

-----

```

```

Static ports:        38.2 W
Dynamic ports:       707.4 W
Total:               745.6 W

```

Available Power to configure

```

-----

```

```

To static ports:     860.0 W
To dynamic ports:    No limit

```

Status

```

-----

```

Reserved Power

```

-----

```

```

Static ports:        38.2 W
Dynamic ports:       15.4 W
Total:               53.6 W

```

Available Power to reserve

```

-----

```

```

To static ports:     860.0 W
To dynamic ports:    844.6 W

```

Config						Status		
Port	PoE	Mode	Max Power (mW)	Priority	Power Supply	Status	PD Power (W)	Provided Power (W)
1/ 1	on	dynamic	4.0	low	limit	off	--	0.0
1/ 2	on	dynamic	7.0	high	restrict	off	--	0.0
1/ 3	on	dynamic	15.4	low	restrict	off	--	0.0
1/ 4	on	dynamic	34.2	high	limit	off	--	0.0
1/ 5	on	static	4.0	static	limit	off	--	0.0
1/ 6	on	static	34.2	static	restrict	off	--	0.0
1/ 7	on	dynamic	15.4	low	restrict	on	15.4	3.1
1/ 8	on	dynamic	15.4	low	restrict	overcurrent	--	0.0
1/ 9	off	dynamic	15.4	low	restrict	off	--	0.0
1/10	off	dynamic	15.4	low	restrict	off	--	0.0
1/11	off	dynamic	15.0	low	restrict	off	--	0.0
1/12	off	dynamic	15.4	low	restrict	off	--	0.0
1/13	off	dynamic	15.4	low	restrict	off	--	0.0
1/14	off	dynamic	15.4	low	restrict	off	--	0.0
1/15	off	dynamic	15.4	low	restrict	off	--	0.0
1/16	off	dynamic	15.4	low	restrict	off	--	0.0
1/17	off	dynamic	15.4	low	restrict	off	--	0.0
1/18	off	dynamic	15.4	low	restrict	off	--	0.0
1/19	on	dynamic	15.4	low	restrict	off	--	0.0
...								
1/48	on	dynamic	15.4	low	restrict	off	--	0.0

DmSwitch#

Related Commands

Command	Description
<code>poe</code>	Configure interface port to transmit both data and electrical energy.
<code>rpu power-sharing</code>	Enables RPU to increase PoE power.

show port-security

show security

show port-security interface ethernet *unit-number/port-number*

show port-security interface port-channel *port-channel-number*

show port-security interface vlan *index*

Description

Shows port-security related information (configuration and status).

Syntax

Parameter	Description
interface ethernet <i>unit-number/port-number</i>	Show port-security information of a specific port
interface port-channel <i>port-channel-number</i>	Show port-security information of a specific port-channel
interface vlan <i>index</i>	Show port-security information of a specific VLAN

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command shows the port-security global status, indicating the configuration and status of each interface. Specific shows are available for interfaces ethernet, port-channels and VLANs.

Example

This example illustrates how to show the port-security information on some interface.

```
DmSwitch#show port-security interface ethernet 12
Interface:                               Eth  1/12
Configuration:
  Maximum:                               10
  Violation:                             Protect
  Sticky learning:                       Enable
Status:
  MAC address count:                     10
  MAC address count last update:         3 s ago
  MAC address count next update:         in 23 s
  Configuration state:                   Idle

-----
Sticky MAC address list:
MAC: 00:08:54:2F:88:18 - VLAN 1
MAC: AC:D0:B3:0E:9E:15 - VLAN 1
MAC: 38:02:E9:7F:E6:71 - VLAN 1
MAC: EA:3B:A8:56:37:C1 - VLAN 1
MAC: 80:E3:09:74:FB:ED - VLAN 1
MAC: 2E:5E:AF:49:78:5F - VLAN 1
MAC: 30:88:9D:0E:D1:6D - VLAN 1
MAC: 42:D0:E6:74:55:20 - VLAN 1
MAC: DE:0C:5E:68:21:F1 - VLAN 1
MAC: A6:90:5E:29:EE:A8 - VLAN 1

DmSwitch#
```

Related Commands

Command	Description
<code>switchport port-security</code>	Configures port-security maximum.
<code>maximum</code>	

show privilege

show privilege

Description

Shows the privilege level for the current user.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the current privilege level.

```
DmSwitch#show privilege
Current privilege level is 1
DmSwitch#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
username	Creates users and configures access to the DmSwitch.

show processes

show processes

Description

Shows managed processes information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command shows the managed processes information. The current managed processes are: cli, httpd, httpsd, main, snmpd, sntpd, traps, lldpd, multicastd, dclld, rpcdiag, ipcrecorder, eventd, psmd, auditd, dot1xd, httpd_captive, httpsd_captive, watchdog and cpumond.

Example

This example illustrates how to show the managed processes information.

```
DmSwitch#show processes
```

System Processes

PID	Process	State	Admin Status	Admin Request	Uptime	Restarts
3022	httpd	STARTED	Enabled	-	00:00	1
3023	httpsd	STARTED	Enabled	-	00:00	1
3911	main	STARTED	Enabled	-	00:00	1
3024	snmpd	STARTED	Enabled	-	00:00	2
-	sntpd	STOPPED	Disabled	-	-	0
3025	traps	STARTED	Enabled	-	00:00	1
3914	lldpd	STARTED	Enabled	-	00:00	1
3915	multicastd	STARTED	Enabled	-	00:00	1

```

3916 dcld          STARTED Enabled -      00:00      1
3917 rpcdiag       STARTED Enabled -      00:00      1
3918 ipcrecorder   STARTED Enabled -      00:00      1
3919 eventd        STARTED Enabled -      00:00      1
3994 psmd         STARTED Enabled -      00:00      1
3920 auditd        STARTED Enabled -      00:00      1
3995 dot1xd        STARTED Enabled -      00:00      1
-      httpd_captive STOPPED Disabled -      -          0
-      httpsd_captive STOPPED Disabled -      -          0
3921 watchdog     STARTED Enabled -      00:00      1
3922 cpumond       STARTED Enabled -      00:00      1
DmSwitch#

```

Related Commands

Command	Description
process	Control software processes.

show profile-config

```
show profile-config { metro }
```

Description

Shows the predefined DmSwitch profile configuration.

Output modifiers are available for this command.

Syntax

Parameter	Description
metro	A predefined profile to be used with Metropolitan Area Networks.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the predefined DmSwitch profile configuration.

```
DmSwitch#show profile-config metro
Building configuration...
!
hostname DmSwitch
!

(...)

!
interface vlan 1
```

```
name DefaultVlan
ip address dhcp
set-member untagged ethernet range 1/1 1/24
set-member tagged ethernet range 1/25 1/28
!
interface ethernet 1/1
shutdown
no spanning-tree 1
no switchport ingress-filtering
switchport egress-block ethernet range 1/2 1/24
!

(...)

!
spanning-tree 1
spanning-tree 1 vlan all
!
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
copy	Copies configuration and firmware.
diff	Compares and shows the differences between two configurations.
show running-config	Shows the current operating configuration.

show ptp

show ptp unit *unit-id*

Description

Shows information about PTP of an unit.

Syntax

Parameter	Description
<i>unit-id</i>	Number of an unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show ptp info of unit 1.

```
DmSwitch#show ptp unit 1
PTP Unit 1 Global Configuration:
  Operation Mode:      ordinary master
  Domain id:           0
  Enable:              yes

DmSwitch#
```

Related Commands

Command	Description
<code>domain</code>	Setup PTP domain.
<code>enable</code>	Enables PTP protocol.
<code>mode</code>	Configures PTP operation mode.

show public-key

show public-key [**host** | **user**]

Description

Shows the public key information.

Syntax

Parameter	Description
host	(Optional) Shows the public key for switch.
user	(Optional) Shows the public key for users.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The user option was added.
15.0	RSA1 key type is no longer supported.

Usage Guidelines

The **show public-key host** command shows the information after generating DSA/RSA host key pair.

Entering this command without parameters, all public key information will be shown.

Example

This example illustrates how to show the public key.

```
DmSwitch#show public-key host
DSA public key:
ssh-dss AAAAB3NzaC1kc3MAAACBAK1YoucNWs7AnqvhB60SDvqIe197mS/LoCo43h7Ptf3x62n+DkQLkjigB7Xi jYaD
yQrqBK51UmUhcHX610rObgDBZRLYfer9mWUQVKmJMTS2MycVY/MQgCVfN1Yvs9JHiAbRoqTL7BeEoi8SUbUm9qJ8tzOb
4vKM4niPgOzHbJLzAAAAFQCoEq2FDHgPlKK243nnQJKpGj/NMQAAAIv43oklJwQX2R+8L/ESiO8vuWrrzrvK7rL+gi5
OexU2xuS4e1ZpVF2AUhmmYP0jaWolNo22R9CxQaWdlEbTrX+wJ2ci0whJHh2inuDxAF+HSj2LX1yWj8KdqiOwroVxv17
```

```
T/wg1yeYyBDmaWHvCDkuvlTCbuYuxyVqkHlwcF4JygAAAIBoobnThzwGFVViwcfBwsFSAv3e7OiTmNRrGclAY7HAfBab
3V1sRJuEZH5kcrO0s0jGpQL8VKSHqjgn0yFSG9gefXay2Ae4YWEAxTDI3wGVCptlqwUHI LwrPBe6/bDgQ4NN1biafFEf
+3Nhbt1XDYgHMvKdbrmqF7PQ7Udn2TkaIA==
```

```
RSA public key:
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA5EdQ32K7CCyggZ6MdzxR+QUypdE4NUAnUot94ZEVLe/HyNdFFGuJ1lLe
9cUFC4n/7CUg7UFq6EgdOuSFLqNTJfKZOBMnBqXYk3GD1CE6riVxH5vTbacaKKqMMsEgq7O5Ng59TqMfvci1ag9UKq3h
LFM4m8fgLdRbGDYGiVjDhJ0=
```

```
DmSwitch#
```

Related Commands

Command	Description
ip ssh host-key clear	Configures the internal SSH server for external access.
ip ssh host-key generate	Configures the internal SSH server for external access.
show ip ssh	Shows the SSH server information.

show queue config

```
show queue config [ ethernet { range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } | [ unit-number/ ] port-number } | port-channel port-channel-number ]
```

Description

Use to show the queue configuration.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Shows a specific unit and port queue configuration. (Range: 1-1/1-28)
ethernet range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	(Optional) Shows a range of specific units and ports queue configuration. (Range: 1-1/1-28)
port-channel <i>port-channel-number</i>	(Optional) Shows a specific port-channel configuration. (Range: 1-32)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced. Before this was called show qos config .
7.8	The option port-channel was introduced.

Usage Guidelines

Entering this command without parameters, the entire CoS configuration table will be shown.

Example

This example illustrates how to show the queue configuration.

```
DmSwitch#show queue config ethernet 2
-----
Port  Queue  Mode    Max-Bw    Min-Bw  Weight  SP-Queue
```

```

-----
1/ 2    0    WRR    unlimit    -----    1    NO
1/ 2    1    WRR    unlimit    -----    2    NO
1/ 2    2    WRR    unlimit    -----    4    NO
1/ 2    3    WRR    unlimit    -----    6    NO
1/ 2    4    WRR    unlimit    -----    8    NO
1/ 2    5    WRR    unlimit    -----   10    NO
1/ 2    6    WRR    unlimit    -----   12    NO
1/ 2    7    WRR    unlimit    -----   14    NO
-----
DmSwitch#

```

Related Commands

Command	Description
queue max-bw	Configures the maximum bandwidth allocation per queue
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue sched-mode wdrp	Configures Ethernet interface queues in Weighted Deficit Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues

show queue cos-map

show queue cos-map

Description

Use to show map of CoS priorities to queues.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced. Before this was called show qos cos-map .

Usage Guidelines

Not available.

Example

This example illustrates how to show the CoS mappings.

```
DmSwitch#show queue cos-map
-----+-----+
Queue | 802.1P Priority |
-----+-----+
  0   | 0               |
  1   | 1               |
  2   | 2               |
  3   | 3               |
  4   | 4               |
  5   | 5               |
  6   | 6               |
  7   | 7               |
-----+-----+
DmSwitch#
```

Related Commands

Command	Description
<code>queue max-bw</code>	Configures the maximum bandwidth allocation per queue
<code>queue sched-mode sp</code>	Configures Ethernet interface queues in Strict Priority schedule mode.
<code>queue sched-mode wfq</code>	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
<code>queue sched-mode wrr</code>	Configures Ethernet interface queues in Weighted Round Robin schedule mode
<code>queue sched-mode wdrp</code>	Configures Ethernet interface queues in Weighted Deficit Round Robin schedule mode
<code>queue cos-map</code>	Maps CoS priorities to queues

show radius-server

show radius-server

Description

Shows RADIUS server information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the RADIUS server information.

```
DmSwitch#show radius-server
RADIUS authentication configuration:
  Default Key:  *****
  Default Port:  1812
  Timeout:      5
  Retries:      2
  Host 1:
    Address:    10.10.10.15
    Port:       333
  Host 2:
  Host 3:
  Host 4:
  Host 5:
DmSwitch#
```

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>radius-server acct-port</code>	Configures the default RADIUS server accounting port.
<code>radius-server auth-port</code>	Configures the default RADIUS server authentication port.
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server key</code>	Configures the default RADIUS server key string.
<code>radius-server retries</code>	Configures the RADIUS server retries.
<code>radius-server timeout</code>	Configures the RADIUS server timeout.

show redundancy-status ^[5]

show redundancy-status

Description

Shows redundancy information.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.
13.0	Switchover reason information was implemented.
13.4	Protocol port and Legacy-Port Mode informations were added.

Usage Guidelines

Not available.

Example

This example shows the redundancy status of the system.

```
DmSwitch#show redundancy-status
MPU Redundancy

Basic Information:
  Protocol Version:
    Local  MPU:          0
    Remote MPU:          0
  Protocol Port:        61039

Configuration:
  Legacy-Port Mode:     Disabled
  Non-Stop Forward:     Enabled
  NSF-ID:               01

Current Status:
  MPU Role:             Active
  Synchronization Items:
    Protocol State:      Synced
    Flash Configuration: Synced
    Running Configuration: Synced
```

```
Startup Configuration Selection:      Synced
Graceful Restart Information:         Synced
Current Error:
Local  MPU:                          (none)
Remote MPU:                          (none)
Switchover Reason:                   Safe switchover
NSF Port Status:
  (.)Enabled; (E)Disabled by EAPS; (lx)Disabled by 802.1x;

Unit 2
  2  4  6  8 10 12 14 16 18 20 22 24 26
  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .  .  .  .  .  .  .  .  .  .  .
  1  3  5  7  9 11 13 15 17 19 21 23 25

DmSwitch#
```

Related Commands

Command	Description
redundancy	Redundancy configuration and operation

show remote-devices

```
show remote-devices [ fail ]
```

```
show remote-devices interface ethernet unit-number/port-number
```

```
show remote-devices interface ethernet range first-unit-number/first-port-number  
last-unit-number/last-port-number
```

```
show remote-devices interface ethernet all
```

Description

Remote device management configuration and status.

Syntax

Parameter	Description
fail	(Optional) Show information about remote devices in a fail condition.
interface ethernet all	Show the remote-devices information on all ports
interface ethernet range { [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Show the remote-devices information of a given range of ports
interface ethernet [<i>unit-number/</i>] <i>port-number</i>	Show the remote-device information of a specific given port

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.
13.0	Added more options for showing information on specific ports.

Usage Guidelines

Not available.

Example 1

This example shows remote devices information and all detected devices.

```
DmSwitch#show remote-devices
```

```
Remote Devices Management:
```

```
Global enable:          Enabled
Devices VLAN:
  VLAN ID:              Not configured
Rate limit:             100 packet/s
Conflict solving:       Manual
Services:
  Service 1:            TCP 23
  Service 2:            TCP 80
```

Port	Enable	Fail	Status
1/ 1	NO	NO	Disabled
1/ 2	YES	NO	No Device Detected
1/ 3	YES	NO	Device Ready
1/ 4	NO	NO	Disabled
1/ 5	NO	NO	Disabled
1/ 6	NO	NO	Disabled
1/ 7	NO	NO	Disabled
1/ 8	NO	NO	Disabled
1/ 9	NO	NO	Disabled
1/10	NO	NO	Disabled
1/11	NO	NO	Disabled
1/12	NO	NO	Disabled
1/13	NO	NO	Disabled
1/14	NO	NO	Disabled
1/15	NO	NO	Disabled
1/16	NO	NO	Disabled
1/17	NO	NO	Disabled
1/18	NO	NO	Disabled
1/19	NO	NO	Disabled
1/20	NO	NO	Disabled
1/21	NO	NO	Disabled
1/22	NO	NO	Disabled
1/23	NO	NO	Disabled
1/24	NO	NO	Disabled
1/25	NO	NO	Disabled
1/26	NO	NO	Disabled

```
DmSwitch#
```

Example 2

This example shows remote devices information of a given range of ports.

```
DmSwitch#show remote-devices interface ethernet range 9 12
```

```
Interface: Eth 1/9
State: Disabled
```

```
Interface: Ethernet 1/10
State: Device ready
```

```

OUI: 00:1e:90
OID: 1.3.6.1.4.1.3709.1.2.17
Vendor number: 1
MAC address: 00:1e:90:fa:61:88
Factory ID: 890788
Firmware version: 7.8
Remote interface: 1/27

```

```

Interface: Eth 1/11
State: Disabled

```

```

Interface: Eth 1/12
State: Disabled

```

```
DmSwitch#
```

Related Commands

Command	Description
remote-devices	Configure a VLAN to manage remote devices locally.
devices-vlan	
remote-devices enable	Enable remote devices management.
remote-devices force	Force configuration of remote devices with configuration conflict.
remote-devices rate-limit	Configure maximum number of packets per second sent to remote devices.

show rmon alarm

show rmon alarm

Description

Shows the RMON alarm table.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the RMON alarm table.

```
DmSwitch#show rmon alarm
Alarm 1 is active, owned by test
Monitors .1.3.6.1.2.1.2.2.1.14.5 every 30 second(s)
Taking delta sample, last value was 0
Rising threshold is 10, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising or falling alarm

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
rmon	Configures an RMON.

Command	Description
<code>rmon alarm</code>	Configures an RMON alarm.
<code>rmon collection history</code>	Configures a RMON history group of statistics.
<code>rmon collection stats</code>	Configures a RMON collection of statistics.
<code>rmon event</code>	Configures an RMON event.
<code>show rmon event</code>	Shows the RMON event table.
<code>show rmon history</code>	Shows the RMON history table.
<code>show running-config</code>	Shows the current operating configuration.
<code>show rmon statistics</code>	Shows the RMON statistics table.

show rmon event

show rmon event

Description

Shows the RMON event table.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the RMON event table.

```
DmSwitch#show rmon event
Event 1 is active, owned by test
Description is HighErrors
Event firing causes log and trap to community eventtrap, last fired at sysUpTime 0

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
rmon	Configures an RMON.
rmon alarm	Configures an RMON alarm.
rmon collection history	Configures a RMON history group of statistics.

Command	Description
<code>rmon collection stats</code>	Configures a RMON collection of statistics.
<code>rmon event</code>	Configures an RMON event.
<code>show rmon alarm</code>	Shows the RMON alarm table.
<code>show rmon history</code>	Shows the RMON history table.
<code>show running-config</code>	Shows the current operating configuration.
<code>show rmon statistics</code>	Shows the RMON statistics table.

show rmon history

show rmon history [*index*]

Description

Shows the RMON history table.

Output modifiers are available for this command.

Syntax

Parameter	Description
<i>index</i>	(Optional) Identifies the RMON history group of statistics. (Range: 1-65535)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Entering this command without parameters, the entire RMON history table will be shown.

Example

This example illustrates how to show the RMON history table.

```
DmSwitch#show rmon history
Entry 5 is active, and owned by test
Monitors ifEntry.1.5 every 30 second(s)
Requested # of time intervals, ie buckets, is 8,
Sample # 1 began measure at sysUpTime 1505
Drop events           :0
Octets                :5236
Pkts                  :77
Broadcast pkts        :0
Multicast pkts        :77
```



```

CRCA align errors      :0
Undersize pkts        :0
Oversize pkts         :0
Fragments             :0
Jabbers               :0
Collisions            :0
Utilization           :0
Sample # 2 began measure at sysUpTime 1535
Drop events           :0
Octets                :5236
Pkts                  :77
Broadcast pkts        :0
Multicast pkts        :77
CRCA align errors      :0
Undersize pkts        :0
Oversize pkts         :0
Fragments             :0
Jabbers               :0
Collisions            :0
Utilization           :0
Sample # 3 began measure at sysUpTime 1565
Drop events           :0
Octets                :5372
Pkts                  :79
Broadcast pkts        :0
Multicast pkts        :79
CRCA align errors      :0
Undersize pkts        :0
Oversize pkts         :0
Fragments             :0
Jabbers               :0
Collisions            :0
Utilization           :0

DmSwitch#

```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
rmon	Configures an RMON.
rmon alarm	Configures an RMON alarm.
rmon collection history	Configures a RMON history group of statistics.
rmon collection stats	Configures a RMON collection of statistics.
rmon event	Configures an RMON event.
show rmon alarm	Shows the RMON alarm table.
show rmon event	Shows the RMON event table.
show running-config	Shows the current operating configuration.
show rmon statistics	Shows the RMON statistics table.

show rmon statistics

`show rmon statistics [index]`

Description

Shows the RMON statistics table.

Output modifiers are available for this command.

Syntax

Parameter	Description
<i>index</i>	(Optional) Identifies the RMON group of statistics. (Range: 1-65535)

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Entering this command without parameters, the entire RMON statistics table will be shown.

Example

This example illustrates how to show the RMON statistics table.

```
DmSwitch#show rmon statistics
Collection 5 on Eth 1/5 is active, and owned by test
Monitors ifEntry.1.5 wich has received:
Drop events           : 0
Octets                : 340
Pkts                  : 5
Broadcast pkts        : 0
Multicast pkts        : 5
CRCA align errors     : 0
Undersize pkts        : 0
```

```

Oversize pkts      : 0
Fragments          : 0
Jabbers            : 0
Collisions         : 0
Pkts 640 octets    : 0
Pkts 65 to 127 octets : 5
Pkts 128 to 2550 octets : 0
Pkts 256 to 5110 octets : 0
Pkts 512 to 10230 octets : 0
Pkts 1024 to 1518 Octets : 0

```

```
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
rmon	Configures an RMON.
rmon alarm	Configures an RMON alarm.
rmon collection history	Configures a RMON history group of statistics.
rmon collection stats	Configures a RMON collection of statistics.
rmon event	Configures an RMON event.
show rmon alarm	Shows the RMON alarm table.
show rmon event	Shows the RMON event table.
show rmon history	Shows the RMON history table.
show running-config	Shows the current operating configuration.

show running-config

show running-config

Description

Shows the current operating configuration.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This show command can be use to look, for example, configured users, the status of internal servers, enabled protocols, the status of VLANs and interfaces, etc.

Example

This example illustrates how to show the current operating configuration.

```
DmSwitch#show flash-config 4
Building configuration...
!
hostname DmSwitch
!
username admin access-level 15
username admin password 7 d033e22ae348aeb5660fc2140aec35850c4da997
username guest access-level 0
username guest password 7 35675e68f4b5af7b995d9205ad0fc43842f16450
!
ip telnet server
ip http server
ip http secure-server
no ip ssh server
!
ip snmp-server community public ro
!
interface vlan 1
 name DefaultVlan
```

```
ip address 192.168.0.25/24
set-member untagged ethernet all
!
spanning-tree 1
spanning-tree 1 vlan all
!
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
diff	Compares and shows the differences between two configurations.
show flash-config	Shows the configuration stored in a specific flash position.
show startup-config	Shows the startup flash configuration.

show running-config cfm

show running-config cfm

Description

Shows the current operating configuration for Connectivity Fault Management (CFM).

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.6	This command was introduced.

Usage Guidelines

This show command can be use to look details about the CFM configuration.

Example

This example illustrates how to show the current operating configuration for CFM

```
DmSwitch#show running-config cfm
cfm enable
!
cfm md Domain level 7
ma Ma1 vlan-list 1
  mep-list 1 2 3 4
  mep id 1 direction down ethernet 1/1
  enable
  generate-ccm
  primary-vid 1
ma Ma2 vlan-list 1
  mep-list 1 2 3 4
  mep id 3 direction down ethernet 2/1
  enable
  generate-ccm
  primary-vid 1
!
DmSwitch#
```

Related Commands

Command	Description
<code>show flash-config</code>	Shows the configuration stored in a specific flash position.
<code>show running-config</code>	Shows the current operating configuration.

show running-config interface

```
show running-config interface [ ethernet { all | range | unit/port | } | port-channel {  
all | range | unit/port | } | bundle { all | range | unit/bundle | } | g704 { all | range | unit/g704 | } | ptp  
{ all | range | unit/ptp | } | enter ]
```

Description

Shows the current operating configuration for a specific interface.

Syntax

Parameter	Description
ethernet [<i>unit/port</i> <i>all</i> <i>range</i>]	Shows running configuration for ethernet ports.
port-channel [<i>unit/port</i> <i>all</i> <i>range</i>]	Shows running configuration for port-channel interfaces.
bundle [<i>unit/bundle</i> <i>all</i> <i>range</i>]	Shows running configuration for bundle interfaces on pwe3 capable boards.
g704 [<i>unit/g704</i> <i>all</i> <i>range</i>]	Shows running configuration for g704 interfaces on pwe3 capable boards.
ptp [<i>unit/ptp</i> <i>all</i> <i>range</i>]	Shows running configuration for ptp interfaces on pwe3 IEEE1588 capable boards.
<i>enter</i>	Shows running configuration for all interfaces.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.2	This command was introduced.
13.2	Added support to pwe3 interfaces.

Usage Guidelines

This show command can be use to look, for example, configured ethernet and ptp interfaces.

Example

This example illustrates how to show the current operating configuration for all interfaces and for a range of

bundle interfaces.

```
DmSwitch#show running-config interface
interface ethernet 1/5
shutdown
!
interface ptp 1/1
role slave
source-ip-address 1.1.1.1/24
destination-ip-address 1.1.1.2
no shutdown
!
interface ptp 1/16
role slave
source-ip-address 16.1.1.1/24
destination-ip-address 16.1.1.2
no shutdown
!
ptp unit 1 mode ordinary slave
ptp unit 1 enable
!
interface g704 1/1
no shutdown
!
interface g704 1/6
no shutdown
!
interface bundle 1/1
destination-bundle 23
destination-ip-address 9.9.9.10
source-ip-address 9.9.9.9
vlan 1 priority 1
no shutdown
!
interface bundle 1/23
destination-ip-address 1.1.23.6
tdm-channel g704 6
source-ip-address 1.1.23.5
vlan 5 priority 5
no shutdown
!
DmSwitch#

DmSwitch#show running-config interface bundle range 1/10 1/200
interface bundle 1/23
destination-ip-address 1.1.23.6
no shutdown
source-ip-address 1.1.23.5
tdm-channel g704 6
vlan 5 priority 5
!
DmSwitch#
```

Related Commands

Command	Description
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.

show running-config private-vlan

```
show running-config private-vlan [ id { vlan_id } | name { name } | range { first_id  
last_id } | enter ]
```

Description

Shows the current operating configuration for a specific Private VLAN.

Output modifiers are available for this command.

Syntax

Parameter	Description
id <i>vlan_id</i>	Shows running configuration for a specific Private VLAN ID (Range: 1-4094)
name <i>name</i>	Shows running configuration for a specific Private VLAN name.
range <i>first_id last_id</i>	Shows running configuration for a specific Private VLAN range.
<i>enter</i>	Shows running configuration for all Private VLANs.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This show command can be use to look, for example, specific configured Private VLANs or a range of Private VLANs

Example

This example illustrates how to show the current operating configuration for all Private VLANs and for a specific Private VLAN

```
DmSwitchshow running-config private-vlan
```

```

interface private-vlan 100
  set-member promiscuous tagged ethernet 1/4
  set-member promiscuous tagged ethernet 2/1
  isolated-vlan 200
    set-member tagged ethernet range 1/2 1/3
  community-vlan 300
    set-member tagged ethernet 2/2
  community-vlan 400
    set-member tagged ethernet range 2/3 2/4
!
interface private-vlan 500
  set-member interswitch tagged ethernet 1/10
  set-member promiscuous tagged ethernet 5/4
  set-member promiscuous tagged ethernet 6/4
  isolated-vlan 700
    set-member tagged ethernet range 5/10 5/15
  community-vlan 900
    set-member tagged ethernet 2/20
!
DmSwitch#

DmSwitch#show running-config private-vlan id 100
interface private-vlan 100
  set-member promiscuous tagged ethernet 1/4
  set-member promiscuous tagged ethernet 2/1
  isolated-vlan 200
    set-member tagged ethernet range 1/2 1/3
  community-vlan 300
    set-member tagged ethernet 2/2
  community-vlan 400
    set-member tagged ethernet range 2/3 2/4
!
DmSwitch#

```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.

show running-config sdh-map

show running-config sdh-map

Description

Shows the current operating configuration for sdh-map.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

This show command can be use to look details about the sdh-map configuration.

Example

This example illustrates how to show the current operating configuration for sdh-map

```
DmSwitch#show running-config sdh-map
sdh-map unit 1 id 1 e1c 2 to sdh 4 vc4 1 vc12 111
sdh-map unit 1 id 2 e1c 1 to sdh 2 vc4 1 vc12 111
sdh-map unit 1 id 3 e1c 3 to sdh 2 vc4 1 vc12 311
sdh-map unit 1 id 4 e1c 4 to sdh 2 vc4 1 vc12 121
sdh-map unit 1 id 5 e1c 5 to sdh 2 vc4 1 vc12 221
sdh-map unit 1 id 6 e1c 6 to sdh 2 vc4 1 vc12 321
sdh-map unit 1 id 7 e1c 7 to sdh 2 vc4 1 vc12 131
sdh-map unit 1 id 8 e1c 8 to sdh 2 vc4 1 vc12 231
sdh-map unit 1 id 9 e1c 9 to sdh 2 vc4 1 vc12 331
!
DmSwitch#
```

Related Commands

Command	Description
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.

show running-config vlan

```
show running-config vlan [ id { vlan_id } | name { name } | range { first_id last_id } | enter ]
```

Description

Shows the current operating configuration for a specific VLAN.

Output modifiers are available for this command.

Syntax

Parameter	Description
id <i>vlan_id</i>	Shows running configuration for a specific VLAN ID (Range: 1-4094)
name <i>name</i>	Shows running configuration for a specific VLAN name.
range <i>first_id last_id</i>	Shows running configuration for a specific VLAN range.
<i>enter</i>	Shows running configuration for all VLANs.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.6.12	This command was introduced.

Usage Guidelines

This show command can be use to look, for example, specific configured VLANs or a range of VLANs

Examples

This example illustrates how to show the current operating configuration for all VLANs and for a range of VLANs

```
DmSwitch#show running-config vlan
interface vlan 1
name DefaultVlan
```

```
set-member untagged ethernet range 1/1 7/50
!  
interface vlan 2  
name management  
ip address 192.168.110.52/24  
set-member untagged ethernet 6/1  
!  
interface vlan 102  
ip address 192.168.110.1/24  
set-member untagged ethernet 1/13  
!  
interface vlan 202  
ip address 1.1.1.1/24  
!  
DmSwitch#  
  
DmSwitch#show running-config vlan range 2 102  
interface vlan 2  
name management  
ip address 192.168.110.52/24  
set-member untagged ethernet 6/1  
!  
interface vlan 102  
ip address 192.168.110.1/24  
set-member untagged ethernet 1/13  
!  
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.

show sdh-map

```
show sdh-map [ unit unit-id [ id map-id ] ]
```

Description

Use this command to show information about mappings of a SDH interface.

Syntax

Parameter	Description
unit <i>unit-id</i>	Shows information of one specific unit.
id <i>map-id</i>	Shows information of one specific mapping.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

If unit and/or map-id are not supplied, all SDH maps from all units are shown.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows information about the first mapping done on unit 4.

```
DmSwitch(config)#show sdh-map unit 4 id 1
SDH mapping unit 4 id 1:
  Enable:                Yes
  Node A:
    Type:                 E1C
    Index:                 1
  Node B:
    Type:                 VC-12
    SDH:                   1
```

```
VC-4: 1
VC-12: 111
DmSwitch(config)#
```

Related Commands

Command	Description
<code>sdh-map</code>	Configure mapping of SDH interfaces and E1C.
<code>show sdh-map table</code>	Show the mappings of SDH interfaces.

show sdh-map table

```
show sdh-map unit unit-id table [ bundle | e1c | sdh sdh-intf ]
```

Description

Use this command to show information about mappings of the sdh interface.

Syntax

Parameter	Description
bundle	Shows SDH mappings table indexed by bundle.
e1c	Shows SDH mappings table indexed by E1C.
sdh <i>sdh-intf</i>	Shows SDH mappings table indexed by VC12 from a specific SDH interface.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows information about the first mapping done on unit 4.

```
DmSwitch#show sdh-map unit 4 table sdh 1
```

Destination Index: X/Y/Z , where X is SDH physical interface index, Y is VC4 index and Z is KLM number.

```
Interface SDH 1:
```

```
VC-4 1:
```

```
TUG3-100:
```

```
-----
Origin  Destination      Origin  Destination      Origin  Destination
```

VC12	Type	Index	VC12	Type	Index	VC12	Type	Index

111	VC-12	2/1/242	112	VC-12	2/1/241	113	--	--
121	VC-12	2/1/232	122	VC-12	2/1/231	123	--	--
131	VC-12	2/1/222	132	VC-12	2/1/221	133	--	--
141	VC-12	2/1/212	142	VC-12	2/1/211	143	--	--
151	VC-12	2/1/271	152	--	--	153	--	--
161	VC-12	2/1/261	162	--	--	163	--	--
171	VC-12	2/1/251	172	--	--	173	--	--
TUG3-200:								

Origin	Destination		Origin	Destination		Origin	Destination	
VC12	Type	Index	VC12	Type	Index	VC12	Type	Index

211	VC-12	2/1/142	212	VC-12	2/1/141	213	--	--
221	VC-12	2/1/132	222	VC-12	2/1/131	223	--	--
231	VC-12	2/1/122	232	VC-12	2/1/121	233	--	--
241	VC-12	2/1/112	242	VC-12	2/1/111	243	--	--
251	VC-12	2/1/171	252	--	--	253	--	--
261	VC-12	2/1/161	262	--	--	263	--	--
271	VC-12	2/1/151	272	--	--	273	--	--
TUG3-300:								

Origin	Destination		Origin	Destination		Origin	Destination	
VC12	Type	Index	VC12	Type	Index	VC12	Type	Index

311	VC-12	2/1/332	312	VC-12	2/1/331	313	--	--
321	VC-12	2/1/322	322	VC-12	2/1/321	323	--	--
331	VC-12	2/1/312	332	VC-12	2/1/311	333	--	--
341	VC-12	2/1/371	342	--	--	343	--	--
351	VC-12	2/1/361	352	--	--	353	--	--
361	VC-12	2/1/351	362	--	--	363	--	--
371	VC-12	2/1/341	372	--	--	373	--	--

DmSwitch#

Related Commands

Command	Description
show sdh-map	Show the mappings of SDH interfaces.

show sflow config

show sflow config

Description

Shows current configurations about SFLOW agent and receivers.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows the command exit.

```
DmSwitch(config)#show sflow config
Global Config:
  sFlow enable:          Yes
  Agent Address:         192.168.12.34
Receivers:
  Receiver enable:       Yes
  Port:                  6343
  Address:                192.168.12.56
  Maximum datagram size: 1400
  Datagram version:      5

  Receiver enable:       Yes
  Port:                  6343
  Address:                192.168.12.78
  Maximum datagram size: 900
  Datagram version:      5
```

Related Commands

Command	Description
<code>show sflow counters</code>	Shows sFlow global counters.
<code>show sflow interfaces</code>	Shows sFlow interfaces configuration.

show sflow counters

show sflow counters

Description

This command shows informations about SFLOW packet counters. Four counters are showed: Total Samples Dropped - Incremented when internal operation error occurs; Total Samples Deleted - Incremented when incomplete config or error sending packet occurs (receiver/agent disabled or network error); Total Samples Sent - Incremented when packets are successfully sent; Total Samples Received - All packet samples received by agent.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows the command exit.

```
DmSwitch(config)#show sflow counters
Global Counters:
Total Samples Dropped:      284
Total Samples Deleted:      0
Total Samples Sent:         1983674
Total Samples Received:     1983674
```

Related Commands

Command	Description
<code>show sflow config</code>	Shows sFlow global configuration.
<code>show sflow interfaces</code>	Shows sFlow interfaces configuration.

show sflow interfaces

show sflow interfaces

Description

Shows current SFLOW configuration on Ethernet interfaces.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows the command exit.

```
DmSwitch(config)#show sflow interfaces
Ethernet 1/1:
  Enable:                Yes
  Interface index:        1
  Sample rate:            2000
  Counter sample interval: 65535
  Maximum header size:    128
  Receiver index:         3

Ethernet 1/21:
  Enable:                Yes
  Interface index:        21
  Sample rate:            3000
  Counter sample interval: 7200
  Maximum header size:    100
  Receiver index:         1
```

Related Commands

Command	Description
<code>show sflow config</code>	Shows sFlow global configuration.
<code>show sflow counters</code>	Shows sFlow global counters.

show sntp

show sntp

Description

Shows Simple Network Time Protocol information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the SNTP information.

```
DmSwitch#show sntp
  Current time: Tue Aug  8 10:02:06 2006

  SNTP Status: enabled
  SNTP poll interval: 30
  SNTP server 1: 200.132.0.132

  Last successful update: 8 s ago.
    Server used: 200.132.0.132
  Next attempt: in 22 s.
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include

Command

sntp

Description

Configures the Simple Network Time Protocol.

show spanning-tree

show spanning-tree

show spanning-tree configuration

show spanning-tree *instance* [**table**]

show spanning-tree *instance* [**ethernet** [*unit-number/*] *port-number* | **port-channel** *channel-group-number*]

Description

Shows spanning-tree configuration and status.

Output modifiers are available for this command.

Syntax

Parameter	Description
configuration	Shows global spanning-tree configurations.
<i>instance</i>	Specifies the spanning-tree instance (Range: 0-15).
ethernet [<i>unit-number/</i>]	(Optional) Shows spanning-tree instance status of a specific unit and
<i>port-number</i>	port.
port-channel <i>channel-group-number</i>	(Optional) Shows spanning-tree instance status of a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)
table	(Optional) Shows spanning-tree instance status in table format.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15. The configuration parameter was added. Without arguments, the command displays information for all instances. The command output was changed to a more compact format.

Usage Guidelines

You can use this show command to display global, per-instance and per-interface configuration and status for the spanning-tree protocol.

Example

This example illustrates how to show the spanning-tree global configuration.

```
DmSwitch#show spanning-tree configuration

Spanning-tree information
-----
Spanning tree mode:          RSTP
BPDU filter status:         Disabled
BPDU guard status:          Disabled
MST name:
MST revision:                0
MST configuration digest:    0xE13A80F11ED0856ACD4EE3476941C73B

Instance      Protected VLANs
-----
1 (RSTP01)    All

DmSwitch#
```

This example illustrates how to show the spanning-tree instance status.

```
DmSwitch#show spanning-tree 1

Spanning-tree 1 (RSTP01) information
-----
Members:          All VLANs
Bridge info:       32769.0004df006a23, priority: 32768 + ID 1
Root info:         32769.0004df006992, port: PortCh 1, cost: 200000
Bridge times:      hello: 2, forward: 15, max age: 20, max hops: 20
Root times:        hello: 2, forward: 15, max age: 20
Topology changes:  total: 9, last: 13563s

Unit 1            2  4  6  8 10 12 14 16 18 20 22 24 26 28
                                RF RF
                                RF RF
                    1  3  5  7  9 11 13 15 17 19 21 23 25 27

DmSwitch#
```

This example illustrates how to show the spanning-tree interface status.

```
DmSwitch#show spanning-tree 1 ethernet 1/1
Eth 1/ 1 information
-----
Role / State:      Root Forwarding
Port info:         id: 128.1, priority: 128, cost: 200000
Root info:         32769.0004df006992, cost: 0
Designated info:   32769.0004df006992, port: 128.1
Edge port:         admin: disabled, oper: disabled
```

```

Link type:          admin: auto, oper: point-to-point
Received BPDUs:     STP Config.: 0, STP TCN: 0, RSTP/MSTP: 3
Transmitted BPDUs:  STP Config.: 0, STP TCN: 0, RSTP/MSTP: 3
Detected version:    RSTP (version 2) or newer
Restricted role:     disabled
Restricted TCN:      disabled

```

DmSwitch#

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree <i>instance</i>	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree <i>instance</i> forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree <i>instance</i> hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree <i>instance</i> max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree <i>instance</i> max-hops	Configures the Spanning-Tree Algorithm maximum hops parameter.
spanning-tree <i>instance</i> priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree <i>instance</i> vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type (Interface configuration)	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.

show stacking

show stacking

Description

Shows stacking information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced on pizza-box stacking.
14.0	This command was introduced on chassis stacking.

Usage Guidelines

This command shows stacking-related information.

For pizza-box stacking, both global stacking information such as stack status and topology, and local attributes (e.g. MAC address, priority, stacking port and synced status of each unit) are displayed.

For chassis stacking, local attributes such as MAC address, role, data channels and control channels of each unit are displayed.

Example

This example illustrates the output generated by the command for pizza-box stacking.

DmSwitch#show stacking

Unit	MAC Address	Priority	Role	Port S1	Port S2	Synced Status
1	00:04:DF:62:87:C5	150	Master	Up	Up	RST
3	00:04:DF:1A:9D:D8	10	Slave	Up	Up	R-T
4	00:04:DF:62:89:0F	2	Slave	Up	Up	R-T
7	00:04:DF:62:89:4B	0	Slave	Up	Up	R-T


```

Stacking information:

Stacking state: Enabled
Status:  connected, 4 units total
Topology: Ring

Synced status: (R) Running config, (S) Startup config,
               (T) Saved topology, (-) Not synced.

DmSwitch#

```

This example illustrates the output generated by the command for chassis stacking.

```

DmSwitch#show stacking

Unit  MAC Address           Role           Data-Channels*  Control-Channels*
-----
1-A   00:04:DF:17:8D:D0  MPU-Active     6/6/16          5/5/7
1-B   00:04:DF:16:6C:53  MPU-Standby    0/0/16          2/2/7
2     00:04:DF:1A:98:B2  Intf-Card      2/2/2           1/1/1
4     00:04:DF:1B:34:E9  Intf-Card      4/4/4           1/1/1

(*) Up/Expected/Total

DmSwitch#

```

Related Commands

Command	Description
show stacking priority	Show local unit's stacking priority
show stacking saved-topology	Show stacking saved topology
show stacking synced-status	Show stacking synced status
stacking	Manage stacked switches

show stacking priority

show stacking priority

Description

Shows local unit's stacking priority in a pizza-box stack.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
10.4	This command was introduced.

Usage Guidelines

Use command **show stacking priority** to view local unit's stacking priority.

This command is available only for boards that support pizza-box stacking.

Example

This example illustrates the output generated by the command.

```
DmSwitch#show stacking priority
Stacking priority: 0

DmSwitch#
```

Related Commands

Command	Description
stacking	Manage stacked switches
show stacking	Show stacking information

Command	Description
<code>show stacking saved-topology</code>	Show stacking saved topology
<code>show stacking synced-status</code>	Show stacking synced status

show stacking saved-topology

show stacking saved-topology

Description

Shows pizza-box stacking saved topology.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command shows stacking saved-topology information. Shows MAC address, detected card and saved status of each unit. Unsaved cards are displayed in new cards section.

This command is available only for boards that support pizza-box stacking.

Example

This example illustrates the output generated by the command.

```
DmSwitch#show stacking saved-topology
Saved Topology:
Unit  MAC Address           Detected  Status
----  -
1      00:04:DF:1A:9D:D8   Yes      Ok
2      00:04:DF:62:87:C5   Yes      Ok
3      00:04:DF:62:89:4B   Yes      Ok
```

```
New Cards (*):
Unit  MAC Address
----  -
4      00:04:DF:62:89:0F
```

(*) To add new cards in the desired topology is necessary to use the command stacking save-topology.

DmSwitch#

Related Commands

Command	Description
show stacking	Show stacking information
show stacking priority	Show local unit's stacking priority
show stacking synced-status	Show stacking synced status
clear stacking saved-topology	Clear stacking saved topology information.
stacking	Manage stacked switches

show stacking synced-status

show stacking synced-status

Description

Shows pizza-box stacking synced status.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command shows stacking synced-status information. Shows MAC address, role and synced status of each unit. If the card has the correct CRC displays "Synced", otherwise "Not Synced".

This command is available only for boards that support pizza-box stacking.

Example

This example illustrates the output generated by the command.

```
DmSwitch#show stacking synced-status
```

Unit	MAC Address	Role	Running Config	Startup Config	Saved Topology
1	00:04:DF:62:89:0F	Master	Synced	Synced	Synced
2	00:04:DF:1A:9D:D8	Slave	Synced	Unknown	Synced
3	00:04:DF:62:87:C5	Slave	Synced	Unknown	Synced
5	00:04:DF:62:89:4B	Slave	Synced	Unknown	Not Synced

```
DmSwitch#
```

Related Commands

Command	Description
<code>show stacking</code>	Show stacking information
<code>show stacking priority</code>	Show local unit's stacking priority
<code>show stacking saved-topology</code>	Show stacking saved topology
<code>stacking</code>	Manage stacked switches

show startup-config

show startup-config

Description

Shows the startup flash configuration.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command shows the stored configuration in a specific flash memory position set as startup. It also shows the configuration in the same structure that the information presented in the **show running-config** command.

Example

This example illustrates how to show the startup flash configuration.

```
DmSwitch#show startup-config
Building configuration...
!
hostname DmSwitch
!
username admin access-level 15
username admin password 7 d033e22ae348aeb5660fc2140aec35850c4da997
username guest access-level 0
username guest password 7 35675e68f4b5af7b995d9205ad0fc43842f16450
!
ip telnet server
ip http server
ip http secure-server
no ip ssh server
!
ip snmp-server community public ro
!
```



```
interface vlan 1
  name DefaultVlan
  ip address 192.168.0.25/24
  set-member untagged ethernet all
!
spanning-tree 1
spanning-tree 1 vlan all
!
DmSwitch#
```

Related Commands

Command	Description
copy	Copies configuration and firmware.
erase	Erases spare firmware or configuration position.
select	Selects the startup firmware and flash for the next reboot.
show flash	Shows flash information.
show flash-config	Shows the configuration stored in a specific flash position.
show running-config	Shows the current operating configuration.

show sync-source

show sync-source unit { { **range** *first-unit last-unit* } | **all** | *unit-number* }

Description

Shows information about sync-source.

Syntax

Parameter	Description
all	Show information of all units.
range [<i>first-unit</i>] [<i>last-unit</i>]	Show information of a range of units.
<i>unit-number</i>	Show information about an specific unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example show all synchronization source global configuration on unit 1.

```
DM4000(config)#show sync-source unit 1
Synchronization Source Unit 1 Global Configuration:
  Sync Switching:                Enable
  Revertive:                     Enable
  External Clock
    Operation Mode:              2MHz

DM4000(config)#
```

Related Commands

No related command.

show sync-source bits-clock-mode

```
show sync-source unit { { range first-unit last-unit } | all | unit-number }  
bits-clock-mode
```

Description

Shows information of sync-source external clock mode.

Syntax

Parameter	Description
all	Show information of all units.
range [<i>first-unit</i>] [<i>last-unit</i>]	Show information of a range of units, defined from <i>first-unit</i> to <i>last-unit</i> .
<i>unit-number</i>	Show information about an specific unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example show external clock port operation mode on unit 2.

```
DM4000show sync-source unit 2 bits-clock-mode  
External Clock unit 2 Status  
  Operation mode:                2Mbps Unframed (HDB3)  
DM4000#
```

Related Commands

Command	Description
<code>sync-source</code> <code>bits-clock-mode</code>	Configure the bits clock mode of source used to synchronize

show sync-source hierarchy

```
show sync-source unit { { range first-unit last-unit } | all | unit-number }  
hierarchy { { range first-hier last-hier } | all | hierarchy-level }
```

Description

Show information of sync-source hierarchy.

Syntax

Parameter	Description
all	Show information of all units.
range <i>first-unit last-unit</i>	Show information of a range of units, defined from <i>first-unit</i> to <i>last-unit</i> .
<i>unit-number</i>	Shows information about an especific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example show all synchronization source hierarchy on unit 1.

```
DM4000#show sync-source unit 1 hierarchy 1
Sync Source unit 1 Hierarchy 1
Configuration:
  Transmit Source Clock:      Internal

Status:
  Hierarchy in use:          Yes
  Out of limits:             No
  Status Detail:             Locked

DM4000#
```

Related Commands

No related command.

show sync-source status

```
show sync-source unit { { range first-unit last-unit } | all | unit-number } status
```

Description

Shows status of sync-source.

Syntax

Parameter	Description
all	Show information of all units.
range [<i>first-unit</i>] [<i>last-unit</i>]	Show information of a range of units, defined from <i>first-unit</i> to <i>last-unit</i> .
<i>unit-number</i>	Show information about an specific unit.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows synchronization source status on unit 1.

```
DM4000#show sync-source unit 1 status
Sync Source Unit 1 Status
  Active Clock Type:          Internal
  Active Hierarchy:           1
  Status Detail:              -
DM4000#
```


Related Commands

Command	Description
<code>sync-source hierarchy enable</code>	Configure the source used to synchronize

show system

show system

Description

Shows system information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.0	Command output reorganized.
13.4	The master switch will also print other units system information.

Usage Guidelines

You can use this show command to see the product model, capabilities, licences, factory serial number, host-name, location and other characteristics.

The master switch will also print other units system information.

Example

This example illustrates how to show the system information.

```
DmSwitch#show system
```

```
Unit 1-A (Active)
```

```
Product
```

```
Model: DM4008 - MPU384
```

```
OID: 1.3.6.1.4.1.3709.1.2.40
```

```
Factory
```

```
Mainboard ID: 1270916
```

```
MAC Address: 00:04:DF:16:9E:5A
```

```
System Capabilities HW Available License Enabled
```

```
Bridge: yes yes
```

```

Router:          yes          yes
MPLS:           yes          yes
User configurable
Name:           DmSwitch
Location:       Brazil
Contact:        Datacom

Unit 1-B (Standby)
Product
Model:          MPU384
Factory
ID:             949944
MAC Address:    00:04:DF:13:30:DB
System Capabilities HW Available License Enabled
Bridge:         yes          yes
Router:         yes          yes
MPLS:           yes          yes

Unit 4
Product
Model:          ETH24GX+2x10GX
Factory
Mainboard ID:   1030915
MAC Address:    00:04:DF:14:99:4E
System Capabilities HW Available License Enabled
Bridge:         yes          yes
Router:         yes          yes
MPLS:           yes          no

```

Related Commands

Command	Description
hostname	Specifies a host name.
ip snmp-server	Configures the internal SNMP server.

show tacacs-server

show tacacs-server

Description

Shows global TACACS information and all configured servers.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the TACACS server information.

```
DmSwitch#show tacacs-server

TACACS+ configuration:
  Default Key:                None
  Authentication:
    Authentication type:      PAP
    Timeout (s):              10
    Default port:             49
  Authorization:
    Timeout (s):              3
    Default port:             49
  Accounting:
    Authentication type:      PAP
    Timeout (s):              10
    Default port:             49

DmSwitch#
```

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

show tech-support

```
show tech-support [detail | 12 | 13 | mpls | stacking] [| {tftp  
ip-address filename }]
```

Description

Shows relevant information to be used by technical support.

Syntax

Parameter	Description
detail	(Optional) Show detailed information.
12	(Optional) Show layer 2 information.
13	(Optional) Show layer 3 information.
mpls	(Optional) Show MPLS information.
stacking	(Optional) Show Stacking information.
 tftp	(Optional) Send output to TFTP server.
ip-address	IP address of remote host.
filename	File name.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
6.0	This command was introduced.
9.6	Options L2 and L3 were introduced.
13.0	Option TFTP was introduced.
14.2	Option MPLS was introduced.
14.4	Option Stacking was introduced.

Usage Guidelines

Entering this command without parameters, basic technical support information will be shown.

Example

Not available.

Related Commands

No related command.

show terminal

show terminal

Description

Shows terminal information.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
5.0	This command was introduced.
11.0	This command was modified to show information about login-timeout.

Usage Guidelines

Not available.

Example

This example illustrates how to show the terminal information.

```
DmSwitch#show terminal

Login timeout (s):  60
Terminal paging:    Enabled
Session timeout (s): 3600

DmSwitch#
```

Related Commands

Command	Description
terminal paging	Shows terminal one screenful at a time.

Command	Description
<code>terminal timeout</code>	Sets an idle timeout for terminal.

show terminal encrypted-data

`show terminal encrypted-data`

Description

Display status of encryption for secret data (such as passwords and keys) for the current terminal session.

No parameter accepted.

Default

No default is defined.

Commands Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

Not available.

Related Commands

Command	Description
<code>terminal encrypted-data</code>	Display secret data using encrypted format.

show units

show units

Description

Shows information about system units.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the system units information.

```
DmSwitch#show units
```

Unit	Model	ID	Firmware	Stacking Version	Bootloader Version
1	DmSwitch3324F2	688125	7.6	4	1.1.2-10

```
DmSwitch#
```

Related Commands

Command	Description
show firmware	Shows firmware information.

show chassis-load-balance ^[1] ^[5] ^[6] ^[8] ^[9]

show chassis-load-balance

Description

Shows information about port selection criteria used for load balance of traffic in the internal chassis connections.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.10.10	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the load balance configuration for all system units.

```
DmSwitch#show chassis load-balance

Unit  Load-balance criteria
----  -
2  Destination IP
3  Enhanced (MPLS, IP, MAC, TCP/UDP)
4  Enhanced (MPLS, IP, MAC, TCP/UDP)
DmSwitch#
```

Related Commands

Command	Description
---------	-------------

Command	Description
<code>chassis load-balance</code>	Configures load balance for internal chassis connections.

show uptime

show uptime

Description

Shows the system uptime and the estimated started time for all units connected.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Units information was added.

Usage Guidelines

Not available

Example

This example illustrates how to show the system uptime and estimated started time.

```
DmSwitch#show uptime
Local
System uptime: 10 m, 45 s
Estimated startup time: Tue Oct 15 13:50:08 2013

Unit 2
System uptime: 10 m, 40 s
Estimated startup time: Tue Oct 15 13:50:13 2013

Unit 3
System uptime: 10 m, 47 s
Estimated startup time: Tue Oct 15 13:50:06 2013

DmSwitch#
```

Related Commands

Command	Description
<code>show clock</code>	Shows the system clock and time zone.
<code>show cpu</code>	Shows CPU information.

show users

show users

Description

Shows the users information.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example illustrates how to show the users information.

```
DmSwitch#show users
USER                                ACCESS  LEVEL  PASSWORD
-----
admin                               15      d033e22ae348aeb5660fc2140aec35850c4da997
guest                               0       35675e68f4b5af7b995d9205ad0fc43842f16450

DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
username	Creates users and configures access to the DmSwitch.

show vlan

```
show vlan [ id index | name name ]
```

```
show vlan
```

```
show vlan summary id { index | all | range first_index last_index }
```

```
show vlan table [ id { index | range first_index last_index } | name name ]
```

Description

Shows the Virtual LAN settings.

Output modifiers are available for this command.

Syntax

Parameter	Description
id <i>index</i>	(Optional) Shows VLAN settings from a specific VLAN ID. (Range: 1-4094)
name <i>name</i>	(Optional) Shows VLAN settings from a specific VLAN name.
table	(Optional) Shows VLAN settings in table format.
range <i>first_index last_index</i>	(Optional) Shows VLANs on a given range settings
summary	(Optional) Shows a summary of a VLAN settings
all	(Optional) Shows a summary of all VLANs settings
range	(Optional) Shows a summary of a given range of VLANs settings

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
8.0	Introduced MPLS information.
13.0	Introduced range option and summary command.

Usage Guidelines

Entering this command without parameters, all VLAN settings will be shown.

You can use this command to inspect MPLS configuration done on the specified VLAN.

Example

This example illustrates how to show the VLAN settings from a specific VLAN index.

```
DmSwitch#show vlan id 1
VLAN:                1 [VlanName]
Type:                Static
Status
  Admin:              Enabled
  Oper:               Up
IP Address:          143.54.83.172/28
IP Directed Broadcast: Disabled
Management MTU:      1500
Link Detection:      Disabled
Proxy ARP:           Disabled
STP:                 on instance 1
Members:             Eth1/1 (static, untagged)
                   Eth1/4 to Eth1/28 (static, untagged)
                   Port-Channel01 (static, untagged)
MPLS:                Disable
Forwarding VRF:       (none)
Forwarding VPWS:      (none)

DmSwitch#show vlan id 122
VLAN:                122 [L2]
Type:                Static
Status
  Admin:              Enabled
  Oper:               Up
MAC Learn:           Enable
Link Detection:      Disabled
Proxy ARP:           Disabled
Members:             Eth1/10 (static, tagged)
Forbidden:           (none)
MPLS:                Disable
Forwarding VRF:       (none)
Forwarding VPWS:      PWID pwid=1002 group_id=121 (Peer 100.100.100.11)

DmSwitch#show vlan id 130
VLAN:                130 [L3]
Type:                Static
Status
  Admin:              Enabled
  Oper:               Up
IP Address:          10.1.130.15/24
IP Directed Broadcast: Disabled
Management MTU:      1500
MAC Learn:           Enable
Link Detection:      Disabled
Proxy ARP:           Disabled
Members:             Eth1/10 (static, tagged)
Forbidden:           (none)
```

```

MPLS:                               Disable
Forwarding VRF:                     vpn1
Forwarding VPWS:                     (none)

DmSwitch#show vlan id 131
VLAN:                               131 [L3_MPLS]
Type:                               Static
Status
  Admin:                            Enabled
  Oper:                             Up
IP Address:                         10.1.131.1/24
IP Directed Broadcast:              Disabled
Management MTU:                    1500
Link Detection:                     Disabled
Proxy ARP:                          Disabled
Members:                           Eth1/11 (static, tagged)
Forbidden:                          (none)
MPLS:                               Forwarding Enabled
Forwarding VRF:                     (none)
Forwarding VPWS:                     (none)

DmSwitch#show vlan id 200
VLAN:                               200 [MPLS_PE2_P2]
Type:                               Static
Status
  Admin:                            Enabled
  Oper:                             Up
IP Address:                         192.168.200.1/30
IP Directed Broadcast:              Disabled
Management MTU:                    1500
MAC Learn:                          Enable
Link Detection:                     Enabled
Proxy ARP:                          Disabled
Members:                           Eth1/6 (static, untagged)
Forbidden:                          (none)
MPLS:                               Enable
Forwarding VRF:                     (none)
Forwarding VPWS:                     (none)

DmSwitch#

```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
clear mac-address-table	Erases entries stored in the MAC address table.
ip address	Sets an IP address for the selected VLAN.
ip directed broadcast	Configures IP Directed Broadcast forwarding for the selected VLAN.
ip vrf forwarding	Configures the selected VLAN to use the specified VRF instance.
ip proxy-arp	Enables proxy ARP on selected VLAN.
set-member forbidden	Adds via GVRP forbidden members to a selected VLAN.
set-member tagged	Adds tagged members to selected VLAN.
set-member untagged	Adds untagged members to selected VLAN.
show ip vrf	Shows VRF general information.
show mac-address-table	Shows the MAC address table.

Command	Description
shutdown (VLAN configuration)	Deactivates the selected VLAN.
spanning-tree <i>instance</i> vlan-group	Adds VLAN groups to a spanning-tree instance.

show vlan-group

show vlan-group [*id index*]

Description

Shows the VLAN group settings.

Output modifiers are available for this command.

Syntax

Parameter	Description
<i>id index</i>	(Optional) Shows VLAN group settings from a specific group. (Range: 0-31)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, all VLAN group settings will be shown..

Example

This example illustrates how to show the VLAN group settings.

```
DmSwitch#show vlan-group

VLAN Group 1
STP protected:      1
EAPS protected:    (none)
Member VLANs:      VLAN 15 to VLAN 20

VLAN Group 2
STP protected:      1
EAPS protected:      5
```

```
Member VLANs:          VLAN 1 to VLAN 14
```

```
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
eaps domain	Defines the VLAN groups that will be protected by EAPS ring.
protected-vlans	
spanning-tree <i>instance</i>	Adds VLAN groups to a spanning-tree instance.
vlan-group	
vlan-group	Create a VLAN group and manage its members.

show vlan-mac-table ^[1]

show vlan-mac-table [**resources** | **mac-address** *mac-address* | **vlan** *vlan-id*]

Description

Shows the VLAN MAC table.

Syntax

Parameter	Description
resources	(Optional) Shows VLAN MAC table hardware resources.
mac-address <i>mac-address</i>	(Optional) Searches for an entry that matches this MAC address.
vlan <i>vlan-id</i>	(Optional) Searches for an entry that matches this VLAN ID. (Range: 1-4094)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Entering this command without parameters, the entire VLAN MAC table will be shown.

Example

This example illustrates how to show the VLAN MAC table to a specific VLAN.

```
DmSwitch#show vlan-mac-table vlan 1
Entries
Unit  MAC                      VLAN  Prio
-----
1    00:03:DF:34:43:23          1      2
1    00:03:DE:33:43:24          1      5

DmSwitch#
```


Related Commands

Command	Description
vlan-mac-table source-mac	

show vrrp

```
show vrrp [ { vlan vlan-id | group group | summary [ | { after | begin | exclude | include } expression ] } ]
```

Description

Shows Virtual Router Redundancy Protocol information.

Syntax

Parameter	Description
vlan <i>vlan-id</i>	(Optional) Filter VRRP information by the parent VLAN id. (Range: 1-4094)
group <i>group</i>	(Optional) Filter VRRP information by its GROUP id. (Range: 1-255)
summary	(Optional) Show VRRP summary table.
after	(Optional) Print lines after matching a pattern.
begin	(Optional) Print lines in which the beginning matches a pattern.
exclude	(Optional) Print lines not matching a pattern.
include	(Optional) Print lines matching a pattern.
<i>expression</i>	Regular expression to be used as a pattern. The following metacharacters must be backslashed: , (,), {, } and +.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.
13.0	The options vlan , group and summary were introduced. Virtual IPv6 address was added.
13.4	Secondary virtual IP address was added.

Usage Guidelines

Not available.

Example

This example illustrates how to show the VRRP information.

```
DmSwitch#show vrrp
VLAN 2 - Group 100
  State is Master
  Virtual IP address(es):
    10.0.2.1
    10.0.3.1 secondary
  Virtual IPv6 address is 1001::2
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 10.0.2.254/24 (local), priority is 150

VLAN 3 - Group 101
  State is Master
  Virtual IP address(es):
    10.0.4.1
    10.0.5.1 secondary
  Virtual IPv6 address is 1002::2
  Virtual MAC address is 0000.5e00.0165
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 10.0.4.254/24 (local), priority is 100
DmSwitch#
```

It is possible to display only the desired VRRP information. This example shows the output filtering by VLAN 2 and VRRP group 100. Note that the outputs are equal.

```
DmSwitch#show vrrp vlan 2
VLAN 2 - Group 100
  State is Master
  Virtual IP address(es):
    10.0.2.1
    10.0.3.1 secondary
  Virtual IPv6 address is 1001::2
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 10.0.2.254/24 (local), priority is 150

DmSwitch#
DmSwitch#show vrrp group 100
VLAN 2 - Group 100
  State is Master
  Virtual IP address(es):
    10.0.2.1
    10.0.3.1 secondary
  Virtual IPv6 address is 1001::2
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 10.0.2.254/24 (local), priority is 150
DmSwitch#
```

This example presents the overview table for all the VRRP entries.

```
DmSwitch#show vrrp summary
```

```
-----+-----+-----+-----
VLAN | GROUP | Prio | State
-----+-----+-----+-----
    2 |   100 |   150 | Master
    3 |   101 |   100 | Master
-----+-----+-----+-----
```

```
Number of entries: 2
```

```
DmSwitch#
```

Filters can be applied to the summary output. In this example the lines containing "150" were excluded.

```
DmSwitch#show vrrp summary | exclude 150
```

```
-----+-----+-----+-----
VLAN | GROUP | Prio | State
-----+-----+-----+-----
    3 |   101 |   100 | Master
-----+-----+-----+-----
```

```
Number of entries: 2
```

```
DmSwitch#
```

Related Commands

Command	Description
vrrp ip	Configures VRRP IP on a VLAN.
vrrp ipv6	Configures VRRP IPv6 on a VLAN.
vrrp priority	Configures the priority for a VRRP group.
vrrp shutdown	Configures the VRRP group status.
show ip interface	Shows the interface information.
show ipv6 interface	Shows IPv6 interface information.

show warnings

show warnings [units]

Description

Shows system warnings.

Output modifiers are available for this command.

Syntax

Parameter	Description
units	(Optional) Shows system warnings units.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Entering this command without parameters, all system warnings will be shown.

Example

This example illustrates how to show the warnings from the units.

```
DmSwitch#show warnings units
```

- The system contains H-Series units with enabled external memory together with E-Series units.
- The system contains H-Series units with and without external memory enabled.
- The system contains H-Series units with external memory operating in different modes.

```
DmSwitch#
```

Related Commands

Command	Description
<code>output modifiers</code>	Options to filter text output: after, begin, exclude and include
<code>show memory external</code>	Shows memory configuration.
<code>show units</code>	Shows information about system units.

show wred

show wred [**ethernet** [*unit-number/*] *port-number* | **port-channel** *port-channel-number*]

Description

Use to show the wred information.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Shows a specific unit and port wred information. (Range: 1-1/1-28)
port-channel <i>port-channel-number</i>	(Optional) Shows a specific port-channel wred information. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Entering this command without parameters, the WRED information for all ports will be shown.

Example

This example illustrates how to show the wred information.

```
DmSwitch#show wred ethernet 1
```

WRED settings:

DSP: Drop start point value / Slope angle

CNG: Congestion threshold drop start point value / Slope angle

					Queue				
Port	Item	1	2	3	4	5	6	7	8
-----	----	-----	-----	-----	-----	-----	-----	-----	-----

```
1/ 1          DSP      75/15  75/15  75/15  75/15  75/15  75/15  75/15  75/15
              CNG      100/15 100/15 100/15 100/15 100/15 100/15 100/15 100/15
```

DmSwitch#

Related Commands

Command	Description
wred	Enables Weighted Random Early Detection (WRED)

ssh

ssh { *host* [*port-number*] | **remote-device** *unit/port* [**port** *port-number*] [**user** *name*] }

Description

Allows you to ssh from the current command-line interface session to another switch, to a host or to a remote device.

Syntax

Parameter	Description
<i>host</i>	Specifies the IP or host-name to connect.
<i>port-number</i>	(Optional) Specifies the port-number.
remote-device <i>unit/port</i>	SSH to a remote-device connected to the unit/port.
port <i>port-number</i>	(Optional) Specifies the port-number.
user <i>username</i>	(Optional) Specifies the username.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.6	This command was introduced.
11.2	Option remote-device added.

Usage Guidelines

Not available.

Example

This example shows how to start a ssh connection to a host or to another DmSwitch.

```
DmSwitch#ssh 192.168.0.1
```

```
Another_DmSwitch login:
```

This example shows how to start a ssh connection to a remote-device connected in DmSwitch.

```
DmSwitch#ssh remote-device 1/10 user guest
```

```
Remote_Device login:
```

Related Commands

Command	Description
<code>show remote-devices</code>	Remote device management configuration and status.

stacking

```
stacking { change-master unit unit-id | enable | priority priority | save-topology |  
sync-all-flash | swap-unit unit unit-id with unit-id }
```

no stacking

Description

This command allows you to manage stacked switches and configure pizza-box stacking parameters.

This command actually comprises six subcommands, which are described in section Syntax.

Inserting **no** as a prefix for this command will disable pizza-box stacking.

Syntax

Parameter	Description
change-master unit <i>unit-id</i>	Change master to another unit. (Range: 2-8)
enable	Enable stacking.
priority <i>priority</i>	Change local unit's priority. (Range: 0-32)
save-topology	Saves the current topology.
sync-all-flash	Synchronize all flash-config positions.
swap-unit unit <i>unit-id</i> with <i>unit-id</i>	Swap two unit board models in the running-config.

Default

Stacking is enabled.

Stacking priority is zero.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed from stacking to stacking keys .
10.4	This command was renamed from stacking keys to stacking . Subcommands change-master , enable , priority , and swap-unit were introduced, as well as the no prefix functionality.

Release	Modification
13.0	Subcommand sync-all-flash was introduced.
13.4	Subcommand save-topology was introduced.

Usage Guidelines

Pizza-box stacking means stacking of standalone switches, so that they behave like a single equipment. The products that support pizza-box stacking are switches from DM4100 product line.

Use **no stacking** to disable pizza-box stacking functionality (which is enabled by default), and **stacking enable** to re-enable it.

Unit priorities are useful to define which unit will become the master after a normal reboot or in case the current master leaves the stack. The unit having the highest priority value will become the master. Use the command **stacking priority** to change the unit's priority in the stack. If all priorities are equal, units' MAC addresses define which unit becomes master.

Use **stacking change-master** to force that a given unit becomes the master. This command reboots the old master and *temporarily* overrides current priority scenario, making the desired unit the new master. After the new master is up, if all units are rebooted (i.e., by entering **reboot** in the CLI), the old priority scenario takes place and the unit with the highest priority becomes the master again.

The command **stacking swap-unit** swaps two units in the running configuration. Only their unit ID's are swapped, not their configurations. If the latter are not compatible with each other, the units are reattached to the stack with the default configuration. After the command, the given units are rebooted.

The command **sync-all-flash** forces the flash synchronization with all stack units to occur, overriding any configuration saved in any slave flash position with the configuration from the master switch.

The command **save-topology** saves the current state and synchronizes with other members of the stacking. So when the stack is reordered, the information from the previous topology will be read in the new master, ensuring that MODIDs are assigned in the same manner.

Example

This example shows how to disable pizza-box stacking.

```
DmSwitch#no stacking
Done. This command will take effect after the next reboot.

DmSwitch#
```

This example shows how to enable pizza-box stacking, in case you have disabled it.

```
DmSwitch#stacking enable
Done. This command will take effect after the next reboot.
```

```
DmSwitch#
```

This example shows how to change local unit's priority to 25.

```
DmSwitch#stacking priority 25
Done. This command will take effect after the next reboot.

DmSwitch#
```

This example shows how to make unit 2 become the master.

```
DmSwitch#stacking change-master unit 2
This command will cause traffic disruption. Continue? <y/N> y
System restart requested via stacking.

Restarting system.
```

This example shows how to swap units 2 and 3 in the running-config, given that they are not compatible.

```
DmSwitch#stacking swap-unit unit 2 with 3
This command will cause traffic disruption. Continue? <y/N> y

Informed units are different models: configuration might be incompatible
You can force the configuration swap, being aware that in case of
incompatibility the default configuration will be applied.
Are you sure you want to continue? <y/N> y
Rebooting unit 2.
Rebooting unit 3.
```

You can verify current stacking scenario by entering the **show stacking** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show stacking	Show stacking information
show stacking priority	Show local unit's stacking priority
show stacking saved-topology	Show stacking saved topology
show stacking synced-status	Show stacking synced status
show units	Shows information about system units.
clear stacking saved-topology	Clear stacking saved topology information.

telnet

telnet { *host* [*port-number*] | **remote-device** *unit/port* [**port** *port-number*] }

Description

Allows you to Telnet from the current command-line interface session to another host or remote device.

Syntax

Parameter	Description
<i>host</i>	Specifies the IP or host-name to connect to.
<i>port-number</i>	(Optional) Specifies the port-number.
remote-device <i>unit/port</i>	Telnet to a remote-device connected to the unit/port.
port <i>port-number</i>	(Optional) Specifies the port-number.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
11.2	Option remote-device added.

Usage Guidelines

Not available.

Example

This example shows how to start a telnet connection to a host or to another DmSwitch.

```
DmSwitch#telnet 192.168.0.1
```

```
Entering character mode  
Escape character is '^'.
```

```
Another_DmSwitch login:
```

This example shows how to start a telnet connection to a remote-device connected in DmSwitch.

```
DmSwitch#telnet remote-device 1/10
```

```
Entering character mode  
Escape character is '^]'.  

```

```
Remote_Device login:
```

Related Commands

Command	Description
show remote-devices	Remote device management configuration and status.

terminal aux

terminal aux unit *unit-number*

Description

Configure the auxiliary console port.

Syntax

Parameter	Description
unit <i>unit-number</i>	Indicates the unit for connect terminal aux. (Range: 1-8)[1]

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how set terminal aux.

```
DmSwitch#terminal aux unit 3
DmSwitch#
```

Related Commands

No related command.

terminal encrypted-data

terminal encrypted-data

no terminal encrypted-data

Description

Display secret data (such as passwords and keys) using encrypted format instead of masked format.

Inserting **no** as a prefix for this command disable encryption for display of secret data.

Syntax

No parameter accepted.

Default

Disable

Commands Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable encrypted-data.

```
DmSwitch#terminal encrypted-data
DmSwitch#
```

You can verify that the encrypted-data was enable by entering **show terminal encrypted-data** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show terminal encrypted-data</code>	Show status of encryption for secret data
<code>show running-config</code>	Shows the current operating configuration.

trace mpls

```
trace mpls { ldp ip-address/mask | rsvp tunnel-id } [ destination ip-address ] [ exp priority ] [ reply-mode { udp-ipv4 | router-alert } ] [ size value ] [ padding value ] [ timeout seconds ] [ ttl value ] [ verbose]
```

Description

Use **trace mpls** to inspect the route that packets actually take when forwarded within an Label and Switched Path (LSP) to arrive to their destination.

Syntax

Parameter	Description
ldp <i>ip-address/mask</i>	Specifies the LSP type as LDP for a FEC and Prefix Length
rsvp <i>tunnel-id</i>	Specifies the LSP type as RSVP tunnel with the specific tunnel ID.
destination <i>ip-address</i>	(Optional) Specifies an 127/8 address as destination.
exp <i>priority</i>	(Optional) Specifies the EXP bits value in the MPLS header of packets. Range: 0-7. Default: 0
reply-mode udp-ipv4	(Optional) Specifies IPv4 UDP as the reply mode for MPLS echo reply packet. Default: udp-ipv4.
reply-mode router-alert	(Optional) Specifies IPv4 UDP with router alert as the reply mode for MPLS echo reply packet. Default: udp-ipv4.
size <i>value</i>	(Optional) Specifies the packet size in bytes.
padding <i>value</i>	(Optional) Specifies value to fill the pad TLV. Default: 0xFF.
timeout <i>seconds</i>	(Optional) Specifies the timeout interval (in seconds). Default: 2 seconds.
ttl <i>value</i>	(Optional) Specifies a maximum hop count. Default: 30.
verbose	(Optional) Enable the verbose output of commands.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **trace mpls** command is used to inspect each hop along the LSP that packets actually pass through when traveling to their destination.

MPLS echo request packets with incremental TTL are repeatedly sent within the LSP. The router where TTL expires responds with an MPLS echo reply packet. This process finishes when the egress LSR sends its response, or if TTL reaches the maximum value.

Example

This example shows how to trace an LDP LSP to FEC 100.100.100.3/32, sending packets to destination address 127.0.0.100

```
DmSwitch#traceroute mpls ldp 100.100.100.3/32 destination 127.0.0.100

LSP Traceroute transaction ID 1:
  Message size: 100 bytes
  Reply mode: Reply via UDP IPv4
  Interval 1000 ms, Timeout 2000 ms, TTL 255, EXP 0x0
  Seq. 0 from 100.100.100.0
    [DS Router: 100.100.100.1, DS Iface: 100.100.100.1, MTU: 1500, Depth Limit: 0]
      {Label: 16 | Exp: 0 | BoS: 1 | Protocol: 3}
  Seq. 1 from 100.100.100.1, return 8 (1), 7.92 ms
    [DS Router: 100.100.100.2, DS Iface: 100.100.100.2, MTU: 1500, Depth Limit: 255]
      {Label: 19 | Exp: 0 | BoS: 0 | Protocol: 4}
      {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}
  Seq. 2 from 100.100.100.2, return 8 (1), 7.72 ms
    [DS Router: 100.100.100.3, DS Iface: 100.100.100.3, MTU: 1504, Depth Limit: 255]
      {Label: 3 | Exp: 0 | BoS: 1 | Protocol: 3}
  Seq. 3 from 100.100.100.3, return 3 (1), 11.0 ms

  Loss rate: 0.000 %

Session 1 terminated successfully
DmSwitch#
```

Example with verbose output

This example shows how to trace an LDP LSP to FEC 100.100.100.3/32, sending packets to destination address 127.0.0.100 with verbose output

```
DmSwitch#traceroute mpls ldp 100.100.100.3/32 destination 127.0.0.100 verbose

LSP Traceroute transaction ID 1:
  Message size: 100 bytes
  Reply mode: Reply via UDP IPv4
  Interval 1000 ms, Timeout 2000 ms, TTL 255, EXP 0x0
  Seq. 0 from 100.100.100.0
    There is one DownStream Mapping TLV on the response
    DownStream Information (0):
      DS Router: 100.100.100.1, DS Iface: 100.100.100.1
```

```

MTU: 1504, Depth Limit: 0
There is one label on response:
  {Label: 16 | Exp: 0 | BoS: 1 | Protocol: LDP}
Seq. 1 from 100.100.100.1, return 8 (1), 7.92 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
  DS Router: 100.100.100.2, DS Iface: 100.100.100.2
  MTU: 1500, Depth Limit: 255
  There are 2 labels on response:
    {Label: 19 | Exp: 0 | BoS: 0 | Protocol: RSVP-TE}
    {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}
Seq. 2 from 100.100.100.2, return 8 (1), 7.72 ms
There is one DownStream Mapping TLV on the response
DownStream Information (0):
  DS Router: 100.100.100.3, DS Iface: 100.100.100.3
  MTU: 1504, Depth Limit: 255
  There is one label on response:
    {Label: Implicit Null | Exp: 0 | BoS: 1 | Protocol: LDP}

Seq. 3 from 100.100.100.3, return 3 (1), 11.0 ms

Loss rate: 0.000 %

Session 1 terminated successfully
DmSwitch#

```

Related Commands

Command	Description
ping mpls	Check MPLS data plane and LSP connectivity.
show mpls ldp database	List LSP database
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

traceroute

```
traceroute { destination-host [ source source-address ] }
```

Description

Enables you to trace the routed path between the switch and a destination host.

Syntax

Parameter	Description
<i>destination-host</i>	Specifies the IP or host-name of the destination host.
source <i>source-address</i>	(Optional) IPv4 source address.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.6	New optional parameter was introduced: source .
3.1	This command was introduced.

Usage Guidelines

To use a host-name parameter, you must first configure DNS.

Each router along the path is displayed.

Example

This example shows how to trace the routed path between the switch and a destination host.

```
DmSwitch#traceroute 192.168.0.1
```

Related Commands

Command	Description
traceroute vrf	Traces the routed path between the switch and a destination endstation from a VRF.
traceroute6	Traces the IPv6 routed path between the switch and a destination end station.

traceroute vrf

```
traceroute vrf { [VRF name] [destination-host] [ source source-address ] }
```

Description

Enables you to trace the routed path between the switch and a destination host from a VRF.

Syntax

Parameter	Description
<i>VRF name</i>	Specifies the VRF name.
<i>destination-host</i>	Specifies the IP or host-name of the destination host.
source <i>source-address</i>	(Optional) IPv4 source address.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.8	This command was introduced.

Usage Guidelines

To use a host-name parameter, you must first configure DNS.

Each router along the path is displayed.

Example

This example shows how to trace the routed path between the switch and a destination host from a VRF.

```
DmSwitch#traceroute vrf blue 172.16.79.1
traceroute to 172.16.79.1 (172.16.79.1), 30 hops max, 60 byte packets
 1  172.16.79.1  1.419 ms  3.901 ms  4.164 ms
```


Related Commands

Command	Description
traceroute	Traces the routed path between the switch and a destination endstation.
traceroute6	Traces the IPv6 routed path between the switch and a destination end station.

traceroute6

```
traceroute6 { destination-host [ source source-address ] }
```

Description

Enables you to trace the IPv6 routed path between the switch and a destination host.

Syntax

Parameter	Description
<i>destination-host</i>	Specifies the IPv6 or host-name of the destination host.
source <i>source-address</i>	(Optional) IPv6 source address.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
14.6	New optional parameter was introduced: source .
12.2	This command was introduced.

Usage Guidelines

To use a host-name parameter, you must first configure DNS.

Each router along the path is displayed.

Example

This example shows how to trace the routed path between the switch and a destination host.

```
DmSwitch#traceroute6 2101::2
```

Related Commands

Command	Description
traceroute	Traces the routed path between the switch and a destination endstation.
traceroute vrf	Traces the routed path between the switch and a destination endstation from a VRF.

transceiver identification-restart

`transceiver identification-restart { interface-type } { [unit-number/] port-number }`

Description

Use to restart the transceiver identification.

Syntax

Interface Types	Description
ethernet	Inform that it's an Ethernet interface
sdh	Inform that it's an SDH interface

Parameter	Description
<code>[unit-number/] port-number</code>	Restart a specific unit and port transceiver identification

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.6	This command was introduced.
13.6	Interface type SDH was included.
14.0	Interface type Ethernet must be explicated.

Usage Guidelines

Not available.

Example

This example illustrates how to show the transceiver identification-restart.

```
DmSwitch#transceiver identification-restart sdh 3
DmSwitch#
```

Related Commands

No related command.

unit

unit *unit*

Description

Sets a default unit for the current session.

Syntax

Parameter	Description
<i>unit</i>	Specifies the new default unit. (Range: 1-8)[1]

Default

Disabled.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how set the unit 2 as the default unit.

```
DmSwitch#unit 2
DmSwitch#
```

Related Commands

No related command.

Notes

[1] - Range 1-8 available only to DM4000 Switches.

Chapter 3. Configure Commands

arp aging-time

arp aging-time *seconds*

no arp aging-time

Description

Defines the aging time of all entries in the Data plane's ARP table.

Inserting **no** as a prefix for this command will reset the aging time to the default value.

Syntax

Parameter	Description
<i>seconds</i>	Specifies the arp aging time in seconds. (Range: 200-1000000)

Default

300 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
14.4	Changed the minimal arp aging time allowed from 10s to 200s.

Usage Guidelines

ARP aging time is used to remove from the ARP table entries that are not reachable anymore. Although it's globally configured, each entry ages independently. Whenever an entry expires (i.e. entry is present on table for an 'ARP aging time' seconds cycle) it is probed and updated if an answer is received.

There are two different behaviors depending on the entry being probed. Entries that are next-hop to routes: an ARP request is sent and the entry is never removed, independent if an answer is received or not. In case of all other entries: an ARP request is sent, and it will be removed after 5 ARP request attempts failures.

Note that this command affects only the L3 Forwarding Tables. Control plane has its own ARP table and its behavior is out of the scope of this command. Depending on the L3 protocols that are running on the system, one may see extra ARP Requests to maintain the control plane's ARP Table.

Example

This example shows how to change the aging time to 1000 seconds.

```
DmSwitch#arp aging-time 1000
DmSwitch#
```

You can verify that the value was changed by entering the **show arp aging-time** privileged EXEC configuration command.

Related Commands

Command	Description
show arp aging-time	Shows arp aging-time configuration.

arp static

```
arp static { ip-address } { mac-address } { ethernet unit/port | port-channel portchannel |  
mgmt-eth } [ protection ]
```

```
no arp static { ip-address }
```

Description

Adds a static entry to the ARP table.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the destination IP address.
<i>mac-address</i>	Specifies the destination hardware (MAC) address.
ethernet <i>unit/port</i>	Specifies the Unit number/ Ethernet interface number.
port-channel <i>portchannel</i>	Specifies the Port-channel interface number.
mgmt-eth	Specifies the Management interface.
protection	Sets protection against ARP Spoofing.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The destination's IP address must match a network previously configured in a VLAN or in the management interface.

If the IP address should match a network in a VLAN interface, then an output Ethernet port or a port-channel from the same VLAN must be specified.

If parameter `protection` is given, then this ARP entry is protected against ARP Spoofing.

Example

This example shows how to add a static entry for "10.2.1.1" (in the same network as a VLAN) using the hardware address "AA:BB:CC:DD:EE:FF".

```
DmSwitch(config)#arp static 10.2.1.0 AA:BB:CC:DD:EE:FF ethernet 2/1
DmSwitch(config)#
```

This example shows how to add a static entry for "10.10.11.254" (in the same network as the management interface) the hardware address "AA:BB:CC:DD:EE:FF".

```
DmSwitch(config)#arp static 10.10.11.254 AA:BB:CC:DD:EE:FF mgmt-eth
DmSwitch(config)#
```

This example shows how to add a static entry for "10.2.1.1" (in the same network as a VLAN) using the hardware address "AA:BB:CC:DD:EE:FF" with ARP Spoofing protection.

```
DmSwitch(config)#arp static 10.2.1.0 AA:BB:CC:DD:EE:FF ethernet 2/1 protection
DmSwitch(config)#
```

You can verify that the static entry was added by entering the **show cpu arp-table** privileged EXEC command.

In case the output interface is a VLAN, the **show ip hardware host** privileged EXEC command.

Related Commands

Command	Description
show cpu arp-table	Shows ARP table information.
show ip hardware host	Shows the hardware host table.

authentication login

```
authentication login { local | tacacs | radius } [ local | tacacs | radius ] [ local  
| tacacs | radius ]
```

```
no authentication login
```

Description

Defines the login authentication method and its precedence.

Inserting **no** as a prefix for this command will reset the authentication login to the default method.

Syntax

Parameter	Description
local	Local database authentication.
radius	RADIUS server authentication.
tacacs	Configures login to TACACS server

Default

Local authentication method only.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the RADIUS authentication method as the first option, followed by Local and TACACS, respectively.

```
DmSwitch(config)#authentication login radius local tacacs
```

```
DmSwitch(config)#
```

You can verify the configured authentication method precedence by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
tacacs-server host	Configures the TACACS server IP address.
tacacs-server key	Configures the TACACS server key string.
radius-server acct-port	Configures the default RADIUS server accounting port.
radius-server auth-port	Configures the default RADIUS server authentication port.
radius-server host	Configures a specific RADIUS server.
radius-server key	Configures the default RADIUS server key string.
radius-server retries	Configures the RADIUS server retries.
radius-server timeout	Configures the RADIUS server timeout.
show authentication	Shows information about login authentication method and its precedence.
show radius-server	Shows RADIUS server information.
show running-config	Shows the current operating configuration.
show tacacs-server	Shows global TACACS information and all configured servers.

banner login

banner login

no banner login

Description

Specifies a message to be displayed before the login prompts.

Inserting **no** as a prefix for this command will delete the login banner.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

After entering the **banner login** command, start the message by entering a delimiting character of your choice, followed by one or more lines of text, terminating the message with the second occurrence of the delimiting character. Then, press <enter> to save the text.

Example

This example shows how to set a login banner.

```
DmSwitch(config)#banner login
~ <text> ~, where c is any delimiting character
=You are reading
  a login banner test.
This is a example.=
DmSwitch(config)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

No related command.

batch *index date*

```
batch index date { min { minute... | all | range first-minute last-minute... } [ hour { hour... | all | range first-hour last-hour... } [ day-of-month { day-month... | all | range first-day-month last-day-month... } [ month { month... | all | range first-month last-month... } [ day-of-week { day-week... | all | range first-day-week last-day-week... } ] ] ] ] }
```

Description

Schedules the execution of batch file.

Syntax

Parameter	Description
<i>index</i>	Specifies the batch file index. (Range: 1-16)
min	Schedules the minutes that the batch file will be executed.
<i>minute</i>	Specifies a minute of an hour. (Range: 0-59)
all	Specifies all possibilities of a before parameter in the command.
range <i>first-minute last-minute</i>	Specifies a range of minutes in an hour. (Range: 0-59)
hour	(Optional) Schedules the hours that the batch file will be executed.
<i>hour</i>	Specifies an hour of a day. (Range: 0-23)
range <i>first-hour last-hour</i>	Specifies a range of hours in a day. (Range: 0-23)
day-of-month	(Optional) Schedules the days of month that the batch file will be executed.
<i>day-month</i>	Specifies a day of a month. (Range: 1-31)
range <i>first-day-month last-day-month</i>	Specifies a range of days in a month. (Range: 1-31)
month	(Optional) Schedules the months of year that the batch file will be executed.
<i>month</i>	Specifies a month of an year. (Range: 1-12)
range <i>first-month last-month</i>	Specifies a range of months in an year. (Range: 1-12)
day-of-week	(Optional) Schedules the days of week that the batch file will be executed.
<i>day-week</i>	Specifies a day of week where 0 represents Sunday. (Range: 0-6)
range <i>first-day-week last-day-week</i>	Specifies a range of days in a week where 0 represents Sunday. (Range: 0-6)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The batch file must be enabled for its execution in accordance with its schedules.

Example

This example shows how to schedule the batch file specified by index 1 to be executed on Saturdays at 7 o'clock.

```
DmSwitch#batch 1 date min 0 hour 7 day-of-month all month all day-of-week 6
DmSwitch#
```

You can verify that the batch file was scheduled by entering the **show batch** privileged EXEC command.

Related Commands

Command	Description
batch index disable	Disables the batch file execution.
batch index enable	Enables the batch file execution in accordance with its schedules.
batch index remark	Specifies a remark for a batch file.
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch new	Creates a new batch file.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

batch *index* disable

batch index disable

Description

Disables the batch file execution.

Syntax

Parameter	Description
<i>index</i>	Specifies the batch file index. (Range: 1-16)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable the batch file specified by index 1.

```
DmSwitch#batch 1 disable
DmSwitch#
```

You can verify that the batch file was disabled by entering the **show batch** privileged EXEC command.

Related Commands

Command	Description
batch index date	Schedules the execution of batch file.
batch index enable	Enables the batch file execution in accordance with its schedules.

Command	Description
batch index remark	Specifies a remark for a batch file.
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch new	Creates a new batch file.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

batch *index* enable

batch index enable

Description

Enables the batch file execution in accordance with its schedules.

Syntax

Parameter	Description
<i>index</i>	Specifies the batch file index. (Range: 1-16)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the batch file specified by index 1.

```
DmSwitch#batch 1 enable
DmSwitch#
```

You can verify that the batch file was disabled by entering the **show batch** privileged EXEC command.

Related Commands

Command	Description
batch index date	Schedules the execution of batch file.
batch index disable	Disables the batch file execution.

Command	Description
batch index remark	Specifies a remark for a batch file.
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch new	Creates a new batch file.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

batch *index* remark

batch index remark *remark*

Description

Specifies a remark for a batch file.

Syntax

Parameter	Description
<i>index</i>	Specifies the batch file index. (Range: 1-16)
<i>remark</i>	Specifies a remark.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the remark "test" for the batch file specified by index 1.

```
DmSwitch#batch 1 remark test
DmSwitch#
```

You can verify that the information was deleted by entering the **show batch** privileged EXEC command.

Related Commands

Command	Description
batch index date	Schedules the execution of batch file.

Command	Description
batch index disable	Disables the batch file execution.
batch index enable	Enables the batch file execution in accordance with its schedules.
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch new	Creates a new batch file.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

batch *index* start-session

batch *index* start-session

Description

Starts a batch file session where all sequence of "executed" commands are saved.

Syntax

Parameter	Description
<i>index</i>	Specifies the batch file index. (Range: 1-16)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Show commands are not saved in the batch file because the batch files are executed in background.

Example

This example shows how to start a batch file session for the batch file specified by index 1.

```
DmSwitch#batch 1 start-session
Batch-1#
```

You can verify that the batch file session was started as it is shown in the new prompt.

Related Commands

Command	Description
batch index date	Schedules the execution of batch file.
batch index disable	Disables the batch file execution.

Command	Description
batch index enable	Enables the batch file execution in accordance with its schedules.
batch index remark	Specifies a remark for a batch file.
batch new	Creates a new batch file.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

batch new

batch new *index*

no batch *index*

Description

Creates a new batch file.

Inserting **no** as a prefix for this command will delete the specified batch file.

Syntax

Parameter	Description
new <i>index</i>	Specifies the batch file index. (Range: 1-16)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a new batch file with index 1.

```
DmSwitch#batch new 1
DmSwitch#
```

You can verify that the batch file was created by entering the **show batch** privileged EXEC command.

Related Commands

Command	Description
batch index date	Schedules the execution of batch file.
batch index disable	Disables the batch file execution.
batch index enable	Enables the batch file execution in accordance with its schedules.
batch index remark	Specifies a remark for a batch file.
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch term-session	Finishes a batch file session that was previously started to save all sequence of 'executed' commands.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

batch term-session

batch term-session

Description

Finishes a batch file session that was previously started to save all sequence of "executed" commands.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Show commands are not saved in the batch file because batch files are executed in background.

Example

This example shows how to finish the batch file session for the batch file specified by index 1.

```
Batch-1(config)#batch term-session
Save typed commands? <Y/n> y
DmSwitch#
```

You can verify that the batch file session was finished by entering the **show batch** privileged EXEC command.

Related Commands

Command	Description
batch index date	Schedules the execution of batch file.
batch index disable	Disables the batch file execution.
batch index enable	Enables the batch file execution in accordance with its schedules.
batch index remark	Specifies a remark for a batch file.

Command	Description
batch index start-session	Starts a batch file session where all sequence of 'executed' commands are saved.
batch new	Creates a new batch file.
show batch	Shows the existing batch files and their contents.
show running-config	Shows the current operating configuration.

bridge-ext gvrp

bridge-ext gvrp

no bridge-ext gvrp

Description

Globally enables GVRP (GARP VLAN Registration Protocol) for the switch.

Inserting **no** as a prefix for this command will disable the GVRP.

Syntax

No parameter accepted.

Default

GVRP is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

With the GVRP globally enabled, specific ports that there are GVRP enabled can automatically learn VLANs from connected devices where GVRP is also enabled.

Example

This example shows how to enable the GVRP globally for the switch.

```
DmSwitch(config)#bridge-ext gvrp
DmSwitch(config)#
```

You can verify that the GVRP was enabled by entering the **show bridge-ext** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>garp timer</code>	Set values for GARP timers.
<code>show garp</code>	Shows GARP properties.
<code>show gvrp</code>	Shows GVRP configuration.
<code>show running-config</code>	Shows the current operating configuration.
<code>switchport gvrp</code>	Enables GVRP for a specific port.

cesop idle-byte

cesop unit { *unit-number* } **idle-byte** { *value* }

no cesop unit { *unit-number* } **idle-byte**

Description

Configures idle-byte value for all CESoP TDM interfaces. Inserting **no** as a prefix of this command will reset idle-byte to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the idle byte hexadecimal value. (Range: 0x00 - 0xFF)

Default

Idle-byte default value is 0xFF.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure idle-byte in the unit 1.

```
(config)cesop unit 1 idle-byte 0x A(config-if-pw-1/1)#
```

You can verify that the idle-byte was configured by entering the **show cesop unit** user EXEC configuration command.

Related Commands

Command	Description
<code>show cesop unit</code>	the Section called <i>show cesop</i> in Chapter 2

cfm

```
cfm { enable | md md-name [ level number ] }
```

```
no cfm enable
```

Description

Enables Connectivity Fault Management (CFM) and create a Maintenance Domain (MD).

Inserting **no** as a prefix for command cfm enable will disable CFM.

Syntax

Parameter	Description
<i>enable</i>	Enables Connectivity Fault Management.
md <i>md-name</i>	Configures a Maintenance Domain (MD).
level <i>number</i>	(Optional) Insert a level number. (Range: 0-7)

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a Maintenance Domain (MD) with level 5.

```
DmSwitch(config)#cfm md MD_1 level 5
DmSwitch(config-cfm)#
```

You can verify that the address was added to the list by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

clock timezone

```
clock timezone { name hour [ minute ] }
```

```
no clock timezone
```

Description

Specifies the time zone.

Inserting **no** as a prefix for this command will reset time zone to default value.

Syntax

Parameter	Description
<i>name</i>	Specifies a name for time zone.
<i>hour</i>	Hours offset from UTC. (Range: -23 - +23)
<i>minute</i>	(Optional) Minutes offset from UTC. (Range: 1-59)

Default

0 hours and 0 minutes offset from UTC, without name.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the time zone with name "BRA", and -3 hours and 0 minutes offset from UTC.

```
DmSwitch#clock timezone BRA -3 0
DmSwitch#
```

You can verify that the information was deleted by entering the **show clock** privileged EXEC command.

Related Commands

Command	Description
show clock	Shows the system clock and time zone.

counter

```
counter { ingress | egress } { new | id } [ mode upper { all lower none | green lower  
{ not-green | yellow | red } | none lower all | red lower { not-red | yellow } } |  
remark name | type [ bytes | packets ] | ... ]
```

```
no counter { ingress | egress } id
```

Description

Configure a counter to be used by a filter.

Inserting **no** as a prefix for this command will delete the counter specified.

Syntax

Parameter	Description
ingress	Counter is related to ingress stage.
egress	Counter is related to egress stage.
ingress	Counter is related to ingress stage.
egress	Counter is related to egress stage.
new	Creates a new counter
<i>id</i>	Selects a counter to edit by ID
mode	Counter Upper and Lower mode
upper	Set Upper counter's mode
lower	Set Lower counter's mode
all	Upper/Lower count all packets
none	Upper/Lower count no packets
red	Upper/Lower count red packets
green	Upper count green packets
yellow	Lower count yellow packets
not-green	Lower count not green packets
not-red	Lower count not red packets
remark <i>name</i>	(Optional) Adds a remark text
type	Counter type
bytes	Count number of bytes
packets	Count number of packets

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
11.6	<i>ingress</i> <i>egress</i> parameter was added.

Usage Guidelines

Not available.

Example

This example shows how to create a new counter.

```
DmSwitch(config)#counter ingress new remark first_counter
Counter 1 created.
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show counter** privileged EXEC command.

Related Commands

Command	Description
show counter	Shows counters values and configuration
filter	Creates or configures a traffic filter
show running-config	Shows the current operating configuration.

cpu-dos-protect

```
cpu-dos-protect { block { dlf | 13-slow-path | subnet-broadcast } | max-pps value  
[ queue value ] }
```

Description

Limits the rate or blocks packets that are processed by CPU.

Inserting **no** as a prefix for this command will disable feature to **cpu-dos-protect block** commands and set default value to the others **cpu-dos-protect** commands.

Syntax

Parameter	Description
block 13-slow-path	Avoids that unicast packets with TTL=1 are copied to CPU.
block dlf	Avoids that packet classified as DLF (Destination Lookup Fail) are copied to CPU.
block subnet-broadcast	Limit packets reaching the CPU when the destination address is a network (all-zeros) or a broadcast (all-ones) subnet address.
max-pps value	Configure the global maximum of rate limit in PPS. If the queue is specified, it refers to queue's max PPS, otherwise it refers to global max PPS.
queue value	Queue related to configured max-pps.

Default

block subnet-broadcast option is enabled by default.

block 13-slow-path, **block dlf** and **rate-limit** options are disabled by default.

max-pps default value is 2000.

max-pps queues and **weight queues** default values are:

Queue	Protocol	max-pps weight	
47	Stacking ATP Discovery	2000	SP
46	Stacking ATP Control	2000	SP
45	OAM	500	1
44	EAPS	500	1
43	ERPS	250	1
42	CFM	100	1
41	STP	50	1
40	BPDU Tunneling	250	1

Queue	Protocol	max-pps weight	
39	E-LMI	250	1
38	LACP	250	1
37	Dot1X	500	1
36	L2 Move	10	1
35	ARP	500	1
34	GARP	250	1
33	IGMP	100	1
32	ICMPv6	200	1
31	VRRP	250	1
30	LBD	250	1
29	BGP	250	1
28	OSPF	250	1
27	RIP	250	1
26	RIPng	250	1
25	IS-IS	250	1
24	BFD	550	1
23	RSVP	500	1
22	LDP	250	1
21	Telnet	250	1
20	TFTP	250	1
19	SNTP	250	1
18	HTTP	250	1
17	SNMP	250	1
16	DHCP	250	1
15	SSH	250	1
14	LLDP	500	1
13	ICMPv4	150	1
12	Unknown Mcast PIM	250	1
11	Unknown L3 Slowpath	50	1
10	Unicast and Internal Commun	500	1
9	MPLS OAM	2	1
8	HTTPS	200	1
7	Stacking ATP Data	1000	SP
6	ICMPv4 Time Exceeded	20	1
5	-	-	1
4	L3 MTU Fail	20	1
3	Reserved IPv4 Mcast	200	1
2	Multicast	100	1
1	Broadcast	100	1
0	Others	250	1

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
7.8	The options global and queue were introduced.
11.6	The options block , arp request , 13-slow-path and reserved-multicast were introduced.
13.6.4	The option block subnet-broadcast was introduced.
14.0	The option rate-limit was removed. The options queue and max-pps and all their parameters were introduced.
14.2	The options block arp request and block reserved-multicast were removed.
15.2.6	The default value for queue 9 max-pps, which is related to MPLS OAM protocol, has been changed from 150 to 2.

Usage Guidelines

This command can be used to prevent attacks to the CPU, where an attacker could generate a packet flood and require a large amount of processing that would negatively affect execution of other system tasks.

However, a very low limit could cause loss of critical traffic as protocol PDUs, management connections, etc.

block 13-slow-path should not be enabled if L3 protocols are running.

block subnet-broadcast will allow an initial flow of packets since, in this case, the learning process is done by the CPU and not by the hardware. The block can be verified by checking the blackhole hosts using the command **show ip hardware host-table**

Example

This example shows how to limit CPU packet rate in 3000 packets per second.

```
DmSwitch#
DmSwitch#configure
DmSwitch(config)#
DmSwitch(config)#cpu-dos-protect max-pps 3000
DmSwitch(config)#
```

You can verify that the rate limit was changed by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cpu</code>	Shows CPU information.
<code>show cpu-dos-protect</code>	Shows the CPU denial of service protection information.
<code>show ip hardware</code> <code>host-table</code>	Shows the hardware host table.
<code>show running-config</code>	Shows the current operating configuration.

cpu egress-block

```
cpu egress-block ethernet parameters [ ingress ethernet parameters ] [ vlan parameters ]
```

```
no cpu egress-block ethernet parameters [ ingress ethernet parameters ] [ vlan parameters ]
```

Description

Configures the switch to block CPU traffic with a range of VLAN IDs from a set of specified Ethernet interfaces to another set of Ethernet interfaces

Inserting **no** as a prefix for this command will delete the specified CPU Egress-Block rule.

Syntax

Parameter	Description
egress-block	The traffic must match the specified egress interfaces to be blocked.
ingress	The traffic must match the specified ingress interfaces to be blocked.
vlan	The VLAN ID of the traffic must match the specified set of VLAN IDs to be blocked.
Ethernet parameters	Adds ethernet interfaces to the CPU Egress-Block rule.
[<i>unit-number</i> /] <i>port-number</i>	Adds a single Ethernet interface to the CPU Egress-Block rule.
all	Adds all Ethernet interface to the CPU Egress-Block rule.
range [<i>first-unit-number</i> /] <i>first-port-number</i> [<i>last-unit-number</i> /] <i>last-port-number</i>	Adds the range of Ethernet interface to the CPU Egress-Block rule.
VLAN parameters	Adds a set of VLAN IDs to the CPU Egress-Block rule.
<i>vlan-id</i>	Adds a single VLAN ID to the CPU Egress-Block rule.
all	Adds all VLAN IDs to the CPU Egress-Block rule.
range <i>first-vlan-id last-vlan-id</i>	Adds the range of VLAN IDs to the CPU Egress-Block rule.

Default

By default, no CPU Egress-Block rule is created.

A new CPU Egress-Block rule matches all ingress interfaces if no ingress parameters are specified.

A new CPU Egress-Block rule matches all VLAN IDs if no VLAN parameters are specified.

Command Modes

Global configuration.

Command History

Release	Modification
13.5	This command was introduced.

Usage Guidelines

The maximum number of simultaneous CPU Egress-Block rules is 512.

A new rule is created only if it is not completely contemplated by existing rules.

If a new rule includes one or more existing rules, the previous rules will be merged with the new one.

Example

This example shows how to set a rule for blocking traffic from ingress Ethernet 5, egress Ethernet 6, 7 or 8, and VLAN ID 126.

```
DmSwitch(config)#cpu egress-block ethernet range 6 8 ingress ethernet 5 vlan 126
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show running-config** command.

Related Commands

Command	Description
show cpu egress-block	Shows the rules for blocking forwarding of packets by the CPU.
filter	Creates or configures a traffic filter
switchport egress-block	Configures the switch to block traffic from a specified Ethernet interface to another.
show running-config	Shows the current operating configuration.

cpu protocol-priority default

`cpu protocol-priority default packet`

`no cpu protocol-priority default`

Description

Configure the default packet priority.

Inserting **no** as a prefix for this command will disable the default priority.

Syntax

Parameter	Description
<i>packet</i>	Specifies the packet priority. (Range: 0-7)

Default

1

Command Modes

Global configuration.

Command History

Release	Modification
7.6	This command was introduced.

Example

This example shows how to configure the priority 1 for default packets

```
DmSwitch#cpu protocol priority default 1
DmSwitch#
```

You can verify that protocol priority default was introduced by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cpu</code>	Shows CPU information.
<code>show running-config</code>	Shows the current operating configuration.

cpu protocol-priority enable

`cpu protocol-priority enable`

`no cpu protocol-priority enable`

Description

Enables packet enqueueing according to priority.

Inserting **no** as a prefix for this command will disable the enqueueing. All packets will use a single queue when arriving at CPU port.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
10.4	This command was introduced.

Example

This example shows how to configure enable packet enqueueing.

```
DmSwitch#cpu protocol priority enable
DmSwitch#
```

You can verify that CPU protocol was activated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cpu	Shows CPU information.
show running-config	Shows the current operating configuration.

cpu protocol-priority l2-protocol

```
cpu protocol-priority l2-protocol packet
```

```
no cpu protocol-priority l2-protocol
```

Description

Configure priority to l2 protocols packets.

Inserting **no** as a prefix for this command will disable the l2-protocol priority.

Syntax

Parameter	Description
<i>packet</i>	Specifies the packet priority. (Range: 0-7)

Default

7

Command Modes

Global configuration.

Command History

Release	Modification
7.6	This command was introduced.

Example

This example shows how to configure the priority 3 for l2-protocol packets

```
DmSwitch#cpu protocol priority l2-protocol 3
DmSwitch#
```

You can verify that protocol priority l2-protocol was introduced by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cpu</code>	Shows CPU information.
<code>show running-config</code>	Shows the current operating configuration.

cpu protocol-priority hardware

`cpu protocol-priority hardware`

`no cpu protocol-priority hardware`

Description

Enables packet according to priority defined by hardware configuration

Inserting **no** as a prefix for this command will disable the hardware mode. All packets will be configured with priority defined by other cpu protocol priority configurations.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
14.10	This command was introduced.

Usage Guidelines

This command only has effect on packets being tunneled/untunneled. It does not modify, for example, PDUs packets generated by the equipment.

Once this feature is enabled. Packets will receive priority given by hardware configuration such as filters, vlan-translates, vlan native default priority. When disabled, packets will receive the priority configured with **cpu protocol-priority** command.

Example

This example shows how to enable hardware mode.

```
DmSwitch#config
DmSwitch(config)#cpu protocol priority hardware
DmSwitch(config)#
```

You can verify that CPU protocol was activated by entering the **show running-config** or **show cpu protocol priority** privileged EXEC command.

Related Commands

Command	Description
cpu protocol-priority l2-protocol	Configure priority to l2 protocols packets.
cpu protocol-priority tunnel	Configure priority to tunneled packets.
cpu protocol-priority default	Configure the default packet priority
show cpu	Shows CPU information.
show running-config	Shows the current operating configuration.

cpu protocol-priority management

`cpu protocol-priority management priority`

`no cpu protocol-priority management`

Description

Configure the management packets priority.

Inserting **no** as a prefix for this command will disable the management priority configuration.

Syntax

Parameter	Description
<i>priority</i>	Specifies the packet priority. (Range: 0-7)

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
10.4	This command was introduced.

Example

This example shows how to configure the priority 6 for management packets

```
DmSwitch#cpu protocol priority management 6
DmSwitch#
```

You can verify that management packets priority was introduced by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cpu</code>	Shows CPU information.
<code>show running-config</code>	Shows the current operating configuration.

cpu protocol-priority tunnel

`cpu protocol-priority tunnel packet`

`no cpu protocol-priority-tunnel`

Description

Configure priority to tunneled packets.

Inserting **no** as a prefix for this command will disable the tunnel priority.

Syntax

Parameter	Description
<i>packet</i>	Specifies the packet priority. (Range: 0-7)

Default

6

Command Modes

Global configuration.

Command History

Release	Modification
7.6	This command was introduced.

Example

This example shows how to configure the priority 5 for tunnel packets

```
DmSwitch#cpu protocol priority tunnel 5
DmSwitch#
```

You can verify that protocol priority tunnel was introduced by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cpu</code>	Shows CPU information.
<code>show running-config</code>	Shows the current operating configuration.

cpu protocol-priority unknown

`cpu protocol-priority unknown packet`

`no cpu protocol-priority unknown`

Description

Configure priority to unknown source/destination packets.

Inserting **no** as a prefix for this command will disable the unknown priority.

Syntax

Parameter	Description
<i>packet</i>	Specifies the packet priority. (Range: 0-7)

unknown

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.6	This command was introduced.

Example

This example shows how to configure the priority 7 for unknown packets

```
DmSwitch#cpu protocol priority unknown 7
DmSwitch#
```

You can verify that protocol priority unknown was introduced by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cpu</code>	Shows CPU information.
<code>show running-config</code>	Shows the current operating configuration.

cpu protocol bpdprotect

```
cpu protocol bpdprotect
```

```
no cpu protocol bpdprotect
```

Description

Enable control BPDU packets per second monitoring.

Inserting **no** as a prefix for this command will disable the VLAN link detect.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
9.6	This command was introduced.

Usage Guidelines

This command can be used to prevent problems in protocols when there is flood of BPDUs.

Example

This example shows how to enable this feature.

```
DmSwitch#cpu protocol bpdprotect
DmSwitch#
```

You can verify that this configuration was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show_cpu</code>	Shows CPU information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x accounting

dot1x accounting

dot1x accounting interval *seconds*

dot1x traffic-monitoring

no dot1x accounting

no dot1x accounting interval

no dot1x traffic-monitoring

Description

Configures the 802.1X RADIUS accounting.

Syntax

Parameter	Description
accounting	Enable 802.1X RADIUS accounting
accounting interval <i>seconds</i>	Specify an interval between accounting updates. (Range: 60-86400)
accounting traffic-monitoring	Enable traffic monitoring in octets.

Default

The 802.1X RADIUS accounting is disabled by default.

The accounting interval is disabled by default.

The accounting traffic-monitoring is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
14.0	The accounting option was introduced.

Usage Guidelines

With 802.1X accounting enabled, the switch will send an accounting start packet when a client authenticates and an accounting stop when he disconnects.

You specify the interval between accounting interim packets during the session. The "no dot1x accounting interval" command disables the sending of interim packets.

If 802.1X accounting traffic-monitoring is enabled, the accounting stop packet will contain the amount of input/output octets transmitted during the client's session. This option will have effect on new supplicants only.

For the mode *multi-auth* the traffic-monitoring will not distinguish each user traffic, showing the interface total traffic history on the stop of each session.

Example

This example shows how to enable 802.1X accounting and its options.

```
DmSwitch(config)#dot1x accounting
DmSwitch(config)#dot1x accounting interval 100
DmSwitch(config)#dot1x accounting traffic-monitoring
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
radius-server host	Configures a specific RADIUS server.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x captive-portal

```
dot1x captive-portal { filter { disable | priority priority } | vlan id }
```

```
no dot1x captive-portal
```

Description

Enables the 802.1X Captive Portal. Specifies a VLAN as Captive Portal VLAN in which the interfaces are put when Captive Portal is active.

Syntax

Parameter	Description
priority <i>priority</i>	Priority of filters used by Captive Portal. (Range: 1-14)
disable	Disables the use of filters by Captive Portal.
vlan <i>id</i>	VLAN ID. (Range: 1-4094)

Default

The filters of Captive Portal are enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	The captive-portal option was introduced.

Usage Guidelines

When you configure a Captive Portal, clients that are not 802.1x-capable are able to authenticate through a Web interface.

The Captive Portal VLAN must have an IP.

The Captive Portal VLAN must provide the minimum set of services needed to client be able to open a browser and enter an address.

These services include at least: DHCP server, DNS server and ARP replies.

In the moment that Captive Portal is activated as a DOT1X authentication method, the port is unblocked and put in Captive Portal VLAN.

In the moment that the client tries to open a Web page in his browser, the HTTP (or HTTPS) traffic is redirected to the Login page of Captive Portal HTTP server. Then, the client must enter with his credentials to get access and to be added in the correct VLAN.

Example

This example shows how to configure VLAN 3 as an 802.1X Captive Portal VLAN.

```
DmSwitch(config)#interface vlan 3
DmSwitch(config)#ip address 1.1.1.1/24
DmSwitch(config)#dot1x captive-portal vlan 3
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x captive-portal	Enables Captive Portal as an 802.1X authentication mechanism on the interface.
dot1x system-auth-control	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x port-control	Sets the dot1x mode on a port interface.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x default

dot1x default

Description

Changes the 802.1X global and port settings to default values.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

By using the **dot1x default** command, 802.1X global and per port configurations has set a default value.

Example

This example shows how to set dot1x to default values.

```
DmSwitch(config)#dot1x default
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x port-control	Sets the dot1x mode on a port interface.

Command	Description
<code>dot1x re-auth-enable</code>	Enables or disables periodic re-authentication.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x quiet-period</code>	Defines dot1x quiet period timeout value.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x max-users

dot1x max-users *number*

no dot1x max-users

Description

Configures maximum users that can be learned via 802.1X authentication globally. Only effective on ports with host-mode multi-auth configured.

Syntax

Parameter	Description
max-users <i>number</i>	Maximum number of users that can be learned via 802.1X authentication globally. (Range: 1-1024)

Default

The maximum users are 256 by default.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	The max-users option was introduced.

Usage Guidelines

The multi-auth mode distinguishes the connected users by the origin MAC adress, and this parameter limits the maximum number of MAC users which can be learned by all interfaces operating in multi-auth mode.

Example

This example shows how to configure global max-users.

```
DmSwitch(config)#dot1x max-users 500
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>dot1x system-auth-control</code>	Configures global options for 802.1X.
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x host-mode</code>	Sets the dot1x host-mode on a port interface.
<code>dot1x re-auth-max</code>	Sets the maximum EAP request/identity packet retransmissions.
<code>dot1x max-users</code>	Sets the maximum users that can be learned via 802.1X per port.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>dot1x re-auth-enable</code>	Enables or disables periodic re-authentication.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x quiet-period</code>	Defines dot1x quiet period timeout value.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x sytem-auth_control

dot1x system-auth-control

no dot1x system-auth-control

Description

Enables the 802.1X protocol.

Inserting **no** as a prefix for this command will disable 802.1X.

Syntax

Parameter	Description
dot1x system-auth-control	Enables the 802.1X globally.
no dot1x system-auth-control	Disables the 802.1X globally.

Default

802.1X is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Example

This example shows how to enable the 802.1X authentication globally on the DmSwitch

```
DmSwitch(config)#dot1x system-auth-control
DmSwitch(config)#
```

You can verify the 802.1X status by entering the **show dot1x** privileged EXEC command.

show running-config privileged EXEC command.

Related Commands

Command	Description
<code>dot1x captive-portal</code>	Configures global options for 802.1X.
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>dot1x re-auth-enable</code>	Enables or disables periodic re-authentication.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x quiet-period</code>	Defines dot1x quiet period timeout value.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dscp-table

```
dscp-table all-dscp { same | to-DSCP } priority [ green | red ]
```

```
dscp-table range first-DSCP last-DSCP { same | to-DSCP } priority [ green | red ]
```

```
dscp-table from-DSCP { same | to-DSCP } priority [ green | red ]
```

```
no dscp-table
```

Description

Configure Differentiated Services Code Point mappings. It is possible to map a DSCP to another DSCP, and also add an 802.1p and a color.

Inserting **no** as a prefix for this command will restore the default configuration.

Syntax

Parameter	Description
all-dscp	Creates mapping for all 64 DSCP values.
range <i>first-DSCP</i> <i>last-DSCP</i>	Creates mapping for DSCP values between first-DSCP and last-DSCP.
<i>from-DSCP</i>	Creates mapping for indicated from-DSCP.
same	Maps previous selected DSCP value(s) to itself (themselves).
<i>to-DSCP</i>	Maps previous selected DSCP value(s) to to-DSCP value.
<i>priority</i>	Changes 802.1p priority.
green	Marks packet as green.
red	Marks packet as red.

Default

By default, all DSCP are mapped to themselves, 802.1p 0 and green color.

Command Modes

Global configuration.

Command History

Release	Modification
7.6.4	This command was introduced.
13.0	The green/red command option were added.

Usage Guidelines

To set only 802.1p and/or color of all or a range of DSCPs it is recommended the use of keyword "same", to keep all DSCPs' mapping to themselves.

If no color is informed, the mapping will use green as default.

Example

This example shows how to map a range of DSCP starting at 0 and ending at 10 to DSCP 5, 802.1p 2 and color red.

```
DmSwitch(config)#dscp-table range 0 10 5 2 red
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show dscp-table** user EXEC command.

Related Commands

Command	Description
show dscp-table	Shows Differentiated Services Code Point mapping table.
show running-config	Shows the current operating configuration.

eaps *domain*

eaps *domain*

no eaps *domain*

Description

Creates a new EAPS domain.

Inserting **no** as a prefix for this command will delete the EAPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

Before you create a EAPS domain, you must disable the spanning-tree protocol.

Example

This example shows how to create a domain with id 1.

```
DmSwitch(config)#eaps 1
DmSwitch(config)#
```

You can verify that the domain was created by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain port-block-aware	[removed] Configures interaction between EAPS domain and blocking L2 protocols in DmSwitch.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* control-vlan

eaps domain control-vlan { **id** *index* | **name** *name* }

no eaps domain control-vlan

Description

Configures the control VLAN for the EAPS domain.

Inserting **no** as a prefix for this command will remove the control VLAN records for the specified EAPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
id <i>index</i>	Specifies an enabled VLAN by index. (Range: 1-4094)
name <i>name</i>	Specifies an enabled VLAN by name.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

The control VLAN is used for control traffic from the EAPS protocol. It cannot be used for data traffic.

For the primary and secondary ports of the domain, the control VLAN always have a forwarding state. For the remaining ports, the control VLAN always have a blocked state.

Example

This example shows how to configure the VLAN index 100 to be the control VLAN for the EAPS domain.

```
DmSwitch(config)#eaps 1 control-vlan id 100
DmSwitch(config)#
```

You can verify that the information was deleted by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* failtime

eaps domain failtime { *seconds* **milliseconds** *milliseconds* }

no eaps domain failtime

Description

Configures the amount of time that causes the EAPS Master node to enter the FAILED state if no hello packet is received.

Inserting **no** as a prefix for this command will reset failtime to the default value.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
<i>seconds</i>	Specifies the maximum time, in seconds, to declare the FAILED state when no hello packets are received. Must be greater than hellotime for this domain.
<i>milliseconds</i>	Specifies the maximum time, in milliseconds, to declare the FAILED state when no hello packets are received. In conjunction with the above parameter, must be greater than hellotime for this domain.

Default

3 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

The "hello" packets are sent on the primary port from the Master switch and are expected to be received on its secondary port. If no hello packets are received on the secondary port after failtime seconds the Master switch enters the FAILED state.

This is an alternate method for detecting ring failures. In most situations, the Master switch will enter the FAILED state after receiving link down notifications from other switches or from itself which is faster than the failtime method.

Use lower values of failtime to ensure faster ring protection. Use higher values to be more tolerant to hello packet losses.

Example

This example shows how to change the failtime parameter for an EAPS domain

```
DmSwitch(config)#eaps 1 failtime 5
DmSwitch(config)#
```

You can verify that the interval time was changed by entering the **show eaps detail** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* hellotime

```
eaps domain hellotime { seconds milliseconds milliseconds }
```

```
no eaps domain hellotime
```

Description

Configures the sending interval for "hello" packets.

Inserting **no** as a prefix for this command will reset hellotime to the default value.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
<i>seconds</i>	Specifies the interval between the sending of two "hello" packets in seconds. It must be less than the failtime parameter for this domain.
<i>milliseconds</i>	Specifies the interval between the sending of two "hello" packets in milliseconds. It must be less than the failtime parameter for this domain.

Default

1 second.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

The "hello" packets are sent on the primary port from the Master switch and are expected to be received on its secondary port. A hello packet received puts the EAPS domain in the COMPLETE state (Master switch).

Use lower values to ensure faster state transitions for the EAPS protocol. Use higher values to reduce control traffic on the network.

Example

This example shows how to change the interval time between two "hello" packets to 2 seconds.

```
DmSwitch(config)#eaps 1 hellotime 2
DmSwitch(config)#
```

You can verify that the interval time was changed by entering the **show eaps detail** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* mode

eaps domain mode { master | transit }

Description

Configures the mode of a switch in the EAPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
master	Defines the master mode.
transit	Defines the transit mode.

Default

After an EAPS domain is created, the switch is in Transit mode.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

You must configure exactly one switch as Master on each EAPS domain. The remaining switches must be configured as Transit.

The Master switch performs some control operations on the EAPS domain. In normal conditions, the secondary port of the Master switch is the one that is blocked for traffic in order to avoid the Ethernet ring becoming a network loop.

Example

This example shows how to configure a DmSwitch as master.

```
DmSwitch(config)#eaps 1 mode master
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* packet-mode

```
eaps domain packet-mode { standard | rrpp }
```

Description

Configures how EAPS PDUs are encapsulated in the domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
standard	Encapsulates EAPS PDUs with standard mode.
rrpp	Encapsulates PDUs with RRPP mode.

Default

After an EAPS domain is created, the PDU encapsulation mode is standard.

Command Modes

Global configuration.

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

All switches in the EAPS domain must be configured with the same encapsulation mode. *A single switch in an EAPS domain with an incorrect encapsulation mode can affect negatively the behavior of the whole EAPS ring.*

The RRPP encapsulation mode is provided only for compatibility reasons. When RRPP encapsulation mode is enabled, the protocol executed still is EAPS. This mode should be used only in single ring topologies (subrings are not supported). Furthermore, ring id must match domain id in all other RRPP equipments in the same ring as the DmSwitch.

Example

This example shows how to configure the encapsulation mode of EAPS PDUs to RRPP, in a DmSwitch.

```
DmSwitch(config)#eaps 1 packet-mode rrpp
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* name

eaps *domain* [**name** *name*]

no eaps *domain* [**name**]

Description

Renames the EAPS domain.

Inserting **no** as a prefix for this command will delete the EAPS domain specified.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
<i>name</i>	Specifies a new name for domain.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

Not available.

Example

This example shows how to set the domain 1 name to "test".

```
DmSwitch(config)#eaps 1 name test
DmSwitch(config)#
```

You can verify that the domain was renamed by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps domain port

```
eaps domain port { primary | secondary } { ethernet [ unit-number/ ] port-number |  
port-channel channel-group-number }
```

```
no eaps domain port { primary | secondary }
```

Description

Configures the two ports that participate on an EAPS domain.

Inserting **no** as a prefix for this command will remove the configured ports from the EAPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
primary	Sets a specific port as primary.
secondary	Sets a specific port as secondary.
ethernet <i>unit-number/port-number</i>	Specifies an Ethernet unit (optional) and port.
port-channel <i>channel-group-number</i>	Specifies a port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id.

Usage Guidelines

The primary and secondary ports have no distinct functionality on Transit switches.

In normal conditions, the secondary port of the Master switch is the one that is blocked for traffic in order to

avoid the Ethernet ring becoming a network loop.

Example

This example shows how to define the ethernet port 1/25 as the primary port on the EAPS domain.

```
DmSwitch(config)#eaps 1 port primary ethernet 1/25
DmSwitch(config)#
```

You can verify that the information was configured by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps *domain* port-block-aware

eaps *domain* **port-block-aware**

no eaps *domain* **port-block-aware**

Description

This command is no longer available. The EAPS domain will always consider other L2 protocols (e.g. Link-Flap, Loopback Detection or OAM) blocking its ports to achieve rapid convergence.

Command History

Release	Modification
9.6	This command was introduced.
13.0	This command was removed.

eaps *domain* protected-vlans

```
eaps domain protected-vlans vlan-group { index | range first-index last-index | all }
```

```
no eaps domain protected-vlans vlan-group { index | range first-index last-index | all }
```

Description

Defines the VLAN groups that will be protected by an EAPS domain.

Inserting **no** as a prefix for this command will remove the protected VLAN group records for the specified EAPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain id.
<i>index</i>	Specifies a single VLAN group. (Range: 0-31)
range <i>first-index last-index</i>	Specifies a range of VLAN group IDs.
all	Specifies all VLAN groups.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	A specific domain is no longer referenced by name, but by id. The protected VLANs are specified using VLAN groups.

Usage Guidelines

For the primary and secondary ports of the domain, the protected VLAN groups have a forwarding or blocked state depending on the EAPS protocol execution. For the remaining ports, the protected VLAN groups always have a forwarding state.

Example

This example shows how to protect VLAN groups 1 to 5 on an EAPS ring.

```
DmSwitch(config)#eaps 1 protected-vlans vlan-group range 1 5
DmSwitch(config)#
```

You can verify that the configuration was done by entering the **show eaps detail** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

eaps hw-forwarding

eaps hw-forwarding

no eaps hw-forwarding

Description

Enables EAPS hardware forwarding in DmSwitch.

Inserting **no** as a prefix for this command will disable the EAPS hardware forwarding.

Syntax

No parameter accepted.

Default

EAPS hardware forwarding is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.6.4	This command was introduced.

Usage Guidelines

Filter priority 14 must be free or matching MAC and VLAN ID in order to use EAPS hardware forwarding.

Example

This example shows how to enable eaps hardware forwarding.

```
DmSwitch(config)#eaps hw-forwarding
DmSwitch(config)#
```

You can verify that EAPS hardware forwarding is enabled by entering the **show eaps** privileged EXEC command.

Related Commands

No related command.

elmi

elmi

Description

Enters on Ethernet Local Management Interface (E-LMI) protocol configuration mode.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enter on E-LMI configuration mode.

```
DmSwitch(config)#elmi
DmSwitch(config-elmi)#
```

Related Commands

Command	Description
show elmi	Shows Ethernet Local Management Interface settings.
show running-config	Shows the current operating configuration.
uni-c	Creates or edits User Network Interface (UNI) on Customer Edge devices.
uni-n	Creates or edits User Network Interface (UNI) on Provider Edge devices.

erps domain

erps domain

no erps domain

Description

Creates a new ERPS domain.

Inserting **no** as a prefix for this command will delete the ERPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID (range: 0-63).

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

It's recommended to disable spanning-tree protocol in ports used by ERPS.

Example

This example shows how to create a domain with ID 1.

```
DmSwitch(config)#erps 1
DmSwitch(config)#
```

You can verify that the domain was created by entering the **show erps** privileged EXEC command.

Related Commands

Command	Description
<code>erps domain accept</code>	Accept changes from other domains.
<code>erps domain control-vlan</code>	Configures the control VLAN for the ERPS domain.
<code>erps domain guard-time</code>	Set the domain guard time.
<code>erps domain holdoff-time</code>	Set the domain holdoff time.
<code>erps domain name</code>	Renames the domain.
<code>erps domain port0</code>	Configure the port 0 of ERPS protocol.
<code>erps domain port1</code>	Configure the port 1 of ERPS protocol.
<code>erps domain protected-vlans</code>	Defines the VLAN groups that will be protected by ERPS ring.
<code>erps domain restore-time</code>	Set the domain restore time.
<code>show erps</code>	Shows ERPS settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>vlan group</code>	Create a VLAN group and manage its members.

erps *domain* accept

```
erps domain accept { all | id target-domain | name target-domain-name | range first-domain last-domain }
```

```
no erps domain accept
```

Description

Accept topology change from specified domains.

Inserting **no** as a prefix for this command will clear the accepted domain list.

Syntax

Parameter	Description
all	Accept topology changes from all domains.
id target-domain	Accept topology changes from specified domain (referred by ID).
name target-domain-name	Accept topology changes from specified domain (referred by name).
range first-domain last-domain	Accept topology changes from a range of domains (referred by IDs).

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

When a topology change occurs in a sub-ring attached to a ring, the ring should be notified in order to avoid traffic problems. This is done by configuring the ring to accept topology changes from the sub-ring.

Example

This example shows how to accept topology changes in domain 1 from domain 2:

```
DmSwitch(config)#erps 1 accept id 2
DmSwitch(config)#
```

You can verify that the accept list changed by entering the **show erps detail** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps *domain* control-vlan

erps domain control-vlan { **id** *index* | **name** *name* }

no erps domain control-vlan

Description

Configures the control VLAN for the ERPS domain.

Inserting **no** as a prefix for this command will remove the control VLAN records for the specified ERPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
id <i>index</i>	Specifies an enabled VLAN by index. (Range: 1-4094)
name <i>name</i>	Specifies an enabled VLAN by name.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The control VLAN is used by protocol messages of the ERPS protocol. It should not be used for data traffic.

Example

This example shows how to configure the VLAN index 100 to be the control VLAN for the ERPS domain.

```
DmSwitch(config)#erps 1 control-vlan id 100
DmSwitch(config)#
```

You can verify that the control VLAN was configured by entering the **show erps** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps *domain* guard-time

erps *domain* **guard-time** *time*

no erps *domain* **guard-time**

Description

Set the guard time of domain.

Inserting **no** as a prefix for this command will set the guard time to default value.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
guard-time <i>time</i>	Specifies a new guard time value for domain (range: 10-2000 ms).

Default

The default value for guard time is 500 ms.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The guard timer prevents ring nodes from receiving outdated ERPS protocol messages. During the duration of the guard timer, all received ERPS protocol messages are ignored by the ring node. The guard time should be greater than the maximum expected forwarding delay for which one ERPS protocol message circles around the ring.

Example

This example shows how to set the domain 1 guard time to 800 ms.

```
DmSwitch(config)#erps 1 guard-time 800
```

```
DmSwitch(config)#
```

You can verify the new value of guard time by entering the **show erps detail** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps *domain* holdoff-time

erps *domain* **holdoff-time** *time*

no erps *domain* **holdoff-time**

Description

Set the holdoff time of domain.

Inserting **no** as a prefix for this command will set the holdoff time to default value.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
holdoff-time <i>time</i>	Specifies a new holdoff time for domain (range: 0-10000 ms, with steps of 100 ms).

Default

The default value for holdoff time is 0 ms.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The holdoff time is the time that the ERPS node will wait after an error is signaled to consider this error valid. Its purpose is to allow port0 or port1 to recover from a transient error.

Example

This example shows how to set the holdoff time to 100 ms:

```
DmSwitch(config)#erps 1 holdoff-time 100
DmSwitch(config)#
```

You can verify that the holdoff time was configured by entering the **show erps detail** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps *domain name*

erps *domain name* *name*

no **erps** *domain name*

Description

Renames the ERPS domain.

Inserting **no** as a prefix for this command will clear the name of the ERPS domain specified.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
<i>name</i>	Specifies a new name for domain.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the domain 1 name to "test".

```
DmSwitch(config)#erps 1 name test
DmSwitch(config)#
```

You can verify that the domain was renamed by entering the **show erps** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps domain port0

```
erps domain port0 { virtual-channel control-vlan index { id target-domain | name
target-domain-name } | { rpl | node } { ethernet [ unit-number/ ] port-number | port-channel
channel-group-number } }
```

```
no erps domain port0
```

Description

Configure the port 0 of ERPS protocol.

Inserting **no** as a prefix for this command will clear the port 0 configuration.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
virtual-channel	Configure this ERPS protocol port as part of a virtual channel.
control-vlan <i>index</i>	Specifies the control VLAN ID to be used in the virtual channel.
id <i>target-domain</i>	Specifies the ID of the domain to be used as virtual channel.
name <i>target-domain-name</i>	Specifies the name of the domain to be used as virtual channel.
rpl	Configure this port as RPL.
node	Configure this port as non-RPL.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Configure this port as an ethernet interface, specifying the unit and port number of interface.
port-channel <i>channel-group-number</i>	Configure this port as a port-channel interface, specifying the port channel ID.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The virtual channel configuration is used in a sub-ring to connect it to other rings. In any ring or sub-ring, exactly 1 ERPS protocol port must be configured as RPL in only one node of the ring or sub-ring. The other ERPS protocol ports not set as RPL or as virtual channel must be configured as non-RPL.

Example

Setting port0 of domain 2 in this node as part of the virtual channel through domain 1 using control VLAN 6:

```
DmSwitch(config)#erps 2 port0 virtual-channel control-vlan 6 id 1
DmSwitch(config)#
```

Setting port0 of domain 2 in this node as an RPL ethernet port:

```
DmSwitch(config)#erps 2 port0 rpl ethernet 1/20
DmSwitch(config)#
```

Setting port0 of domain 2 in this node as a non-RPL port-channel:

```
DmSwitch(config)#erps 2 port0 node port-channel 3
DmSwitch(config)#
```

You can verify that port0 was configured by entering the **show erps** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps domain port1

```
erps domain port1 { virtual-channel control-vlan index { id target-domain | name
target-domain-name } | { rpl | node } { ethernet [ unit-number/ ] port-number | port-channel
channel-group-number } }
```

```
no erps domain port1
```

Description

Configure the port 1 of ERPS protocol.

Inserting **no** as a prefix for this command will clear the port 1 configuration.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
virtual-channel	Configure this ERPS protocol port as part of a virtual channel.
control-vlan <i>index</i>	Specifies the control VLAN ID to be used in the virtual channel.
id <i>target-domain</i>	Specifies the ID of the domain to be used as virtual channel.
name <i>target-domain-name</i>	Specifies the name of the domain to be used as virtual channel.
rpl	Configure this port as RPL.
node	Configure this port as non-RPL.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Configure this port as an ethernet interface, specifying the unit and port number of interface.
port-channel <i>channel-group-number</i>	Configure this port as a port-channel interface, specifying the port channel ID.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The virtual channel configuration is used in a sub-ring to connect it to other rings. In any ring or sub-ring, exactly 1 ERPS protocol port must be configured as RPL in only one node of the ring or sub-ring. The other ERPS protocol ports not set as RPL or as virtual channel must be configured as non-RPL.

Example

Setting port1 of domain 2 in this node as part of the virtual channel through domain 1 using control VLAN 6:

```
DmSwitch(config)#erps 2 port1 virtual-channel control-vlan 6 id 1
DmSwitch(config)#
```

Setting port1 of domain 2 in this node as an RPL ethernet port:

```
DmSwitch(config)#erps 2 port1 rpl ethernet 1/20
DmSwitch(config)#
```

Setting port1 of domain 2 in this node as a non-RPL port-channel:

```
DmSwitch(config)#erps 2 port1 node port-channel 3
DmSwitch(config)#
```

You can verify that port1 was configured by entering the **show erps** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps *domain* protected-vlans

erps domain protected-vlans vlan-group { *index* | **range** *first-index last-index* | **all** }

no erps domain protected-vlans vlan-group { *index* | **range** *first-index last-index* | **all** }

Description

Defines the VLAN groups that will be protected by an ERPS domain.

Inserting **no** as a prefix for this command will remove the protected VLAN group from the specified ERPS domain.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
<i>index</i>	Specifies a single VLAN group. (Range: 0-127)
range <i>first-index last-index</i>	Specifies a range of VLAN group IDs.
all	Specifies all VLAN groups.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to protect VLAN groups 1 to 5 on an ERPS ring.

```
DmSwitch(config)#erps 1 protected-vlans vlan-group range 1 5
```

```
DmSwitch(config)#
```

You can verify that the configuration was done by entering the **show erps detail** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain restore-time	Set the domain restore time.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

erps *domain* restore-time

erps domain restore-time *time*

no erps domain restore-time

Description

Set the restore time of domain.

Inserting **no** as a prefix for this command will set the restore time to default value.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain ID.
restore-time <i>time</i>	Specifies a new restore time for domain (range: 5-12 minutes).

Default

The default value for restore time is 5 minutes.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The restore time is the time that the ERPS node will wait after an error is cleared from a blocked port0 or port1 to unblock the port. Its purpose is to filter transient recoveries on port0 or port1.

Example

This example shows how to set the recovery time to 10 minutes:

```
DmSwitch(config)#erps 1 restore-time 10
DmSwitch(config)#
```

You can verify the value of recovery time by entering the **show erps detail** privileged EXEC command.

Related Commands

Command	Description
erps domain	Creates a new ERPS domain.
erps domain accept	Accept changes from other domains.
erps domain control-vlan	Configures the control VLAN for the ERPS domain.
erps domain guard-time	Set the domain guard time.
erps domain holdoff-time	Set the domain holdoff time.
erps domain name	Renames the domain.
erps domain port0	Configure the port 0 of ERPS protocol.
erps domain port1	Configure the port 1 of ERPS protocol.
erps domain protected-vlans	Defines the VLAN groups that will be protected by ERPS ring.
show erps	Shows ERPS settings.
show running-config	Shows the current operating configuration.
vlan group	Create a VLAN group and manage its members.

evc

```
evc { evc-id type { multipoint-to-multipoint | point-to-point } cfm md md-name ma  
ma-name }
```

Description

Creates an Ethernet Virtual Circuit.

Syntax

Parameter	Description
<i>text</i>	Specifies EVC identifier (up to 32 characters)
type	Specifies the EVC type
md <i>md-name</i>	Specifies a CFM Maintenance Domain (MD).
ma <i>ma-name</i>	Specifies a CFM Maintenance Association (MA).

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure an EVC.

```
DmSwitch#configure  
DmSwitch(config)#evc EVC_ID type point-to-point cfm md MD ma MA
```

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>uni-n</code>	Creates or edits User Network Interface (UNI) on Provider Edge devices.
<code>cfm</code>	Enables Connectivity Fault Management (CFM) and create a Maintenance Domain (MD).

external-alarm

```
external-alarm { fan | psu | in1 [ invert ] | in2 [ invert ] | in3 [ invert ] }
```

```
no external-alarm { fan | psu | in1 [ invert ] | in2 [ invert ] | in3 [ invert ] }
```

Description

Enables the external alarm output which is based on configurable sources.

Inserting **no** as a prefix for this command will disable the external alarm.

Syntax

Parameter	Description
fan	Enables external alarm for fan failure.
psu	Enables external alarm for power supply failure.
in1	Enables external alarm for external alarm input 1.
in2	Enables external alarm for external alarm input 2.
in3	Enables external alarm for external alarm input 3. Available only on equipments with DB9 alarm interface.
invert	(Optional) Disable inverted read of alarm input signal levels.

Default

External alarm output is disabled for all sources.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
7.8	The option invert was introduced.
14.6	The option in3 was removed from equipments with RJ45 alarm interface.

Usage Guidelines

Use the external alarm output to send an electrical signal to an external device based on internal and/or external events.

Example

This example shows how to enable the external alarm for fan failure.

```
DmSwitch(config)#external-alarm fan
DmSwitch(config)#
```

You can verify that the alarm was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

debug-counters rx

```
debug-counters rx { all | attack { all | dsfrag | dsicmp | dsl3he | dsl4he }  
discard { all | pdisc | rdisc | ripd4 | ripd6 } drop { all | classbasedmovedrop |  
dstdiscarddrop | maclmt_drop | maclmt_ndrop | rdrop | rfildr | rimdr | rportd |  
vfpdr | vlandr } error { all | hghdre | mcidxe | mplseerr | parityd | riphe4 | riphe6 }  
received/others { all | irhol | iribp | mpl | rhgmc | rhguc | ripc4 | ripc6 | rtun |  
rtune | ruc | imbp | imirror | imrp4 | imrp6 | irpse | iunkhdr | laglup | laglupd |  
mtuerr | urpf | urpferr } } [ unit { unit-number | range first-unit-number last-unit-number } ]
```

Description

Configures debug-counters to count according to the enabled triggers.

Inserting **no** as a prefix for this command will disable the selected configuration.

If the configured unit is not present, the configuration will be applied when it is detected.

Syntax

Parameter	Description
all	Enable all triggers of all groups. If a group was specified, will enable all triggers for that group.
attack	Configure the attack trigger's group.
dsfrag	Configure the dsfrag trigger.
dsicmp	Configure the dsicmp trigger.
dsl3he	Configure the dsl3he trigger. Note that this trigger is only applicable to packet from 10GE port and should not be enabled otherwise.
dsl4he	Configure the dsl4he trigger. Note that this trigger is only applicable to packet from 10GE port and should not be enabled otherwise.
discard	Configure the discard trigger's group.
pdisc	Configure the pdisc trigger.
rdisc	Configure the rdisc trigger.
ripd4	Configure the ripd4 trigger.
ripd6	Configure the ripd6 trigger.
drop	Configure the drop trigger's group.
classbasedmovedrop	Configure the classbasedmovedrop trigger.
dstdiscarddrop	Configure the dstdiscarddrop trigger.
maclmt_drop	Configure the maclmt_drop trigger.
maclmt_ndrop	Configure the maclmt_ndrop trigger.
rdrop	Configure the rdrop trigger.
rfildr	Configure the rfildr trigger.
rimdr	Configure the rimdr trigger.

Parameter	Description
rportd	Configure the rportd trigger.
vfpdr	Configure the vfpdr trigger.
vlandr	Configure the vlandr trigger.
error	Configure the error trigger's group.
hghdre	Configure the hghdre trigger.
mcidxe	Configure the mcidxe trigger.
mplserr	Configure the mplserr trigger.
parityd	Configure the parityd trigger.
riphe4	Configure the riphe4 trigger.
riphe6	Configure the riphe6 trigger.
received/others	Configure the attack trigger's group.
irhol	Configure the irhol trigger.
iribp	Configure the iribp trigger.
mpls	Configure the mpls trigger.
rhgmc	Configure the rhgmc trigger.
rhguc	Configure the rhguc trigger.
rpc4	Configure the rpc4 trigger.
rpc6	Configure the rpc6 trigger.
rtun	Configure the rtun trigger.
rtune	Configure the rtune trigger.
ruc	Configure the ruc trigger.
imbp	Configure the imbp trigger.
imirror	Configure the imirror trigger. Note that this triggers is only applicable to packet from HiGig port and should not be enabled otherwise.
imrp4	Configure the imrp4 trigger.
imrp6	Configure the imrp6 trigger.
irpse	Configure the irpse trigger.
iunkhdr	Configure the iunkhdr trigger. Note that this triggers is only applicable to packet from HiGig port and should not be enabled otherwise.
laglup	Configure the laglup trigger.
laglupd	Configure the laglupd trigger.
mtuerr	Configure the mtuerr trigger.
urpf	Configure the urpf trigger.
urpferr	Configure the urpferr trigger.
unit <i>unit-number</i>	Specify a unit to receive the configuration.
unit range <i>first-unit-number last-unit-number</i>	Configure a range of units.

Default

Default is all triggers disabled. If no unit is specified for the command, the configuration will be applied for all units of the stacking.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command configures the counting of debug packets in the debug counters. To display the counters values refer to **show interfaces counters** command.

Example

This example shows how to enable all triggers that increment the RX counter of the attack group for all units.

```
DmSwitch(config)#debug-counters rx attack all
DmSwitch(config)#
```

You can verify the debug-counters configuration by entering the **show debug-counters rx all** privileged EXEC command.

Related Commands

Command	Description
show debug counters rx	Shows debug-counters RX configuration.
show interfaces counters	Shows the interface counters information.

fetch tftp

```
fetch tftp { public-key { ip-address public-key-file-name user-name } |  
https-certificate { ip-address certificate-file-name private-key-file-name password } }
```

Description

Fetches a key or certificate from a tftp server.

Syntax

Parameter	Description
public-key	Fetches a public-key.
<i>ip-address</i>	Specifies the server from which the public key will be obtained.
<i>public-key-file-name</i>	Specifies the file that contains the public key.
<i>user-name</i>	Specifies the user name for the key or certificate.
https-certificate	Fetches a https-certificate.
<i>certificate-file-name</i>	Specifies the filename that contains the https certificate.
<i>private-key-file-name</i>	Specifies the name of the file for the private key.
<i>password</i>	Specifies the password for the certificate.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to fetch a public key from TFTP server for user "test".

```
DmSwitch#fetch tftp public-key 10.20.30.40 key_dsa.pub test  
DmSwitch#
```

Related Commands

Command	Description
<code>show public-key</code>	Shows the public key information.
<code>show running-config</code>	Shows the current operating configuration.

filter

```
filter { pre-ingress | ingress | egress } new { action parameters } [ out-action parameters | match parameters | meter meter-id [ meter-id ] | remark text | priority priority | ethernet parameters | local-tunnel ltn-endpoint endpoint | cpu | disable | enable ]
```

```
filter { pre-ingress | ingress | egress } id { action parameters | out-action parameters | match parameters | meter meter-id [ meter-id ] | remark text | priority priority | ethernet parameters | local-tunnel ltn-endpoint endpoint | cpu | disable | enable }
```

```
no filter { all | { pre-ingress | ingress | egress { all | id } } }
```

Description

Create or configure a traffic filter. Filters can match packets by various protocol fields and perform actions that change, discard or forward the packet in some ways.

Inserting **no** as a prefix for this command will delete the filter specified.

Syntax

Parameter	Description
pre-ingress	Filter is related to pre-ingress stage.
ingress	Filter is related to ingress stage.
egress	Filter is related to egress stage.
new	Creates a new filter
<i>id</i>	Selects a filter to edit by ID
Action parameters	Adds an action to the filter
permit	Causes the packet to be switched
deny	Discards the packet
802.1p-from-inner-vlan	Change packet and internal 802.1p priority from inner VLAN tag
802.1p priority	Change packet and internal 802.1p priority value
802.1p-from-tos	Change packet and internal 802.1p priority from IP ToS Precedence
green-802.1p priority	Change packet and internal 802.1p priority of green packet
yellow-802.1p priority	Change packet and internal 802.1p priority of yellow packet
red-802.1p priority	Change packet and internal 802.1p priority of red packet
counter counter-id	Associate a counter
drop-precedence green	Internally set the drop-precedence of the packet to green
drop-precedence yellow	Internally set the drop-precedence of the packet to yellow
drop-precedence red	Internally set the drop-precedence of the packet to red
dscp ip-value	Change Differentiated Services Code Point
ecn enc-value	Change ECN-Capable Transport (ECT) bit in the DSCP/ToS field

Action parameters	Adds an action to the filter
egress-block ethernet range <i>[first-unit-number/] first-port-number [last-unit-number/] last-port-number</i>	Set range of ethernet ports to block
egress-block ethernet <i>[unit-number/] port-number</i>	Set Ethernet port to block
egress-block cpu	Block traffic to CPU
int-802.1p priority	Change internal 802.1p priority value
int-802.1p-from-inner-vlan	Change internal 802.1p priority from inner VLAN tag
int-802.1p-from-tos	Change internal 802.1p priority from IP ToS Precedence
pkt-802.1p priority	Change packet 802.1p priority value
pkt-802.1p-from-inner-vlan	Change packet 802.1p priority from inner VLAN tag
pkt-802.1p-from-tos	Change packet 802.1p priority from IP ToS Precedence
red-deny	Discard red packet
red-drop-precedence green	Internally change the drop precedence of red packet to the green
red-drop-precedence yellow	Internally change the drop precedence of red packet to yellow
red-drop-precedence red	Internally change the drop precedence of red packet to red
red-dscp <i>ip-dscp-value</i>	Change Differentiated Services Code Point of red packet
red-int-prio priority	Change internal 802.1p priority of red packet
yellow-deny	Discard yellow packet
yellow-drop-precedence green	Internally change the drop precedence of yellow packet to green
yellow-drop-precedence yellow	Internally change the drop precedence of yellow packet to yellow
yellow-drop-precedence red	Internally change the drop precedence of yellow packet to red
yellow-dscp <i>ip-dsc-value</i>	Change Differentiated Services Code Point of yellow packet
yellow-int-prio priority	Change internal 802.1p priority of yellow packet
green-int-prio priority	Change internal 802.1p priority of green packet
inner-vlan <i>vlan-id</i>	Change inner VLAN ID of packet
inner-vlan-802.1p priority	Change inner VLAN 802.1p priority of packet
vlan <i>vlan-id</i>	Change outer VLAN ID of packet
vlan-802.1p priority	Change outer VLAN 802.1p priority of packet
destination-mac <i>MAC address</i>	Overwrite destination MAC address of packet
source-mac <i>MAC address</i>	Overwrite source MAC address of packet

Match parameters	Sets a packet field to be matched
802.1p priority	Specifies 802.1p priority value (for outer or single tag)
802.1p-inner priority	Specifies 802.1p priority value (for inner tag)
all	Matches all packets
destination-ip host <i>ip</i>	Specify a single IP address
destination-ip range <i>first-ip last-ip</i>	Specify a range of IP addresses
destination-ip <i>ip netmask</i>	Specify a maskable IP address
destination-ipv6 host <i>ipv6</i>	Specify a single IPv6 address
destination-ipv6 high <i>ipv6</i>	Specify top 64 bits of an IPv6 address

Match parameters	Sets a packet field to be matched
destination-ipv6 <i>ipv6/prefix</i>	Specify destination IPv6 address and its prefix
destination-mac <i>host mac-address</i>	Specify host destination MAC address
destination-mac <i>mac-netmask</i>	Specify a maskable destination MAC address (XX:XX:XX:XX:XX:XX)
destination-port <i>first-L4-port last-L4-port</i>	Specify range of destination L4 port
destination-port <i>range L4-port</i>	Specify destination L4 port
dscp <i>ip-dscp-value</i>	Specify IP DSCP field
ethertype <i>ethertype</i>	Specify single EtherType field
ethertype <i>range first-ethertype last-ethertype</i>	Specify range of L4 port numbers
ipv6-flow-label <i>flow-label mask</i>	Specify 20 bits of an IPv6 Flow-Label
mpls-label <i>mpls-label-value</i>	Specify MPLS label
protocol <i>icmp</i>	Set L4 protocol to Internet Control Message Protocol
protocol <i>tcp</i>	Set L4 protocol to Transmission Control Protocol
protocol <i>udp</i>	Set L4 protocol to User Datagram Protocol
protocol <i>value</i>	Set L4 protocol to IP Protocol field value
source-ip <i>host ip</i>	Specify source single IP address
source-ip <i>range first-ip last-ip</i>	Specify source range of IP addresses
source-ip <i>ip-netmask</i>	Specify source maskable IP address
source-ipv6 <i>host ipv6</i>	Specify source single IPv6 address
source-ipv6 <i>high ipv6</i>	Specify top 64 bits of an IPv6 address
source-ipv6 <i>ipv6/prefix</i>	Specify source IPv6 address and its prefix
source-mac <i>host mac-address</i>	Specify host source MAC address
source-mac <i>mac-netmask</i>	Specify maskable source MAC address (XX:XX:XX:XX:XX:XX)
source-port <i>L4-port</i>	Specify single source L4 port
source-port <i>range L4-port</i>	Specify source source L4 port
tos-bits <i>tos-value</i>	Specify IP ToS lower bits
tos-precedence <i>tos-precedence-value</i>	Specify IP ToS Precedence
ttl <i>ttl-value</i>	Specify IP TTL value
vlan <i>vlan-id</i>	Specify single VLAN ID (outer/single tag)
vlan <i>range first-vlan-id last-vlan-id</i>	Specify range of VLAN ID (outer/single tag)
vlan-inner <i>vlan-id</i>	Specify single VLAN ID (inner tag)
vlan-inner <i>range first-vlan-id last-vlan-id</i>	Specify range of VLAN ID (inner tag)
Other parameters	Description
disable	Disables the filter
enable	Enables the filter
ethernet	Applies the filter to an Ethernet port
ethernet all	Apply the filter to all Ethernet ports

Other parameters	Description
ethernet range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Apply the filter to a range of specific units and ports
local-tunnel ltn-endpoint <i>endpoint</i>	Applies the filter to an endpoint in local-tunnel interface
cpu	Applies the filter to the CPU interface
meter <i>meter-id</i> [<i>meter-id</i>]	Sets a meter to be associated to this filter. A second meter-id may be specified to configure hierarchical metering.
out-action <i>parameters</i>	Action when the packet is out-of-profile (meter) [1]
remark <i>text</i>	Adds a remark text
priority <i>priority</i>	Configures the filter priority. Higher values indicate better priority.

Default

By default, no filter is created.

A new filter matches all packets if no match parameters are specified.

A new filter is applied to all ports if no ingress ports are specified.

A new ingress filter has a default priority of 8 if no priority is specified.

A new egress filter has a default priority of 0 if no priority is specified.

Command Modes

Global configuration.

Command History

Release	Modification	
3.1	This command was introduced.	
4.0	The <i>match generic</i> parameter was added.	
4.1	The following matching options were added: vlan-inner , 802.1p-inner , source-ip range and destination-ip range . In a new filter with no ingress port set, the default behavior was changed to apply it to all ingress ports.	
11.6	<i>ingress</i> <i>egress</i> parameter was added.	
12.0	The mpls-label matching option were added.	
12.2	The following matching options were added: ipv6-flow-label , source-ipv6 , source-ipv6-high , destination-ipv6 , destination-ipv6-high and mpls-label .	The following matching
12.4	The following actions options were added: inner-vlan , inner-vlan-802.1p , vlan and vlan-802.1p .	
13.4	Added egress filter support to DM4100 boards.	

Release	Modification
13.5	The following matching options were added for egress filters: 802.1p , 802.1p-inner , destination-mac , dscp .
13.8.4	Added new match for egress filters: vlan-inner .
14.4	Added support to hierarchical metering.
14.6	The following actions options were added: destination-mac and source-mac .
14.10.2	The following matching option was added: ttl .
15.2.6	The TTL matching option was made available for egress filters.

Usage Guidelines

Each filter created may specify multiple non-conflicting actions and multiple matches. Multiple actions are applied in parallel. Multiple matches are combined as a logical AND.

Filter priorities are used when two or more filters match the same packet and their actions conflict (i.e. the actions modify the same packet field(s) or they are permit/deny actions). In that case the highest priority filter has its action executed. Filters can share the same priority if their matches are related to the same packet fields (but not the same field values).

A filter containing matches with ranges of values may require additional resources to be implemented. That corresponds to more than one priority being necessary for the filter. If that is the case, the user will be informed at filter creation. If the filter requires N priorities to be implemented, there must be N available priorities beginning on the filter specified priority.

That need for additional priorities is related to the range starting and ending values. No additional priorities are needed when the range is aligned with power of two values (i.e. when the lower limit is a power of two and the upper limit is a power of two minus one).

When editing a filter, only the specified properties are changed. If the editing includes one or more matches, all original filter matches are removed. If it includes actions, all original actions are removed.

Filter for Local-tunnel and CPU interfaces are only available for egress filters in equipments where such interfaces are available. Enable local-tunnel interface before creating the filter for this interface. Only one kind of interface may be specified for a single filter. Specify one from local-tunnel endpoint, CPU or ethernet interface. When none is specified, an egress filter will match all interfaces, including local-tunnel and CPU.

The table below shows all actions and the stage where they are available.

Action	Ingress	Egress	Pre-ingress
permit	X	X	X
deny	X	X	X
802.1p-from-inner-vlan	X		
802.1p	X		

Action	Ingress	Egress	Pre-ingress
802.1p-from-tos	X		
green-802.1p	X		
yellow-802.1p	X		
red-802.1p	X		
counter	X	X	
drop-precedence green	X		
drop-precedence yellow	X		
drop-precedence red	X		
dscp	X	X	
enc	X		
egress-block	X		
inner-vlan		X	X
inner-vlan-802.1p		X	
int-802.1p	X		
int-802.1p-from-inner-vlan	X		
int-802.1p-from-tos	X		
vlan	X	X	X
vlan-802.1p		X	
pkt-802.1p	X		
pkt-802.1p-from-inner-vlan	X		
pkt-802.1p-from-tos	X		
red-deny	X	X	
red-drop-precedence	X		
red-dscp	X	X	
red-int-prio	X		
yellow-deny	X	X	
yellow-drop-precedence	X		
yellow-dscp	X	X	
yellow-int-prio	X		
green-int-prio	X		
destination-mac	X		
source-mac	X		

The table below shows all matches and the stage where they are available.

Match	Ingress	Egress	Pre-ingress
802.1p	X	X	
802.1p-inner	X	X	
all	X	X	X
destination-ip	X	X	X
destination-ipv6	X	X	X
destination-mac	X	X	
destination-port	X	X	X

Match	Ingress	Egress	Pre-ingress
dscp	X	X	
ethertype	X		
ipv6-flow-label	X		
mpls-label	X		
protocol	X		X
source-ip	X	X	X
source-ipv6	X	X	X
source-mac	X		
source-port	X	X	X
tos-bits	X		
tos-precedence	X		
ttl	X	X	X
vlan	X	X	X
vlan-inner	X	X	

Example

This example shows how to create an ingress filter to discard all tcp packets incoming in the interface Ethernet 1.

```
DmSwitch(config)#filter ingress new action deny match protocol tcp ethernet 1 remark tcp_discard
Filter 1 created.
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show filter** privileged EXEC command.

Related Commands

Command	Description
show filter	Shows filters information.
meter	Configures a meter to be used by a filter
counter	Configures a counter to be used by a filter
show running-config	Shows the current operating configuration.

Notes

[1] - out-action is available only to DM3000 Switches.

hostname

hostname *name*

Description

Specifies a hostname for the equipment.

Syntax

Parameter	Description
<i>name</i>	Specifies a name.

Default

Default hostname is "DmSwitch 3000".

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the hostname "ClientABC".

```
DmSwitch(config)#hostname ClientABC
ClientABC(config)#
```

It is possible to verify the hostname by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

hqos

```
hqos { new | id } ingress ethernet parameters [ ingress ethernet parameters ] { vlan
vlan-id | vlan-inner vlan-id } rate-limit rate-limit burst-size [ priority priority | remark
text ]
```

```
no hqos id
```

Description

Create or configure an HQoS domain. HQoS domains guarantees a constant bandwidth to it's services through traffic shapping mechanism.

Inserting **no** as a prefix for this command will delete the HQoS domain specified.

Syntax

Parameter	Description
new	Create a new HQoS domain
id	Select an HQoS domain to edit by ID
<hr/>	
Ingress Ethernet parameters	Description
[unit-number/]	Apply the HQoS domain to an Ethernet port
port-number	
all	Apply the HQoS domain to all Ethernet ports
range [<i>first-unit-number/</i>]	Apply the HQoS domain to a range of specific units and ports
<i>first-port-number</i> [<i>last-unit-number/</i>]	
<i>last-port-number</i>	
<hr/>	
Other parameters	Description
vlan <i>vlan-id</i>	Specify VLAN ID (outer/single tag)
vlan-inner <i>vlan-id</i>	Specify VLAN ID (inner tag)
rate-limit <i>rate-limit burst-size</i>	Rate limit in kbit/s (64 kbit/s granularity) and Burst size in kbyte (power of 2)
remark <i>text</i>	Add a remark text
priority <i>priority</i>	Configure the HQoS priority. Higher values indicate better priority.

Default

By default, no HQoS domain is created.

A new HQoS domain has a default priority of 8 if no priority is specified.

Command Modes

Privileged EXEC.

Global configuration.

Command History

Release	Modification
11.4	This command was introduced.

Usage Guidelines

The HQoS configuration must be applied at the first equipment of the MPLS network.

The HQoS acts unidirectionally, the traffic shapping will act only over data that will be entering at the specified ports. No action is taken with the data that leaves at the same ports.

Each domain is identified by a vlan. Different domains can't refer to the same vlan.

Example

This example shows how to create an HQoS domain to guarantee 10048 kbit/s to all traffic tagged with vlan 51 that enters by interface ethernet 4.

```
DmSwitch(config)#hqos new ingress ethernet 1/4 vlan 51 rate-limit 10048 4
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show hqos** privileged EXEC command.

Related Commands

Command	Description
service	Creates or configures an HQoS service
show hqos	Shows HQoS information.
show running-config	Shows the current operating configuration.

interface bundle

```
interface bundle { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ]  
first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

Enables the interface configuration mode.

Syntax

Parameter	Description
all	Enables for all ports.
[unit-number/] port-number	Enables for a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Enables for a range of specific units and ports.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the interface configuration mode for interface range 1 to 10 of unit 1.

```
DM4000#interface bundle range 1/1 1/10  
DM4000(config-if-bundle-1/1-to-1/10)#
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

No related command.

interface ethernet

```
interface ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-  
port-number [ last-unit-number/ ] last-port-number } }
```

Description

Enables the interface configuration mode.

Syntax

Parameter	Description
all	Enables for all ports.
[unit-number/] port-number	Enables for a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Enables for a range of specific units and ports.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the interface configuration mode for port range 1 to 10 of unit 1.

```
DmSwitch#interface ethernet range 1/1 1/10  
DmSwitch(config-if-eth-1/1-to-1/10)#
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

No related command.

interface g704

```
interface g704 { all | [ unit-number/ ] interface-number | range { [ first-unit-number/ ]  
first-interface-number [ last-unit-number/ ] last-interface-number } }
```

Description

Enables the interface configuration mode.

Syntax

Parameter	Description
all	Enables for all ports.
[unit-number/] interface-number	Enables for a specific unit and interface.
range { [first-unit-number/] first-interface-number [last-unit-number/] last-interface-number	Enables for a range of specific units and interface.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the interface configuration mode for interface range 1 to 10 of unit 1.

```
DM4000#interface g704 range 1/1 1/10  
DM4000(config-if-g704-1/1-to-1/10)#
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

No related command.

interface e1c

```
interface e1c { all | [ unit-number/ ] interface-number | range { [ first-unit-number/ ]  
first-interface [ last-unit-number/ ] last-interface } }
```

Description

Enables the interface configuration mode.

Syntax

Parameter	Description
all	Enables for all ports.
[<i>unit-number/</i>] <i>interface-number</i>	Enables for a specific unit and interface.
range { [<i>first-unit-number/</i>] <i>first-interface</i> [<i>last-unit-number/</i>] <i>last-interface</i> }	Enables for a range of specific units and interface (range: 1-252).

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to enable the interface configuration mode for interface range 1 to 100 of unit 1.

```
DM4000#interface e1c range 1/1 1/100  
DM4000(config-if-e1c-1/1-to-1/100)#
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

No related command.

interface ip-tunnel

```
interface ip-tunnel { index }
```

Description

Enables the IP tunnel configuration mode. The IP tunnel is created and enabled if it does not exist.

Syntax

Parameter	Description
<i>index</i>	Enables for a specific IP tunnel index. (Range: 1-64)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable a specific IP tunnel.

```
DmSwitch#interface ip-tunnel 10
DmSwitch(config-if-ip-tunnel) #
```

Related Commands

No related command.

interface local-tunnel ^[5][7]

```
interface local-tunnel
```

Description

Enables the local tunnel configuration mode.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the configuration mode for local tunnel interfaces.

```
DmSwitch(config)#interface local-tunnel
DmSwitch(config-local-tunnel)#
```

Related Commands

Command	Description
<code>show interfaces local-tunnel</code>	Shows the local-tunnel interfaces.

interface loopback

interface loopback *loopback-number*

Description

Enables the loopback configuration mode. The loopback is created if it doesn't exist.

Syntax

Parameter	Description
<i>loopback-number</i>	Enables for a specific loopback. The loopback must be specified in accordance with the loopback configured in the switch. (Range: 0-7)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the interface configuration mode for loopback 1.

```
DmSwitch(config)#interface loopback 1
DmSwitch(config-if-lo-1)#
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

Command	Description
mpls enable	Enables MPLS on the specified loopback interface.

Command	Description
<code>show interfaces loopback</code>	Shows the interfaces loopback.

interface port-channel

```
interface port-channel { port-channel-number | range { [ first-port-number ] [ last-port-number ] } }
```

Description

Enables the port-channel configuration mode. The port-channel is created if it doesn't exist.

Syntax

Parameter	Description
<i>port-channel-number</i>	Enables for a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
11.2	The option range in command port-channel was introduced.
13.6	The maximum number of port-channels was raised to 128.

Usage Guidelines

Not available.

Example

This example shows how to enable the interface configuration mode for port-channel 1.

```
DmSwitch#interface port-channel 1
DmSwitch(config-if-port-ch-1)#
```

Other example shows how to enable the interface configuration mode for port range 1 to 3.

```
DmSwitch#interface port-channel range 1 3
```

```
DmSwitch(config-if-port-ch-1-to-3) #
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

No related command.

interface private-vlan

```
interface private-vlan { index }
```

```
no interface private-vlan { index }
```

Description

Enables the Private VLAN configuration mode. The Private VLAN is created and enabled if it does not exist.

Inserting **no** as a prefix for this command will remove the specified Private VLAN.

Syntax

Parameter	Description
<i>index</i>	Enables for a specific Private VLAN index. (Range: 1-4094)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable a Private VLAN with index 10.

```
DmSwitch#interface private-vlan 10
DmSwitch(config-if-pvlan-10)#
```

You can verify that the Private VLAN was accepted as it is shown in the new prompt.

Related Commands

Command	Description
<code>isolated-vlan</code>	Enables the isolated VLAN configuration mode.
<code>community-vlan</code>	Enables the community VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.

interface ptp

```
interface ptp { all | [ unit-number/ ] interface-number | range { [ first-unit-number/ ]  
first-interface-number [ last-unit-number/ ] last-interface-number } }
```

Description

Enables the interface configuration mode.

Syntax

Parameter	Description
all	Enables for all ports.
[unit-number/] interface-number	Enables for a specific unit and interface.
range { [first-unit-number/] first-interface-number [last-unit-number/] last-interface-number	Enables for a range of specific units and interface.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the interface configuration mode for interface range 1 to 10 of unit 1.

```
DM4000#interface ptp range 1/1 1/10  
DM4000(config-if-ptp-1/1-to-1/10)#
```

You can verify that the port range was accepted as it is shown in the new prompt.

Related Commands

No related command.

interface sdh

```
interface sdh { all | [ unit-number/ ] interface-number | range { [ first-unit-number/ ]  
first-interface-number [ last-unit-number/ ] last-interface-number } }
```

Description

Enables the SDH interface configuration mode.

Syntax

Parameter	Description
all	Select configuration mode for all interfaces.
[<i>unit-number/</i>] <i>interface-number</i>	Select configuration mode for a specific unit and interface.
range { [<i>first-unit-number/</i>] <i>first-interface-number</i> [<i>last-unit-number/</i>] <i>last-interface-number</i>	Select configuration mode for a specific range of unit and interfaces.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to enable the interface configuration mode for interface range 1 of unit 2.

```
DM4000#interface sdh 2/1  
DM4000(config-if-sdh-2/1)#
```

You can verify that the command was accepted as it is shown in the new prompt.

Related Commands

Command	Description
<code>show sdh-map</code>	Show the mappings of SDH interfaces.

interface vlan

```
interface vlan { all | index | range first-index last-index }
```

Description

Enables the VLAN configuration mode. The VLAN is created and enabled if it does not exist. Enables the VLAN if it is disabled and already exists.

Syntax

Parameter	Description
all	Enables for all VLANs.
<i>index</i>	Enables for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Enables for a range of specific VLANs index. (Range: 1-4094)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable for all VLANs.

```
DmSwitch#interface vlan all
Iterating over 4094 VLANs. Next commands may take a while...
DmSwitch(config-if-vlan-all)#
```

You can verify that the VLAN range was accepted as it is shown in the new prompt.

Related Commands

No related command.

ip default-gateway

```
ip default-gateway { ip-address | black-hole }
```

```
no ip default-gateway
```

Description

Configures the default gateway for DmSwitch.

Inserting **no** as a prefix for this command will remove the default gateway.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the default gateway IP address.
black-hole	Specifies a default gateway with no output interface (black hole).

Default

No default gateway is configured.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
9.4	The parameter black-hole was introduced.

Usage Guidelines

As opposed to a regular IP based default gateway, a black hole default gateway is installed only in the Routing Information Base (RIB), but not in the Forwarding Information Base (FIB). The black hole default gateway is used in BGP so that, along with the prefix-list command, it can distribute a default route to its neighbors.

Example

This example shows how to configure the IP address "10.1.1.1" for default gateway of DmSwitch.

```
DmSwitch(config)#ip default-gateway 10.1.1.1
DmSwitch(config)#
```

You can verify that the IP address was configured by entering the **show ip default-gateway** privileged EXEC command.

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
show ip default-gateway	Shows the configured default gateway.
show ip route	Shows the IP routing table.
show running-config	Shows the current operating configuration.

ipv6 default-gateway

```
ipv6 default-gateway { ipv6-address | black-hole }
```

```
no ipv6 default-gateway
```

Description

Configures the IPv6 default gateway for DmSwitch.

Inserting **no** as a prefix for this command will remove the IPv6 default gateway.

Syntax

Parameter	Description
<i>ipv6-address</i>	Specifies the default gateway IPv6 address.
black-hole	Specifies a default gateway with no output interface (black hole).

Default

No IPv6 default gateway is configured.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

As opposed to a regular IPv6 based default gateway, a black hole default gateway is installed only in the Routing Information Base (RIB), but not in the Forwarding Information Base (FIB). The black hole default gateway is used in BGP so that, along with the prefix-list command, it can distribute a default route to its neighbors.

Example

This example shows how to configure the IP address "2001:db8::1" for default gateway of DmSwitch.

```
DmSwitch(config)#ipv6 default-gateway 2001:db8::1
DmSwitch(config)#
```

You can verify that the IPv6 address was configured by entering the **show ipv6 default-gateway** privileged EXEC command.

Related Commands

Command	Description
ipv6 address	Sets an IPv6 address for the selected VLAN.
show ipv6 default-gateway	Shows the configured IPv6 default gateway.
show ipv6 route	Shows the IPv6 routing table.
show running-config	Shows the current operating configuration.

ip dhcp relay

ip dhcp relay

no ip dhcp relay

Description

Enables DHCP relay globally.

Inserting **no** as a prefix for this command will disable DHCP relay globally.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate DHCP relay globally.

```
DmSwitch(config)#ip dhcp relay
DmSwitch(config)#
```

You can verify that the DHCP relay was enabled by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>ip dhcp relay</code>	Enables DHCP relay on the selected Vlan.
<code>ip dhcp relay information option</code>	Enables DHCP Agent Information Option (option 82).
<code>ip dhcp relay information trusted</code>	Mark a Vlan as a trusted interface.
<code>ip helper-address</code>	Add an address to the list of DHCP servers global.
<code>ip helper-address</code>	Add an address to the VLAN list of DHCP servers in VLAN.
<code>show ip dhcp relay</code>	Shows the DHCP relay settings.

ipv6 dhcp relay

ipv6 dhcp relay

no ipv6 dhcp relay

Description

It enables the global DHCPv6 relay.

Inserting **no** as a prefix for this command will disable the global DHCPv6 relay.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate the global DHCPv6 relay.

```
DmSwitch(config)#ipv6 dhcp relay
DmSwitch(config)#
```

You can verify that the status of global DHCPv6 relay by entering the **show ipv6 dhcp relay** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
ipv6 dhcp relay	It enables the global DHCPv6 relay.
ipv6 helper-address	It adds unicast or multicast IPv6 address into the list of DHCPv6 servers global.
ipv6 dhcp relay	It enables the DHCPv6 relay agent on a VLAN.
show ipv6 dhcp relay	It shows the details about DHCPv6 relay configurations.

ip dhcp relay information option

```
ip dhcp relay information option
```

```
no ip dhcp relay information option
```

Description

Enables DHCP Agent Information Option (option 82).

Inserting **no** as a prefix for this command will disable DHCP Agent Information Option.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate DHCP Agent Information Option.

```
DmSwitch(config)#ip dhcp relay information option
DmSwitch(config)#
```

You can verify that the DHCP relay was enabled by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>ip dhcp relay</code>	Enables DHCP relay globally.
<code>ip dhcp relay</code>	Enables DHCP relay on the selected Vlan.
<code>ip dhcp relay information trusted</code>	Mark a Vlan as a trusted interface.
<code>ip helper-address</code>	Add an address to the list of DHCP servers global.
<code>ip helper-address</code>	Add an address to the VLAN list of DHCP servers in VLAN.
<code>show ip dhcp relay</code>	Shows the DHCP relay settings.

ip dhcp relay information trusted

```
ip dhcp relay information trusted { all | index | range first-index last-index }
```

```
no ip dhcp relay information trusted { all | index | range first-index last-index }
```

Description

Mark a Vlan as a trusted interface. If a packet is received with the option 82 field set, and a giaddr field not set, the packet is discarded, unless the incoming packet came from a trusted interface.

Inserting **no** as a prefix for this command will mark the selected vlan as untrusted.

Syntax

Parameter	Description
all	Enables for all VLANs.
<i>index</i>	Enables for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Enables for a range of specific VLANs index. (Range: 1-4094)

Default

All untrusted.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.
13.2	This command was removed.

Usage Guidelines

Not available.

Example

This example shows how to mark Vlan 2 as a trusted interface.

```
DmSwitch(config)#ip dhcp relay information trusted 2
```

```
DmSwitch(config)#
```

You can verify that the Vlan is marked as trusted by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
ip dhcp relay	Enables DHCP relay globally.
ip dhcp relay	Enables DHCP relay on the selected Vlan.
ip dhcp relay information option	Enables DHCP Agent Information Option (option 82).
ip helper-address	Add an address to the list of DHCP servers global.
ip helper-address	Add an address to the VLAN list of DHCP servers in VLAN.
show ip dhcp relay	Shows the DHCP relay settings.

ip dhcp relay vlan

```
ip dhcp relay vlan { all | index | range first-index last-index }
```

```
no ip dhcp relay vlan { all | index | range first-index last-index }
```

Description

Enables DHCP relay on the selected vlan.

Inserting **no** as a prefix for this command will disable DHCP relay on vlan.

Syntax

Parameter	Description
all	Enables for all VLANs.
<i>index</i>	Enables for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Enables for a range of specific VLANs index. (Range: 1-4094)

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.
13.2	This command was removed.

Usage Guidelines

Not available.

Example

This example shows how to activate DHCP relay on Vlan 2.

```
DmSwitch(config)#ip dhcp relay
DmSwitch(config)#ip dhcp relay vlan 2
DmSwitch(config)#
```


You can verify that the DHCP relay was activated by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
ip dhcp relay	Enables DHCP relay globally.
ip dhcp relay	Enables DHCP relay on the selected Vlan.
ip dhcp relay information option	Enables DHCP Agent Information Option (option 82).
ip dhcp relay information trusted	Mark a Vlan as a trusted interface.
ip helper-address	Add an address to the list of DHCP servers global.
ip helper-address	Add an address to the VLAN list of DHCP servers in VLAN.
show ip dhcp relay	Shows the DHCP relay settings.

ip dhcp pool

ip dhcp pool

Description

Enables the DHCP pool configuration mode.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

ipv6 dhcp server

ipv6 dhcp server

Description

Enables the DHCPv6 server configuration mode.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

ipv6 dhcp pool

`ipv6 dhcp pool`

Description

Enables the DHCPv6 pool configuration mode. Only stateless mode is supported - RFC 3736.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Related Commands

Command	Description
<code>ipv6 dhcp server</code>	Enables the DHCPv6 server configuration mode.
<code>enable</code>	Enables the DHCPv6 server globally.
<code>ipv6 dhcp pool</code>	Enables the DHCPv6 pool configuration mode.
<code>network</code>	Configure the IPv6/prefix for the DHCPv6 pool.
<code>sip-address</code>	Configure SIP addresses for the DHCPv6 pool.
<code>sip-domain</code>	Configure SIP domain names for the DHCPv6 pool.
<code>dns-server</code>	Configure DNS servers for the DHCPv6 pool.
<code>domain-search</code>	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
<code>show ipv6 dhcp server</code>	Shows the DHCPv6 server settings and status.
<code>show ipv6 dhcp pool</code>	Shows the DHCPv6 pool settings.

ip dhcp server

ip dhcp server

Description

Enables the DHCP server configuration mode.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

ip dhcp snooping

`ip dhcp snooping`

`no ip dhcp snooping`

Description

Enables DHCP Snooping globally.

Inserting **no** as a prefix for this command will disable DHCP Snooping globally.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate DHCP Snooping globally.

```
DmSwitch(config)#ip dhcp snooping
DmSwitch(config)#
```

You can verify that the global DHCP Snooping configuration was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>ip dhcp snooping</code>	Enables DHCP Snooping at VLAN.
<code>ip dhcp snooping verify mac-address</code>	Enables configuration to verify mac-address on a DHCP Snooping message.
<code>ip dhcp snooping trust</code>	Configures port as trusted for DHCP Snooping.

ip dhcp snooping cyclic save timer

```
ip dhcp snooping cyclic-save-timer { flash | file } time-value
```

```
no ip dhcp snooping cyclic-save-timer { flash | file }
```

Description

Configures a DHCP Snooping Database cyclic timer to save the database entries to a file (temporary file or flash memory) to be restored in case of switchover or change master (temporary file) or reboot (flash memory).

Inserting **no** as a prefix for this command will remove the entry.

Syntax

Parameter	Description
<i>time-value</i>	Specifies a time value to save file cyclic. (Range: 1-50000 secs)

Default

No timer configured.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command configures the time interval to save entries of DHCP Snooping Database to a file. The flash option only copies the file from temporary file to flash memory if it exists.

Example

```
DmSwitch(config)#ip dhcp snooping cyclic-save-timer file 10
DmSwitch(config)#
```

You can verify if the configuration is set by using **show ip dhcp snooping database** privileged EXEC command.

Related Commands

Command	Description
<code>ip dhcp snooping vlan binding</code>	Creates a DHCP Snooping Database entry
<code>show ip dhcp snooping database</code>	Shows DHCP Snooping Database informations.

ip dhcp snooping verify mac-address

```
ip dhcp snooping verify mac-address
```

```
no ip dhcp snooping verify mac-address
```

Description

Configures the switch to verify that the source MAC address in a DHCP packet matches the client hardware address.

Inserting **no** as a prefix for this command will disable DHCP Snooping mac-address verification.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate DHCP Snooping mac-address verification.

```
DmSwitch(config)#ip dhcp snooping verify mac-address
DmSwitch(config)#
```

You can verify that the DHCP Snooping mac-address verification was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>ip dhcp snooping</code>	Enables DHCP Snooping globally.
<code>ip dhcp snooping</code>	Enables DHCP Snooping at VLAN.
<code>ip dhcp snooping trust</code>	Configures port as trusted for DHCP Snooping.

ip dhcp snooping vlan

```
ip dhcp snooping vlan index binding ip-address mac-address mac-address { ethernet unit/port | port-channel portchannel } lease-time timer-value
```

```
no ip dhcp snooping vlan index binding ip-address
```

Description

Configures a DHCP Snooping Database entry based on VLAN, IP Address, MAC Address, unit/port and lease time value. This entry expires after lease time ends.

Inserting **no** as a prefix for this command will remove the entry.

Syntax

Parameter	Description
<i>index</i>	Specifies a VLAN index. (Range: 1-4094)
binding <i>ip-address</i>	Defines the ip address that will be stored at database.
mac-address <i>mac-address</i>	Defines the mac address that will be stored at database.
ethernet [<i>unit-number</i>] <i>port-number</i>	Specifies the ethernet unit/port number.
port-channel <i>portchannel</i>	Specifies the Port-channel interface number.
lease-time <i>timer-value</i>	Defines the time that the entry will expires.

Default

No entries configured.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command configures manually an entry in DHCP Snooping Database and it is used by DHCP Snooping feature.

Example

```
DmSwitch(config)#ip dhcp snooping vlan 10 binding 10.1.2.1 mac-address 11:22:33:44:55:66 ethernet 2/11 lease-t
DmSwitch(config)#
```

You can verify that the entry was added by entering the **show ip dhcp snooping database** privileged EXEC command.

Related Commands

Command	Description
show ip dhcp snooping database	Shows DHCP Snooping Database informations.

ip dns server

```
ip dns-server { primary-ip-address [ secondary-ip-address ] }
```

```
no ip dns-server
```

Description

Configures the DNS servers used by DmSwitch.

Inserting **no** as a prefix for this command will remove the specified DNS servers.

Syntax

Parameter	Description
<i>primary-ip-address</i>	Specifies the IP address of primary DNS servers.
<i>secondary-ip-address</i>	(Optional) Specifies the IP address of secondary DNS servers.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the IP address "10.1.1.1" for primary DNS server and "10.1.1.2" for secondary DNS server.

```
DmSwitch(config)#ip dns-server 10.1.1.1 10.1.1.2
DmSwitch(config)#
```


You can verify that the two DNS servers were configured by entering the **show ip dns-servers** privileged EXEC command.

Related Commands

Command	Description
ip address	Sets an IP address for the selected VLAN.
show ip	Shows the IP configuration.
show ip dns-servers	Shows the configured DNS servers.
show running-config	Shows the current operating configuration.

ip domain-name

```
ip domain-name { text }
```

```
no ip domain-name
```

Description

Configures the domain name for DmSwitch.

Inserting **no** as a prefix for this command will remove the domain name.

Syntax

Parameter	Description
<i>text</i>	Specifies the domain name to be configured.

Default

No default domain name is configured.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the domain name of the DmSwitch.

```
DmSwitch(config)#ip domain-name datacom.telematica
DmSwitch(config)#
```

You can verify that the domain name was configured by entering the **show ip domain-name** privileged EXEC command.

Related Commands

Command	Description
<code>ip address</code>	Sets an IP address for the selected VLAN.
<code>show ip</code>	Shows the IP configuration.
<code>show ip domain-name</code>	Shows the configured domain name.
<code>show running-config</code>	Shows the current operating configuration.

ip helper-address

ip helper-address *ip-address*

no ip helper-address *ip-address*

Description

Add an address to the list of DHCP servers global.

Inserting **no** as a prefix for this command will erase the address from the list.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the IP address to the list of DHCP servers global

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add the address 192.168.0.254 to the DHCP relay servers list.

```
DmSwitch(config)#ip helper-address 192.168.0.254
DmSwitch(config)#
```

You can verify that the address was added to the list by entering the **show ip dhcp** privileged EXEC command.

Related Commands

Command	Description
<code>ip dhcp relay</code>	Enables DHCP relay globally.
<code>ip dhcp relay</code>	Enables DHCP relay on the selected Vlan.
<code>ip dhcp relay information option</code>	Enables DHCP Agent Information Option (option 82).
<code>ip dhcp relay information trusted</code>	Mark a Vlan as a trusted interface.
<code>ip helper-address</code>	Add an address to the VLAN list of DHCP servers in VLAN.
<code>show ip dhcp relay</code>	Shows the DHCP relay settings.

ipv6 helper-address

```
ipv6 helper-address { all-dhcp-relay-and-servers | all-dhcp-servers  
| ipv6-address } vlan vid
```

```
no ipv6 helper-address { all-dhcp-relay-and-servers | all-dhcp-servers  
| ipv6-address }
```

Description

It adds unicast, pre-defined or user-defined multicast IPv6 address to the list of DHCPv6 servers global.

Inserting **no** as a prefix for this command will remove the address from the list.

Syntax

Parameter	Description
all-dhcp-relay-and-servers	It uses the predefined multicast IPv6 address FF02::1:2 to be added into DHCPv6 helper-address list.
all-dhcp-servers	It uses the predefined multicast IPv6 address FF05::1:3 to be added into DHCPv6 helper-address list.
<i>ipv6-address</i>	It specifies an unicast or multicast IPv6 address (user defined) to be added into DHCPv6 helper-address list.
vlan vid	It specifies a VLAN to be used when send requests.

Default

None helper-address configured.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add the multicast address FF00:6340::2 to the DHCPv6 servers list and use the VLAN 5 to send multicast requests.

```
DmSwitch(config)#ipv6 helper-address FF00:6340::2 vlan 5
DmSwitch(config)#
```

You can verify that the address was added to the list by entering the **show ipv6 dhcp relay** privileged EXEC command.

Related Commands

Command	Description
ipv6 dhcp relay	It enables the global DHCPv6 relay.
ipv6 helper-address	It adds unicast or multicast IPv6 address into the list of DHCPv6 servers global.
ipv6 dhcp relay	It enables the DHCPv6 relay agent on a VLAN.
show ipv6 dhcp relay	It shows the details about DHCPv6 relay configurations.

ip http

```
ip http { max-connections max-connections-number | server | port port-number |  
secure-server | secure-port port-number }
```

```
no ip http { max-connections | server | port | secure-server | secure-port }
```

Description

Configures the internal HTTP server for external access.

Inserting **no** as a prefix for this command will stop the HTTP server or reset binded ports to the default value.

It can also reset the maximum number of connections on the HTTP server to default value.

Syntax

Parameter	Description
max-connections <i>max-connections-number</i>	Specifies the maximum number of connections on HTTP server. (Range: 1-32)
server	Enables the internal HTTP server.
port <i>port-number</i>	Specifies a port number for access the HTTP server. (Range: 1-65535)
secure-server	Enables the internal secure HTTP server.
secure-port <i>port-number</i>	Specifies a port number for access the secure HTTP server. (Range: 1-65535)

Default

Max-connections: 8

Port: 80

Secure-port: 443

HTTP and secure HTTP are enabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the secure HTTP server.

```
DmSwitch(config)#ip http secure-server
DmSwitch(config)#
```

You can verify that the secure HTTP server was enabled by entering the **show ip http** privileged EXEC command.

This example shows how to change to 3000 the access port of HTTP server.

```
DmSwitch(config)#ip http port 3000
DmSwitch(config)#
```

You can verify that the port of HTTP server was changed by entering the **show ip http** privileged EXEC command.

Related Commands

Command	Description
management	Filters client IP address that tries to access internal servers.
show ip http	Shows the HTTP server information.
show management	Shows the management IP filters.
show running-config	Shows the current operating configuration.

ip igmp

```
ip igmp snooping [ ip ip-address querier | query-count query-count | query-interval  
query-interval | query-max-response-time query-time | router-port-expire-time  
router-time | last-member-query-interval last-member-query-interval | ssm-map  
group-ip-address/mask source-ip-address | version version-number | vlan parameters ]
```

```
no ip igmp snooping [ ip querier | query-count | query-interval  
| query-max-response-time | router-port-expire-time |  
last-member-query-interval | ssm-map [ group-ip-address/mask source-ip-address] |  
version | vlan ]
```

Description

Configures the IGMP snooping.

Inserting **no** as a prefix for this command will stop the IGMP snooping or reset parameters to the default value or delete the IGMP IP address.

Syntax

Parameter	Description
snooping	Enables the IGMP snooping.
ip ip-address	(Optional) Sets the IP address used by the switch when sending IGMP queries.
<i>group-ip-address/maks</i>	(Optional) Sets the IP address range of multicast group.
<i>source-ip-address</i>	(Optional) Sets the IP address of a multicast source.
querier	(Optional) Enables IGMP snooping to act as querier.
query-count query-count	(Optional) Sets the number of queries without response that the switch waits before removing the multicast entries from its forwarding table. (Range: 2-10)
query-interval query-interval	(Optional) Sets the time interval between sending queries. (Range: 60-125)
query-max-response-time query-time	(Optional) Sets the maximum response time that a host waits before replying with a membership report to a querier. (Range: 5-25)
router-port-expire-time router-time	(Optional) Sets the time interval that the switch waits for a query before removing the mrouter entry from its forwarding table. (Range: 300-500)
last-member-query-interval last-interval	(Optional) The last-member query interval is the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You can configure this interval to change the amount of time it takes a routing device to detect the loss of the last member of a group. (Range: 1-12)
ssm-map	(Optional) Source specific multicast mapping

Parameter	Description
version <i>version-number</i>	(Optional) Sets the IGMP version used by the switch. (Range: 1-3)
vlan <i>parameters</i>	(Optional) Enables the VLAN configuration. Click here to see the parameters description.

Default

Query-number: 2

Query-interval: 125 seconds

Query-time: 10 seconds

Router-time: 300 seconds

Last-interval: 1 second

Version-number: 2

IGMP snooping is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
12.2	This command was updated.
14.6	This command was updated with last-member-query-interval.

Usage Guidelines

In some cases where more than one switch is configured as querier on the network, the switch with the lowest IP address will be elected as querier. When the IGMP IP is not configured, the switch will use the first available IP from its IP interfaces. IGMP querier functions will not work without a source IP address.

Example

This example shows how to enable IGMP snooping to act as a querier.

```
DmSwitch(config)#ip igmp snooping querier
DmSwitch(config)#
```

You can verify that the IGMP snooping was enabled by entering the **show ip igmp snooping** privileged EXEC command.

This example shows how to change the IGMP version.

```
DmSwitch(config)#ip igmp snooping version 3
DmSwitch(config)#
```

You can verify that the IGMP version was changed by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping vlan	Configures static multicast entries in the mac address table.
show ip igmp snooping	Shows the IGMP snooping configuration.
show ip igmp snooping mroute	Shows the static entries in mac address table of the multicast routers.

ipv6 mld

```
ipv6 mld snooping [ ipv6 ipv6-address querier | query-count query-count  
| query-interval query-interval | query-max-response-time query-time |  
router-port-expire-time router-time | ssm-map group-ipv6-address/prefix-length  
source-ipv6-address | version version-number | vlan parameters ]
```

```
no ipv6 mld snooping [ ipv6 querier | query-count | query-interval  
| query-max-response-time | router-port-expire-time ssm-map [  
group-ipv6-address/prefix-length source-ipv6-address] | version | vlan ]
```

Description

Configures the MLD snooping.

Inserting **no** as a prefix for this command will stop the MLD snooping or reset parameters to the default value or delete the MLD IP address.

Syntax

Parameter	Description
snooping	Enables the MLD snooping.
ipv6 <i>ipv6-address</i>	(Optional) Sets the IP address used by the switch when sending MLD queries.
<i>group-ipv6-address/prefix-length</i>	(Optional) Sets the IP address range of multicast group.
<i>source-ip-address</i>	(Optional) Sets the IP address of a multicast source.
querier	(Optional) Enables MLD snooping to act as querier.
query-count <i>query-count</i>	(Optional) Sets the number of queries without response that the switch waits before removing the multicast entries from its forwarding table. (Range: 2-10)
query-interval <i>query-interval</i>	(Optional) Sets the time interval between sending queries. (Range: 60-125)
query-max-response-time <i>query-time</i>	(Optional) Sets the maximum response time that a host waits before replying with a membership report to a querier. (Range: 5-25)
router-port-expire-time <i>router-time</i>	(Optional) Sets the time interval that the switch waits for a query before removing the mrouter entry from its forwarding table. (Range: 300-500)
ssm-map	(Optional) Source specific multicast mapping
version <i>version-number</i>	(Optional) Sets the MLD version used by the switch. (Range: 1-3)
vlan <i>parameters</i>	(Optional) Enables the VLAN configuration. Click here to see the parameters description.

Default

Query-number: 2

Query-interval: 125 seconds

Query-time: 10 seconds

Router-time: 300 seconds

Version-number: 2

MLD snooping is disabled.

Command Modes

Global configuration.

Usage Guidelines

In some cases where more than one switch is configured as querier on the network, the switch with the lowest IP address will be elected as querier. When the MLD IP is not configured, the switch will use the first available IP from its IP interfaces. MLD querier functions will not work without a source IP address.

Example

This example shows how to enable MLD snooping to act as a querier.

```
DmSwitch(config)#ipv6 mld snooping querier
DmSwitch(config)#
```

You can verify that the MLD snooping was enabled by entering the **show ipv6 mld snooping** privileged EXEC command.

This example shows how to change the MLD version.

```
DmSwitch(config)#ipv6 mld snooping version 3
DmSwitch(config)#
```

You can verify that the MLD version was changed by entering the **show ipv6 mld snooping** privileged EXEC command.

Related Commands

Command	Description
ipv6 mld snooping vlan	Configures static multicast entries in the mac address table.
show ipv6 mld snooping	Shows the MLD snooping configuration.

Command

show ipv6 mld snooping mroute

Description

Shows the static entries in mac address table of the multicast routers.

ip igmp snooping vlan

```
ip igmp snooping vlan index { mroute | static ip-address } { ethernet [ unit-number/ ]  
port-number | port-channel port-channel-number }
```

```
no ip igmp snooping vlan index { mroute | static ip-address } { ethernet [ unit-number/ ]  
port-number | port-channel port-channel-number }
```

Description

Configures static multicast entries in the mac address table, indicating a port where there is connected a multicast router or a multicast group client.

Inserting **no** as a prefix for this command will delete a static multicast entry.

Syntax

Parameter	Description
<i>index</i>	Specifies a VLAN index. (Range: 1-4094)
mroute	Defines that the entry is connected statically to a multicast router.
static <i>ip-address</i>	Defines that the entry is for a multicast client of the specified multicast group IP address.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Specifies the ethernet unit/port number.
port-channel <i>port-channel-number</i>	Specifies the port-channel number.

Default

No static multicast entries.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

By configuring a static multicast IP entry on an port, the DmSwitch will always forward multicast traffic for this group on this port.

Example

This example shows how to add a static multicast entry in the mac address table, indicating the port where there is connected a multicast router.

```
DmSwitch(config)#ip igmp snooping vlan 1 mroute ethernet 1
DmSwitch(config)#
```

You can verify that the multicast entry was added by entering the **show ip igmp snooping mroute** privileged EXEC command.

Related Commands

Command	Description
ip igmp	Configures the IGMP snooping.
show ip igmp snooping	Shows the IGMP snooping configuration.
show ip igmp snooping mroute	Shows the static entries in mac address table of the multicast routers.

ipv6 mld snooping vlan

```
ipv6 mld snooping vlan index { mroute | static ipv6-address } { ethernet [ unit-number/  
] port-number | port-channel port-channel-number }
```

```
no ipv6 mld snooping vlan index { mroute | static ipv6-address } { ethernet [ unit-  
number/ ] port-number | port-channel port-channel-number }
```

Description

Configures static multicast entries in the mac address table, indicating a port where there is connected a multicast router or a multicast group client.

Inserting **no** as a prefix for this command will delete a static multicast entry.

Syntax

Parameter	Description
<i>index</i>	Specifies a VLAN index. (Range: 1-4094)
mroute	Defines that the entry is connected statically to a multicast router.
static <i>ipv6-address</i>	Defines that the entry is for a multicast client of the specified multicast group IP address.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Specifies the ethernet unit/port number.
port-channel <i>port-channel-number</i>	Specifies the port-channel number.

Default

No static multicast entries.

Command Modes

Global configuration.

Usage Guidelines

By configuring a static multicast IP entry on an port, the DmSwitch will always forward multicast traffic for this group on this port.

Example

This example shows how to adds a static multicast entry in the mac address table, indicating the port where there is connected a multicast router.

```
DmSwitch(config)#ipv6 mld snooping vlan 1 mroute ethernet 1  
DmSwitch(config)#
```

You can verify that the multicast entry was added by entering the **show ipv6 mld snooping mroute** privileged EXEC command.

Related Commands

Command	Description
show ipv6 mld snooping	Shows the MLD snooping configuration.
show ipv6 mld snooping mroute	Shows the static entries in mac address table of the multicast routers.

ip path-mtu-discovery

ip path-mtu-discovery

no ip path-mtu-discovery

Description

Enables Path MTU Discovery (PMTUD) on the router.

The **no** command removes the PMTUD configuration from the router.

Syntax

To enable PMTUD no additional parameter is needed.

Default

PMTUD is enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

This command enables Path MTU Discovery protocol on the router.

Example

This example shows how to disable PMTUD on the router.

```
DmSwitch(config)#no ip path-mtu-discovery
DmSwitch(config)#
```

You can verify PMTUD is disabled by entering the **show running-config** command. If enabled, it will not be shown.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ip pim

ip pim

no ip pim

Description

Enables global PIM (Protocol Independent Multicast) on the router.

The **no** command removes the global PIM configuration from the router.

Syntax

To enable global PIM no additional parameter is needed.

Default

Global PIM protocol is not enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command enables global PIM Multicast Routing Protocol on the router.

Example

This example shows how to enable global PIM on the router.

```
DmSwitch(config)#ip pim
DmSwitch(config)#
```

You can verify global PIM is enabled by entering the **show running-config** or the **show ip pim config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show ip pim config</code>	Shows global PIM configuration.
<code>show running-config</code>	Shows the current operating configuration.

ipv6 pim

ipv6 pim

no ipv6 pim

Description

Enables global PIM (Protocol Independent Multicast) on the router.

The **no** command removes the global PIM configuration from the router.

Syntax

To enable global PIM no additional parameter is needed.

Default

Global PIM protocol is not enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command enables global PIM Multicast Routing Protocol on the router.

Example

This example shows how to enable global PIM on the router.

```
DmSwitch(config)#ipv6 pim
DmSwitch(config)#
```

You can verify global PIM is enabled by entering the **show running-config** or the **show ipv6 pim config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show ipv6 pim config</code>	Shows global PIM configuration.
<code>show running-config</code>	Shows the current operating configuration.

ip pim bootstrap

ip pim bootstrap

no ip pim bootstrap

Description

Enables PIM Bootstrap feature.

The **no** command removes the PIM Bootstrap feature.

Syntax

To enable Bootstrap feature no additional parameter is needed. Additional commands are needed to set BSR (Bootstrap Router) Candidate and RP (Rendezvous Point) Candidate.

Default

PIM Bootstrap feature is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command enables PIM Bootstrap capabilities. With the Bootstrap candidates set, it originates Bootstrap messages used to elect a BSR and to disseminate RP information.

Example

This example shows how to enable PIM Bootstrap.

```
DmSwitch(config)#ip pim bootstrap
DmSwitch(config)#
```

You can verify the PIM Bootstrap configured by entering the **show running-config** or the **show ip pim config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip pim config</code>	Shows global PIM configuration.
<code>show running-config</code>	Shows the current operating configuration.

ipv6 pim bootstrap

```
ipv6 pim bootstrap
```

```
no ipv6 pim bootstrap
```

Description

Enables PIM Bootstrap feature.

The **no** command removes the PIM Bootstrap feature.

Syntax

To enable Bootstrap feature no additional parameter is needed. Additional commands are needed to set BSR (Bootstrap Router) Candidate and RP (Rendezvous Point) Candidate.

Default

PIM Bootstrap feature is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command enables PIM Bootstrap capabilities. With the Bootstrap candidates set, it originates Bootstrap messages used to elect a BSR and to disseminate RP information.

Example

This example shows how to enable PIM Bootstrap.

```
DmSwitch(config)#ipv6 pim bootstrap
DmSwitch(config)#
```

You can verify the PIM Bootstrap configured by entering the **show running-config** or the **show ipv6 pim config** privileged EXEC command.

Related Commands

Command	Description
<code>show ipv6 pim config</code>	Shows global PIM configuration.
<code>show running-config</code>	Shows the current operating configuration.

ip pim bootstrap bsr-candidate

```
ip pim bootstrap bsr-candidate vlan vlan-id [priority value]
```

```
no ip pim bootstrap bsr-candidate vlan vlan-id [priority]
```

Description

This command configures Bootstrap Router (BSR) candidate for Bootstrap feature.

The **no** command removes the PIM BSR-Candidate entry. Additionally with the **no** command, if **priority** is given on the end of the string, the priority is set to its default value

Syntax

Parameter	Description
vlan <i>vlan-id</i>	VLAN to announce as BSR-Candidate.
priority <i>value</i>	Election priority for the BSR-candidate. Higher value indicates higher priority. Range: 0-255.

Default

No BSR-Candidate is configured by default. When there is one set, the default value for the priority is 1.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command configures the respective vlan as a BSR-Candidate, which then can become the Bootstrap Router which will disseminate RP (Rendezvous Point) information on the domain.

Example

This example shows how to configure a BSR-Candidate.

```
DmSwitch(config)#ip pim bootstrap bsr-candidate vlan 420
DmSwitch(config)#
```

You can verify the BSR-Candidate configuration by entering the **show running-config**, **show ip pim config** or the **show ip pim bsr-candidate** privileged EXEC command.

Related Commands

Command	Description
show ip bsr-candidate	Shows PIM BSR-Candidate.
show ip pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ipv6 pim bootstrap bsr-candidate

```
ipv6 pim bootstrap bsr-candidate vlan vlan-id [priority value]
```

```
no ipv6 pim bootstrap bsr-candidate vlan vlan-id [priority]
```

Description

This command configures Bootstrap Router (BSR) candidate for Bootstrap feature.

The **no** command removes the PIM BSR-Candidate entry. Additionally with the **no** command, if **priority** is given on the end of the string, the priority is set to its default value

Syntax

Parameter	Description
vlan <i>vlan-id</i>	VLAN to announce as BSR-Candidate.
priority <i>value</i>	Election priority for the BSR-candidate. Higher value indicates higher priority. Range: 0-255.

Default

No BSR-Candidate is configured by default. When there is one set, the default value for the priority is 1.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command configures the respective vlan as a BSR-Candidate, which then can become the Bootstrap Router which will disseminate RP (Rendezvous Point) information on the domain.

Example

This example shows how to configure a BSR-Candidate.

```
DmSwitch(config)#ipv6 pim bootstrap bsr-candidate vlan 420
DmSwitch(config)#
```


You can verify the BSR-Candidate configuration by entering the **show running-config**, **show ipv6 pim config** or the **show ipv6 pim bsr-candidate** privileged EXEC command.

Related Commands

Command	Description
show ipv6 bsr-candidate	Shows PIM BSR-Candidate.
show ipv6 pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ip pim bootstrap rp-candidate

```
ip pim bootstrap rp-candidate vlan vlan-id [group-prefix ip-address/mask |  
priority value | holdtime seconds]
```

```
no ip pim bootstrap rp-candidate vlan vlan-id [group-prefix | priority |  
holdtime]
```

Description

This command configures RP (Rendezvous Point) Candidate for Bootstrap feature.

The **no** command removes the PIM RP-Candidate entry. Additionally with the **no** command, if **group-prefix** is given on the end of the string, the group-prefix is set to its default value. The same happens with **priority** and **holdtime**.

Syntax

Parameter	Description
vlan <i>vlan-id</i>	VLAN to announce as RP-Candidate.
group-prefix <i>ip-address/mask</i>	Group-prefix for the RP-Candidate.
priority <i>value</i>	Election priority for the RP-Candidate. Higher value indicates lower priority, with the value zero denoting the highest priority. Range: 0-255.
holdtime <i>seconds</i>	Holdtime for the RP-Candidate. The amount of time, in seconds, this RP-Candidate entry is valid. Range: 61-65535.

Default

No RP-Candidate is configured by default. When there is one set, the default value for the group-prefix is 224.0.0.0/4, for the priority is 192, and for the holdtime is 150.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command configures the respective VLAN as an RP-Candidate, which then can become the Rendezvous Point (RP) central router that receives all the traffic from the sources and forwards that traffic to the receivers.

Example

This example shows how to configure a RP-Candidate.

```
DmSwitch(config)#ip pim bootstrap rp-candidate vlan 420
DmSwitch(config)#
```

You can verify the RP-Candidate configuration by entering the **show running-config**, **show ip pim config** or the **show ip pim rp-candidate** privileged EXEC command.

Related Commands

Command	Description
show ip pim rp-candidate	Shows PIM RP-Candidates.
show ip pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ipv6 pim bootstrap rp-candidate

```
ipv6 pim bootstrap rp-candidate vlan vlan-id [group-prefix  
ipv6-address/prefix-length | priority value | holdtime seconds]
```

```
no ipv6 pim bootstrap rp-candidate vlan vlan-id [group-prefix | priority |  
holdtime]
```

Description

This command configures RP (Rendezvous Point) Candidate for Bootstrap feature.

The **no** command removes the PIM RP-Candidate entry. Additionally with the **no** command, if **group-prefix** is given on the end of the string, the group-prefix is set to its default value. The same happens with **priority** and **holdtime**.

Syntax

Parameter	Description
vlan <i>vlan-id</i>	VLAN to announce as RP-Candidate.
group-prefix <i>ipv6-address/prefix-length</i>	Group-prefix for the RP-Candidate.
priority <i>value</i>	Election priority for the RP-Candidate. Higher value indicates lower priority, with the value zero denoting the highest priority. Range: 0-255.
holdtime <i>seconds</i>	Holdtime for the RP-Candidate. The amount of time, in seconds, this RP-Candidate entry is valid. Range: 61-65535.

Default

No RP-Candidate is configured by default. When there is one set, the default value for the group-prefix is FF00::/8, for the priority is 192, and for the holdtime is 150.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command configures the respective VLAN as an RP-Candidate, which then can become the Rendezvous Point (RP) central router that receives all the traffic from the sources and forwards that traffic to the receivers.

Example

This example shows how to configure a RP-Candidate.

```
DmSwitch(config)#ipv6 pim bootstrap rp-candidate vlan 720
DmSwitch(config)#
```

You can verify the RP-Candidate configuration by entering the **show running-config**, **show ipv6 pim config** or the **show ipv6 pim rp-candidate** privileged EXEC command.

Related Commands

Command	Description
show ipv6 pim rp-candidate	Shows PIM RP-Candidates.
show ipv6 pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ip pim rp-address

```
ip pim rp-address IPaddress [group-prefix IPaddress/mask]
```

```
no ip pim rp-address IPaddress [group-prefix]
```

Description

Configures static RP (Rendezvous Point) address for PIM protocol.

The **no** command removes the static RP-address configuration. Additionally with the **no** command, if **group-prefix** is given on the end of the string, the group-prefix is set to its default value.

Syntax

Parameter	Description
<i>IPaddress</i>	The Rendezvous Point IP address.
group-prefix <i>IPaddress/mask</i>	Group Prefix address and netmask.

Default

PIM static RP-address is not configured by default. The Group Prefix default value for an RP-address configured without **group-prefix** is 224.0.0.0/4.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command configures static RP-address for PIM protocol. The RP is the root for the shared tree. It receives multicast traffic from the source hosts and forwards the packets to all the members of the group through a common tree.

Example

This example shows how to configure a static RP-address.

```
DmSwitch(config)#ip pim rp-address 172.16.2.151
```

```
DmSwitch(config)#
```

You can verify the static RP-address configured by entering the **show running-config** or the **show ip pim rps** privileged EXEC command.

Related Commands

Command	Description
show ip pim rps	Shows the configured Rendezvous Points and their parameters.
show running-config	Shows the current operating configuration.

ipv6 pim rp-address

```
ipv6 pim rp-address ipv6-address [group-prefix ipv6-address/prefix-length]
```

```
no ipv6 pim rp-address ipv6-address [group-prefix]
```

Description

Configures static RP (Rendezvous Point) address for IPv6 PIM protocol.

The **no** command removes the static RP-address configuration. Additionally with the **no** command, if **group-prefix** is given on the end of the string, the group-prefix is set to its default value.

Syntax

Parameter	Description
<i>ipv6-address</i>	The Rendezvous Point IPv6 address.
group-prefix <i>ipv6-address/prefix-length</i>	Group Prefix address and netmask.

Default

PIM static RP-address is not configured by default. The Group Prefix default value for an RP-address configured without **group-prefix** is FF00::/8.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command configures static RP-address for PIM protocol. The RP is the root for the shared tree. It receives multicast traffic from the source hosts and forwards the packets to all the members of the group through a common tree.

Example

This example shows how to configure a static RP-address.

```
DmSwitch(config)#ipv6 pim rp-address 2001:DB8::1
```



```
DmSwitch(config)#
```

You can verify the static RP-address configured by entering the **show running-config** or the **show ipv6 pim rps** privileged EXEC command.

Related Commands

Command	Description
show ipv6 pim rps	Shows the configured Rendezvous Points and their parameters.
show running-config	Shows the current operating configuration.

ip pim spt-switch

```
ip pim spt-switch
```

```
no ip pim spt-switch
```

Description

Sets immediate Shortest-Path Tree (SPT) switchover.

The **no** command removes the immediate SPT switchover.

Syntax

No parameter accepted.

Default

When global PIM is enabled, SPT-switch is also enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command enables SPT-switch, which allows switching to the shortest path to deliver the multicast traffic to the group members.

Example

This example shows how to enable SPT-switch.

```
DmSwitch(config)#ip pim spt-switch
DmSwitch(config)#
```

You can verify PIM SPT-switch configured by entering the **show running-config** or the **show ip pim config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip pim config</code>	Shows global PIM configuration.
<code>show running-config</code>	Shows the current operating configuration.

ipv6 pim spt-switch

```
ipv6 pim spt-switch
```

```
no ipv6 pim spt-switch
```

Description

Sets immediate Shortest-Path Tree (SPT) switchover.

The **no** command removes the immediate SPT switchover.

Syntax

No parameter accepted.

Default

When global PIM is enabled, SPT-switch is also enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command enables SPT-switch, which allows switching to the shortest path to deliver the multicast traffic to the group members.

Example

This example shows how to enable SPT-switch.

```
DmSwitch(config)#ipv6 pim spt-switch
DmSwitch(config)#
```

You can verify PIM SPT-switch configured by entering the **show running-config** or the **show ipv6 pim config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ipv6 nd ra

`ipv6 nd ra`

`no ipv6 nd ra`

Description

Enables Router Advertisement protocol on the router.

The **no** command removes the Router Advertisement protocol configuration from the router.

Syntax

To enable Router Advertisement protocol no additional parameter is needed.

Default

Router Advertisement protocol is not enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command enables Router Advertisement protocol on the router.

Example

This example shows how to enable Router Advertisement protocol on the router.

```
DmSwitch(config)#ipv6 nd ra
DmSwitch(config)#
```

You can verify if Router Advertisement protocol is enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>ipv6 nd ra</code>	Configures Router Advertisement parameters.
<code>show running-config</code>	Shows the current operating configuration.

ip prefix-list

```
ip prefix-list name seq seq-number { permit | deny } ipaddress/mask [ ge ge-length ] [ le le-length ] [ labeled-prefix ]
```

```
no ip prefix-list name seq seq-number { permit | deny } ipaddress/mask [ ge ge-length ] [ le le-length ] [ labeled-prefix ]
```

Description

Configure a prefix list.

Inserting **no** as a prefix for this command will erase prefix list.

Syntax

Parameter	Description
<i>name</i>	Specifies a name of a prefix list.
deny	Specifies packets to reject of a prefix list.
permit	Specifies packets to forward of a prefix list.
seq seq-number	Specifies a sequence number of an entry. (Range: 1-65535)
<i>ipaddress/mask</i>	Specifies a IP prefix.
ge ge-length	(Optional) Specifies a matching prefix mask greater or equal than the given value. Range: 0-32.
le le-length	(Optional) Specifies a matching prefix mask less or equal than the given value. Range: 0-32.
labeled-prefix <small>[1] [3] [5]</small>	(Optional) Specifies an IPv4 labeled (AFI 1, SAFI 4) prefix. Without this parameter prefixes are considered of IPv4 unicast (AFI 1, SAFI 1) type.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
5.0	This command was introduced.
12.2	The labeled-prefix parameter was added.

Usage Guidelines

The **ge** (greater or equal) and **le** (less or equal) parameters allow the range of the prefix length to be matched on to be varied. If only the **ge** attribute is specified the range is assumed to be from *ge-length* value to the address length of the family (32 for IPv4). If only the **le** attribute is specified, it matches from *mask* to *le-length* value. A specified **ge** and/or **le** must satisfy the following condition: $mask \leq ge-length \leq le-length \leq \text{address length of family}$.

The **labeled-prefix** allows the matching of IPv4 labeled (AFI 1, SAFI 4) prefixes. Without this parameter prefixes are considered of IPv4 unicast (AFI 1, SAFI 1) type.

Example

This example shows how to insert a ip address in list.

```
DmSwitch(config)#ip prefix-list name permit 192.168.1.1/24
DmSwitch(config)#
```

You can verify that the address was added to the list by entering the **show ip prefix-list** privileged EXEC command.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.
show ip prefix-list	Shows configured prefix-lists.

ip route

```
ip route [ vrf vrf-name ] destination-ip-address/mask { forwarding-ip-address | black-hole } [
bfd { desired | required } ] [ distance value ] [ remark-text ]
```

```
no ip route { all | [ vrf vrf-name ] destination-ip-address/mask { forwarding-ip-address |
black-hole } }
```

Description

Adds a static route to the routing table. To add static routes for a VPN routing/forwarding instance (VRF), use the **vrf** option.

Inserting **no** as a prefix for this command will remove the specified static route.

Syntax

Parameter	Description
<code>all</code>	Specifies all route entries.
<code>vrf vrf-name</code>	(Optional) Name of the VPN routing/forwarding instance (VRF) for the static route.
<code>destination-ip-address/mask</code>	Specifies the destination network.
<code>forwarding-ip-address</code>	Specifies the gateway to reach the destination network.
<code>black-hole</code>	Specifies that the traffic to destination network should be silently discarded.
<code>bfd desired</code>	(Optional) Configures BFD support for this static route. The route will be added to the routing table even if the BFD session never goes up.
<code>bfd required</code>	(Optional) Configures BFD support for this static route. The route will be added to the routing table only if the BFD session goes up.
<code>distance value</code>	(Optional) Specifies an administrative distance for the route. (Range: 1-255)
<code>remark-text</code>	(Optional) Specifies a text description remark for the route.

Default

Default value for option **distance** is 1.

BFD support is disabled by default.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
10.0	Option vrf was added.
12.2	Option black-hole was added.
12.4	Changed range and default value for option distance .
14.6	Options bfd desired and bfd required were added.

Usage Guidelines

Use the mask /32 to indicate a host.

Regarding the BFD related parameters, **bfd desired** means that the route will be added to routing table even if the BFD session never goes to the Up state, and **bfd required** means that the route will be added to routing table only if the BFD session goes to the Up state. However, the difference in behavior for these parameters exists only for the first time the session goes to the Up state. If the session goes to the Down state once, for both configurations, the route will be removed from the routing table and will only be added again if the BFD session returns to the Up state.

Example

This example shows how to establish a static route to the network "10.2.1.0/24" through gateway "10.1.1.1".

```
DmSwitch(config)#ip route 10.2.1.0/24 10.1.1.1
DmSwitch(config)#
```

This example shows how to discard traffic sent to the network "10.2.1.0/24".

```
DmSwitch(config)#ip route 10.2.1.0/24 black-hole
DmSwitch(config)#
```

This example shows how to configure BFD support for a static route.

```
DmSwitch(config)#ip route 10.2.1.0/24 10.1.1.1 bfd required
DmSwitch(config)#
```

You can verify that the static route was added by entering the **show ip route** privileged EXEC command.

Related Commands

Command	Description
<code>ip routing</code>	Enables the IP routing.
<code>show ip route</code>	Shows the IP routing table.
<code>show ip routing</code>	Shows the routing status.
<code>ip vrf</code>	Enables the VRF configuration mode.
<code>show ip route vrf</code>	Shows the RIB of the specified VRF.

ip route pbr

```
ip route pbr seq sequence
```

```
no ip route pbr seq sequence
```

```
no ip route pbr all
```

Description

Routers normally forward traffic to destination addresses installed in their routing table. *Policy Based Routing* (PBR) creates policies for L3 that lead traffic through different paths based on source and/or destination addresses.

Rules for PBR can be set in sequence entry configuration mode matching source or destination address and thereafter applying PBR to the selected interfaces.

The PBR installation on HW whenever configured as 'next-hop' action will occur only after next hop resolution.

Inserting **no** for this command will remove this configuration.

Syntax

Parameter	Description
<i>sequence</i>	IP Route PBR sequence number. (Range:1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

By using the **ip route pbr** command it is possible to create a new PBR sequence.

The sequence number determines the entries priority evaluation. The lowest sequence value has the most priority.

After entering in this mode more options will be available for rules configuration.

Example

This example shows how to create a new PBR sequence into IP Route PBR configuration mode.

```
DmSwitch(config)#ip route pbr seq 10
DmSwitch(config-ip-route-pbr)#
```

To verify the PBR configuration use **show this** command.

Related Commands

Command	Description
action	Set action rule for PBR sequence.
description	Set description for PBR sequence.
match dest-ip	Set destination IP address for PBR sequence.
match src-interface	Set source interface for PBR sequence.
match src-ip	Set source IP address for PBR sequence.
show ip route pbr	Shows the PBR entries.

ipv6 route

```
ipv6 route destination-ipv6-address/prefix { forwarding-ipv6-address | black-hole | ip-tunnel ip-tunnel id } [ bfd { desired | required } ] [ distance value ] [ vlan value ] [ remark-text ]
```

```
no ipv6 route { all | destination-ipv6-address/prefix { forwarding-ipv6-address | black-hole | ip-tunnel ip-tunnel id } }
```

Description

Adds an IPv6 static route to the routing table.

Inserting **no** as a prefix for this command will remove the specified static route.

Syntax

Parameter	Description
<i>all</i>	Specifies all route entries.
<i>destination-ipv6-address/prefix</i>	Specifies the destination network.
<i>forwarding-ipv6-address</i>	Specifies the gateway to reach the destination network.
<i>black-hole</i>	Specifies that the traffic to destination network should be silently discarded.
<i>ip-tunnel ip-tunnel id</i>	Specifies the IP tunnel to reach the destination network.
<i>bfd desired</i>	(Optional) Configures BFD support for this static route. The route will be added to the routing table even if the BFD session never goes up.
<i>bfd required</i>	(Optional) Configures BFD support for this static route. The route will be added to the routing table only if the BFD session goes up.
<i>distance value</i>	(Optional) Specifies an administrative distance for the route. (Range: 0-255)
<i>vlan value</i>	(Optional) Specifies a VLAN interface for outbound route. (Range: 1-4094)
<i>remark-text</i>	(Optional) Specifies a text description remark for the route.

Default

No default is defined.

BFD support is disabled by default.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.
12.2	Option black-hole was added.
13.0	Option ip-tunnel was added.
14.6	Options bfd desired and bfd required were added.

Usage Guidelines

Use the mask /128 to indicate a host.

Regarding the BFD related parameters, **bfd desired** means that the route will be added to routing table even if the BFD session never goes to the Up state, and **bfd required** means that the route will be added to routing table only if the BFD session goes to the Up state. However, the difference in behavior for these parameters exists only for the first time the session goes to the Up state. If the session goes to the Down state once, for both configurations, the route will be removed from the routing table and will only be added again if the BFD session returns to the Up state.

Example

This example shows how to establish a static route to the network "2001:DB8::/64" through gateway "2002:1234::1".

```
DmSwitch(config)#ipv6 route 2001:DB8::/64 2002:1234::1
DmSwitch(config)#
```

This example shows how to discard traffic sent to the network "2001:DB8::/64".

```
DmSwitch(config)#ipv6 route 2001:DB8::/64 black-hole
DmSwitch(config)#
```

This example shows how to establish a static route to the network "2011:DB8::/64" through *ip-tunnel 5*.

```
DmSwitch(config)#ipv6 route 2011:DB8::/64 ip-tunnel 5
DmSwitch(config)#
```

This example shows how to configure BFD support for a static route.

```
DmSwitch(config)#ipv6 route 2001:DB8::/64 2002:1234::1 bfd required
DmSwitch(config)#
```


You can verify that the static route was added by entering the **show ipv6 route** privileged EXEC command.

Related Commands

Command	Description
ip routing	Enables the IP routing.
show ipv6 route	Shows the IPv6 routing table.
show ip routing	Shows the routing status.

ip routing

```
ip routing [ multipath ]
```

```
no ip routing [ multipath ]
```

Description

Enables the IP routing.

Inserting **no** as a prefix for this command will disable IP routing.

Syntax

Parameter	Description
multipath	(Optional) Enable multipath.

Default

The command **ip routing** and option **multipath** are disable.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
7.6	The option multipath was introduced.

Usage Guidelines

Entering this command without parameters, only IP routing will be enabled.

Example

This example shows how to enable the IP routing.

```
DmSwitch(config)#ip routing
```

```
DmSwitch(config)#
```

You can verify that the IP routing was enabled by entering the **show ip routing** privileged EXEC command.

Related Commands

Command	Description
ip route	Adds a static route to the routing table.
show ip route	Shows the IP routing table.
show ip routing	Shows the routing status.
show running-config	Shows the current operating configuration.

ip snmp-server

```
ip snmp-server [ agent-address interface { loopback number | mgmt-eth | vlan
number } { ipv4 | ipv6 } | community text [ ro | rw ] | contact text | host ip-address {
informs [ retries number | timeout number ] | source-iface [ loopback number | vlan
number | mgmt-eth ] | version { 1 text | 2c text | 3 text [ md5 text | sha text ] [ aes text | des text ] }
} | location text | traps [ parameters ] | user text { ro | rw } { md5 text | sha text [ encrypted
] } [ aes text | des text [ encrypted ] ] ]
```

```
no ip snmp-server [ agent-address interface { loopback number | mgmt-eth |
vlan number } { ipv4 | ipv6 } | community text | contact | host ip-address { informs |
source-iface } | location | traps [ parameters ] | user text ]
```

Description

Configures the internal SNMP server.

Inserting **no** as a prefix for this command will stop SNMP server or remove the specified configuration.

Syntax

Parameter	Description
agent-address interface	(Optional) Specifies a listening address for the agent
community text	(Optional) Creates a new community with the specified name
rw	Specifies that the access is read and write
ro	Specifies that the access is read only
contact text	(Optional) Sets the DmSwitch's contact name. Is accepted spaces for the variable <i>text</i>
host ip-address	(Optional) Sets the IP address of a manager device. It will receive the traps of a specific community sent by DmSwitch
source-iface	Specifies the SNMP source interface
informs	Changes SNMP HOST behavior to use INFORM PDUs, instead of TRAPs.
retries	How many retries when an INFORM PDU delivery fails. (Default 3. Range: 2-20)
timeout	Number of seconds to wait for an INFORM PDU response. (Default 15. Range: 1-65535)
vlan number	Select VLAN interface. (Range: 1-4094)
loopback number	Select loopback interface. (Range: 0-7)
mgmt-eth	Select management interface as source address.
ipv4	Select the primary IPv4 address of give interface.
ipv6	Select the primary IPv6 address of give interface.
version	Specifies a SNMP version
1 text	Sets the SNMP version 1
2c text	Sets the SNMP version 2c

Parameter	Description
3 <i>text</i>	Sets the SNMP version 3
location <i>location</i>	(Optional) Sets the DmSwitch's location. It accepts spaces
user <i>text</i>	(Optional) Creates a new user with the specified name
md5 <i>text</i>	Uses MD5 algorithm for the user authentication
sha <i>text</i>	Uses SHA algorithm for the user authentication
aes <i>text</i>	(Optional) Uses AES algorithm for the data transmission privacy
des <i>text</i>	(Optional) Uses DES algorithm for the data transmission privacy
encrypted	Specify an encrypted password.
traps <i>parameters</i>	Disables sending of SNMP traps. Click here to see the parameters description.

Default

SNMP server is enabled.

Community read-only "public".

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
6.6	The option source-interface was introduced.
11.0.4	The option agent-address was introduced.
12.0	Command that undoes the option source-interface was introduced.
12.2	The option ipv4 and ipv6 on agent-address was introduced.
13.0	The option ip-address on agent-address accept IPv6 address.
14.4	The option encrypted was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the manager device for the community "management" using a SNMP version 2c.

```
DmSwitch(config)#ip snmp-server host 10.1.1.10 version 2c management
DmSwitch(config)#
```

You can verify that the manager device was set by entering the **show ip snmp-server** privileged EXEC command.

This example shows how to create a new user called "manager". It has read and write access using the algorithms MD5 and AES for authentication and privacy, respectively.

```
DmSwitch(config)#ip snmp-server user manager rw md5 auth_pswd aes priv_pswd
DmSwitch(config)#
```

You can verify that the user was created by entering the **show running-config** privileged EXEC command.

The **contact** and **location** configurations can be verified by entering the **show system** command.

Related Commands

Command	Description
ip snmp-server trap	Enables sending of SNMP traps.
management	Filters client IP address that tries to access internal servers.
show ip snmp-server	Shows the SNMP server information.
show management	Shows the management IP filters.
show running-config	Shows the current operating configuration.
show system	Shows system information.

Notes

[1] - Parameter not available for Switches from DmSwitch 3000 Family.

ip snmp-server traps

```
ip snmp-server traps [ alarm-status-change | authentication |
bpdu-protect-limit-reached | bpdu-protect-block-time-expired |
cesop-bundle-local | cesop-bundle-next-hop | cesop-bundle-pkt-mismatch |
cesop-bundle-remote | cesop-bundle-tdm-local | cesop-bundle-tdm-remote
| cesop-clock-link-quality | cesop-clock-source | cesop-tdm-link |
cesop-tdm-remote | cesop-tdm-cas | cesop-tdm-crc | cfm | check-mpu-nsf-id |
cold-warm-start | config-change | config-save | core-dump | cpu-usage |
duplicated-ip | eaps-status-change | erps-status-change | evc-status-change
| fan-fuse-change | fan-status-change | fans-board-presence |
forbidden-access | fuse-status-change | high-memory-usage-detected
| high-memory-usage-no-more-detected | high-temperature-detected
| high-temperature-no-more-detected | link-flap-detected |
link-flap-no-more-detected | link-up-down | lldp-remote-changed
| lldp-remote-changed-global | lldp-med-remote-changed |
lldp-med-remote-changed-global | login-fail | login-success |
loopback-detected | loopback-no-more-detected | l3-route-table-full |
mac-move-detected | new-bootloader-version | non-homologated-transceiver
| oam-critical-event-detected | oam-critical-event-recovered
| oam-dying-gasp-received | oam-unidir-link-detected |
oam-unidir-link-recovered | poe-overcurrent | poe-power-restriction |
port-security-violation | power-status-change | remote-device-config-fail |
remote-device-config-forced | remote-device-loss | remote-device-ready |
stack-attach | stack-detach | standby-mpu-presence | status-ldp | status-rsvp
| storm-control-broadcast | storm-control-multicast | transceiver-presence |
traps-lost ]
```

```
no ip snmp-server traps [ alarm-status-change | authentication |
bpdu-protect-limit-reached | bpdu-protect-block-time-expired |
cesop-bundle-local | cesop-bundle-next-hop | cesop-bundle-pkt-mismatch |
cesop-bundle-remote | cesop-bundle-tdm-local | cesop-bundle-tdm-remote
| cesop-clock-link-quality | cesop-clock-source | cesop-tdm-link |
cesop-tdm-remote | cesop-tdm-cas | cesop-tdm-crc | cfm | check-mpu-nsf-id |
cold-warm-start | config-change | config-save | core-dump | cpu-usage |
duplicated-ip | eaps-status-change | erps-status-change | evc-status-change
| fan-fuse-change | fan-status-change | fans-board-presence |
forbidden-access | fuse-status-change | high-memory-usage-detected
| high-memory-usage-no-more-detected | high-temperature-detected
| high-temperature-no-more-detected | link-flap-detected |
link-flap-no-more-detected | link-up-down | lldp-remote-changed
| lldp-remote-changed-global | lldp-med-remote-changed |
lldp-med-remote-changed-global | login-fail | login-success |
loopback-detected | loopback-no-more-detected | l3-route-table-full |
mac-move-detected | new-bootloader-version | non-homologated-transceiver
| oam-critical-event-detected | oam-critical-event-recovered
```

```
| oam-dying-gasp-received | oam-unidir-link-detected |
oam-unidir-link-recovered | poe-overcurrent | poe-power-restriction |
port-security-violation | power-status-change | remote-device-config-fail |
remote-device-config-forced | remote-device-loss | remote-device-ready |
stack-attach | stack-detach | standby-mpu-presence | status-ldp | status-rsvp
| storm-control-broadcast | storm-control-multicast | transceiver-presence |
traps-lost ]
```

Description

Enables the sending of SNMP traps.

Inserting **no** as a prefix for this command will disable all or the specified SNMP trap.

Syntax

Parameter	Description
alarm-status-change	(Optional) Issues alarm-status-change traps.
authentication	(Optional) Issues authentication failure traps.
bpdu-protect-limit-reached	(Optional) Issues bpdu-protect-limit-reached traps.
bpdu-protect-block-time-expired	(Optional) Issues bpdu-protect-block-time-expired traps.
cesop-bundle-local	(Optional) Issues cesop local bundle status change traps.
cesop-bundle-next-hop	(Optional) Issues cesop next hop status change traps.
cesop-bundle-pkt-mismatch	(Optional) Issues cesop packet size mismatch presence traps.
cesop-bundle-remote	(Optional) Issues cesop remote bundle status change traps.
cesop-bundle-tdm-local	(Optional) Issues cesop TDM Interface status change in local bundle traps.
cesop-bundle-tdm-remote	(Optional) Issues cesop TDM Interface status change in remote bundle traps.
cesop-clock-link-quality	(Optional) Issues cesop adaptive clock source link quality traps.
cesop-clock-source	(Optional) Issues cesop clock source traps traps.
cesop-tdm-link	(Optional) Issues cesop TDM Interface link status change traps.
cesop-tdm-remote	(Optional) Issues cesop remote TDM Interface status change traps.
cesop-tdm-cas	(Optional) Issues cesop LOM (loss of multiframe) presence in TDM Interface traps.
cesop-tdm-crc	(Optional) Issues cesop TDM CRC status change traps.
cfm	(Optional) Issues connectivity fault management traps.
check-mpu-nsf-id	(Optional) Issues active and standby MPU NSF-ID differs traps.
cold-warm-start	(Optional) Issues cold-start and warm-start traps.
config-change	(Optional) Issues config-change traps.
config-save	(Optional) Issues config-save traps.

Parameter	Description
core-dump	(Optional) Issues core dump generated traps.
cpu-usage	(Optional) Issues overload CPU usage traps.
duplicated-ip	(Optional) Issues duplicated-ip traps.
eaps-status-change	(Optional) Issues eaps-status-change traps.
erps-status-change	(Optional) Issues erps-status-change traps.
evc-status-change	(Optional) Issues evc-status-change traps.
fan-fuse-change	(Optional) Issues fan board fuse status change traps.
fan-status-change	(Optional) Issues fan-status-change traps.
fans-board-presence	(Optional) Issues fan board presence traps.
forbidden-access	(Optional) Issues forbidden-access traps.
fuse-status-change	(Optional) Issues fuse status change traps.
high-memory-usage-detected	(Optional) Issues low memory resources traps.
high-memory-usage-no-more-detected	(Optional) Issues normal memory resources traps.
high-temperature-detected	(Optional) Issues high temperature condition traps.
high-temperature-no-more-detected	(Optional) Issues normal temperature condition traps.
link-flap-detected	(Optional) Issues link-flap-detected traps.
link-flap-no-more-detected	(Optional) Issues link-flap-no-more-detected traps.
link-up-down	(Optional) Issues link-up or link-down traps.
lldp-remote-changed	(Optional) Issues trap for changes in LLDP remote table of an interface.
lldp-remote-changed-global	(Optional) Issues trap for changes in LLDP remote tables.
lldp-med-remote-changed	(Optional) Issues trap for changes in LLDP-MED remote table of an interface.
lldp-med-remote-changed-global	(Optional) Issues trap for changes in LLDP-MED remote tables.
login-fail	(Optional) Issues login-fail traps.
login-success	(Optional) Issues login-success traps.
loopback-detected	(Optional) Issues loopback-detected traps.
loopback-no-more-detected	(Optional) Issues loopback-no-more-detected traps.
l3-route-table-full	(Optional) Issues routing table is full traps.
mac-move-detected	(Optional) Issues mac move detection traps.
new-bootloader-version	(Optional) Issues new bootloader version traps.
non-homologated-transceiver	(Optional) Issues non-homologated transceiver detection traps.
oam-critical-event-detected	(Optional) Issues oam critical event detection traps.
oam-critical-event-recovered	(Optional) Issues oam critical event recovery traps.
oam-dying-gasp-received	(Optional) Issues oam dying gasp received traps.
oam-unidir-link-detected	(Optional) Issues oam unidirectional link detection traps.
oam-unidir-link-recovered	(Optional) Issues oam unidirectional link recovery traps.
poe-overcurrent	(Optional) Issues PoE overcurrent traps.
poe-power-restriction	(Optional) Issues PoE power restriction traps.
port-security-violation	(Optional) Issues port-security violation traps.
power-status-change	(Optional) Issues power-status-change traps.
stack-attach	(Optional) Issues stack-attach traps.

Parameter	Description
stack-detach	(Optional) Issues stack-detach traps.
standby-mpu-presence	(Optional) Issues standby-mpu insertion/removal traps.
remote-device-config-fail	(Optional) Issues remote device configuration failure traps.
remote-device-config-forced	(Optional) Issues remote device configuration force traps.
remote-device-loss	(Optional) Issues remove device management loss traps.
remote-device-ready	(Optional) Issues remote device management availability traps.
status-ldp	(Optional) Issues ldp status change traps.
status-rsvp	(Optional) Issues rsvp status change traps.
storm-control-broadcast	(Optional) Issues storm-control alarm for broadcast packets traps.
storm-control-multicast	(Optional) Issues storm-control alarm for multicast packets traps.
transceiver-presence	(Optional) Issues transceivers insertion/removal traps.
traps-lost	(Optional) Issues traps-lost traps.

Default

The sending of all SNMP traps are enabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	New traps: critical event, link flap and unidirectional link. The "loopback-on-port" trap has changed its name.
12.0	New traps: bpdu-protect-limit-reached and bpdu-protect-block-time-expired.
13.0	New traps: lldp-med-remote-changed and lldp-med-remote-changed-global.
12.2	New traps: evc-status-change.
13.0	New traps: erps-status-change, status-ldp and status-rsvp. Also, the description of several traps was updated.

Usage Guidelines

Not available.

Example

This example shows how to enable the DmSwitch to send both cold-start and warm-start SNMP traps.

```
DmSwitch(config)#ip snmp-server traps cold-warm-start
DmSwitch(config)#
```

You can verify that the sending was enabled by entering the **show running-config** privileged EXEC command. As default, all traps are enable and only the disable traps are shown by this command. Then, if you do not see a trap that was enabled, the command was completed successfully.

Related Commands

Command	Description
ip snmp-server	Configures the internal SNMP server.
show ip snmp-server	Shows the SNMP server information.
show running-config	Shows the current operating configuration.

ip ssh

```
ip ssh { max-connections max-connections-number | server [ legacy-support ]  
timeout seconds | source-iface [ vlan number | loopback number | mgmt-eth ] }
```

```
ip ssh { host-key { generate [ dsa | rsa ] | clear [ dsa | rsa ] } }
```

```
no ip ssh { max-connections | server | timeout | source-iface }
```

Description

Configures the internal SSH server for external access.

Inserting **no** as a prefix for this command will stop the SSH server or reset the specified parameter to the default value.

Syntax

Parameter	Description
max-connections <i>max-connections-number</i>	Specifies the maximum number of connections on SSH server. (Range: 1-16)
server	Enables the internal SSH server.
legacy-support	(Optional) Enables the internal SSH server in Legacy mode. This mode is useful for enabling connections by older SSH clients.
timeout <i>seconds</i>	Defines the amount of time that the SSH server wait a response from a client during the authentication. (Range: 0-600)
host-key	Configures the host key pair (public and private)
generate	Generates the specified host key pair
dsa	(Optional) Specifies the DSA key for SSH version 2 with 1024 bits.
rsa	(Optional) Specifies the RSA key for SSH version 2 with 2048 bits.
clear	Clears the specified host keys from memory
source-iface	Specify SSH source interface.
vlan <i>number</i>	Select VLAN interface. (Range: 1-4094)
loopback <i>number</i>	Select loopback interface. (Range: 0-7)
mgmt-eth	Select management interface.

Default

Max-connections: 8 connections

Timeout: 120 seconds

SSH server is disabled.

SSH source-iface is disabled.

SSH server legacy-support is enabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
11.2	Maximum number of sessions was changed from 32 to 16.
11.6	The source-iface option was added.
15.0	OpenSSH updated to version 7.4p1.
15.0	RSA key size increased to 2048.
15.0	RSA1 key type is no longer supported.
15.0	The server-key option was removed.
15.0	The legacy-support option was added.
15.0	DSA and RSA fingerprint algorithm changed from MD5 to SHA256 and format from hexadecimal to Base64.

Usage Guidelines

The host-key pair must be generated in order to enable SSH.

Example

This example shows how to generate the RSA host key pair for SSH and how to enable the SSH server.

```
DmSwitch(config)#ip ssh host-key generate rsa
Generating dsa keys...
Fingerprint: SHA256:X2SpI5f1VvFN0DV3plwaaMBVIawB6seQHzc4u0+l0bo
DmSwitch(config)#ip ssh server
DmSwitch(config)#
```

You can verify that the key pair was generated by entering the **show ip ssh** privileged EXEC command.

Related Commands

Command	Description
management	Filters client IP address that tries to access internal servers.

Command	Description
<code>show ip ssh</code>	Shows the SSH server information.
<code>show management</code>	Shows the management IP filters.
<code>show running-config</code>	Shows the current operating configuration.
<code>show system</code>	Shows system information.
<code>terminal timeout</code>	Sets an idle timeout for terminal.

ipv6 ssh

```
ipv6 ssh { max-connections max-connections-number }
```

```
no ipv6 ssh { max-connections }
```

Description

Configures SSH maximum number of IPv6 connections.

Inserting **no** as a prefix for this command will reset the specified parameter to the default value.

Syntax

Parameter	Description
max-connections <i>max-connections-number</i>	Specifies the maximum number of IPv6 connections on SSH server. (Range: 1-32)

Default

Max-connections: 8 connections

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set a maximum number of SSH IPv6 connections.

```
DmSwitch(config)#ipv6 ssh max-connections 5
DmSwitch(config)#
```

You can verify that the maximum number of SSH connections was changed by entering the **show ip ssh** privileged EXEC command.

Related Commands

Command	Description
<code>management</code>	Filters client IP address that tries to access internal servers.
<code>show ip ssh</code>	Shows the SSH server information.
<code>show management</code>	Shows the management IP filters.
<code>show running-config</code>	Shows the current operating configuration.

ip telnet

```
ip telnet { max-connections max-connections-number | server | source-iface [ vlan number | loopback number | mgmt-eth ] }
```

```
no ip telnet { max-connections | server | source-iface [ vlan number | loopback number | mgmt-eth ] }
```

Description

Configures the internal Telnet server for external access.

Inserting **no** as a prefix for this command will stop the Telnet server or reset the maximum number of connections to the default value.

Syntax

Parameter	Description
max-connections <i>max-connections-number</i>	Specifies the maximum number of connections on Telnet server. (Range: 1-16)
server	Enables the internal Telnet server.
source-iface	Specify Telnet source address.
vlan <i>number</i>	Select VLAN interface as source address. (Range: 1-4094)
loopback <i>number</i>	Select loopback interface as source address. (Range: 0-7)
mgmt-eth	Select management interface as source address.

Default

Max-connections: 8 connections

Telnet server is enabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
11.2	Maximum number of sessions was changed from 32 to 16.
11.6	The option source-iface was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the maximum number of connections to 20.

```
DmSwitch(config)#ip telnet max-connections 20
DmSwitch(config)#
```

You can verify that the maximum number os connections was changed by entering the **show ip telnet** privileged EXEC command.

Another example enables the ip telnet source-iface command with its options.

```
DM4000(config)#ip telnet source-iface
vlan          Select VLAN interface as source address
loopback      Select loopback interface as source address
mgmt-eth       Select management interface as source address
```

Related Commands

Command	Description
management	Filters client IP address that tries to access internal servers.
show ip telnet	Shows the Telnet server information.
show management	Shows the management IP filters.
show running-config	Shows the current operating configuration.
terminal timeout	Sets an idle timeout for terminal.

ip tftp

```
ip tftp { source-interface [ vlan number | loopback number | mgmt-eth ] }
```

```
no ip tftp { source-interface }
```

Description

Configures the internal TFTP client options.

Inserting **no** as a prefix for this command will reset the chosen option to the default value.

Syntax

Parameter	Description
source-interface	Specify TFTP source address.
vlan number	Select VLAN interface as source address. (Range: 1-4094)
loopback number	Select loopback interface as source address. (Range: 0-7)
mgmt-eth	Select management interface as source address.

Default

No default source interface is chosen, nearest IP address will be used.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the source interface to VLAN 1.

```
DmSwitch(config)#ip tftp source-interface vlan 1
```

```
DmSwitch(config)#
```

You can verify that the source interface was changed by entering the **show ip tftp** privileged EXEC command.

Related Commands

Command	Description
show ip tftp	Shows the TFTP client information.
show running-config	Shows the current operating configuration.

ipv6 telnet

```
ipv6 telnet { max-connections max-connections-number }
```

```
no ipv6 telnet { max-connections }
```

Description

Configures Telnet maximum number of IPv6 connections.

Inserting **no** as a prefix for this command will reset the maximum number of connections to the default value.

Syntax

Parameter	Description
max-connections <i>max-connections-number</i>	Specifies the maximum number of IPv6 connections on Telnet server. (Range: 1-32)

Default

Max-connections: 8 connections

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the maximum number of IPv6 connections to 20.

```
DmSwitch(config)#ipv6 telnet max-connections 20
DmSwitch(config)#
```

You can verify that the maximum number of connections was changed by entering the **show ip telnet** privileged EXEC command.

Related Commands

Command	Description
<code>management</code>	Filters client IP address that tries to access internal servers.
<code>show ip telnet</code>	Shows the Telnet server information.
<code>show management</code>	Shows the management IP filters.
<code>show running-config</code>	Shows the current operating configuration.

ip vrf

ip vrf *vrf-name*

no ip vrf *vrf-name*

Description

Creates a VPN routing and forwarding (VRF) routing table instance and assigns to it a name. This command also enables the VRF configuration mode.

Inserting **no** as a prefix for this command will delete the specified VRF.

Syntax

Parameter	Description
<i>vrf-name</i>	Name assigned to a VRF.

Default

No VRF is created.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

By using the **ip vrf** command it's possible to instantiate a VRF and associate it to a Layer 3 Virtual Private Network (L3VPN) which is deployed over an MPLS infrastructure.

After creating the VRF, the user must associate a Router Distinguisher, which will compose a VPNv4 route when associated to each prefix present on the VRF.

Specifying one or more route-target external communitys enables the user to deploy L3VPN services.

Finally, it's necessary to configure BGP **address-family vpnv4** in order to exchange vpnv4 routes into MPLS cloud.

Example

This example shows how to create a VRF and enter into VRF configuration mode.

```
DmSwitch(config)#ip vrf vrf1
DmSwitch(config-ip-vrf)#
```

To verify the VRF configuration enter the **show ip vrf** command.

Related Commands

Command	Description
ip vrf forwarding	Configures the selected VLAN to use the specified VRF instance.
rd	Specifies the route distinguisher for a VRF instance.
route-target	Creates a route-target extended community for a VRF instance.
show ip route vrf	Shows the RIB of the specified VRF.
show ip vrf	Shows VRF general information.

key chain

key chain *name*

no key chain *name*

Description

Configures a key chain.

Inserting **no** as a prefix for this command will remove the configured key chain.

Syntax

Parameter	Description
<i>name</i>	Specifies the name of key chain.

Default

No key chain is configured.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Key chain management is a method of authentication to configure shared secrets on all the entities, which exchange secrets such as keys before establishing trust with each other.

Example

This example shows how to specify a key chain name.

```
DmSwitch(config)#key chain test
```

```
DmSwitch(config-keychain) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
key id	Specifies a key identifier.
key-string	Configures the text string for a key identifier.
show running-config	Shows the current operating configuration.

l2protocol-tunnel

```
l2protocol-tunnel { dest-mac-address mac-address }
```

```
no l2protocol-tunnel { dest-mac-address }
```

Description

Configures the layer 2 protocols tunneling.

Inserting **no** as a prefix for this command will delete the destination MAC address defined for the layer 2 protocol tunneling.

This configuration does not apply on L2 Control Protocol Tunneling, and Extended Tunneling which always uses DATACOM OUI MAC address prefix (01:04:DF:CD:CD) as destination.

Syntax

Parameter	Description
dest-mac-address <i>mac-address</i>	Defines a destination MAC address. It will be used by the packets that have been tunneled.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The configured destination MAC address must be the same on all switches on the tunnelling path.

Example

This example shows how to define a MAC address to be used by the layer 2 protocol tunneling.

```
DmSwitch(config)#l2protocol-tunnel dest-mac-address 01-02-03-04-05-06
DmSwitch(config)#
```

You can verify that the MAC address was defined by entering the **show l2protocol-tunnel** privileged EXEC command.

Related Commands

Command	Description
show l2protocol-tunnel	Shows Layer 2 Protocols Tunneling information.
l2protocol-tunnel (Interface configuration)	Configures Layer 2 protocols tunneling for the Ethernet interface.

lacp mode

```
lacp mode { active | passive }
```

```
no lacp mode
```

Description

Configures LACP operation mode.

Inserting **no** as a prefix for this command will reset it to its default value.

Syntax

Parameter	Description
active	Configures LACP in active mode.
passive	Configures LACP in passive mode.

Default

The default value for LACP mode is active.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable LACP in passive mode.

```
DmSwitch(config)#lacp mode passive
DmSwitch(config)#
```

You can verify that the active mode was enabled by entering the **show lacp internal** command.

Related Commands

Command	Description
<code>show lacp internal</code>	Shows the LACP internal information.
<code>show lacp neighbors</code>	Shows the LACP neighbors information.

lacp rate

```
lacp rate { normal | fast }
```

```
no lacp rate
```

Description

Configures LACPDU transmission rate .

Inserting **no** as a prefix for this command will reset it to its default value.

Syntax

Parameter	Description
normal	Configures normal LACPDU transmission rate (30s).
fast	Configures fast LACPDU transmission rate (1s).

Default

The default value for LACP rate is normal.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable LACP rate in fast mode.

```
DmSwitch(config)#lacp rate fast
DmSwitch(config)#
```

You can verify that the fast rate was enabled by entering the **show lacp internal** command.

Related Commands

Command	Description
<code>show lacp internal</code>	Shows the LACP internal information.
<code>show lacp neighbors</code>	Shows the LACP neighbors information.

lacp system-priority

lacp system-priority *priority*

no lacp system-priority

Description

Configures LACP System priority.

Inserting **no** as a prefix for this command will reset it to its default value.

Syntax

Parameter	Description
priority	System priority value. (Range: 0-65535)

Default

The default value for LACP System priority is 32768

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set LACP System priority to 2000.

```
DmSwitch(config)#lacp system-priority 2000
DmSwitch(config)#
```

You can verify that the system priority was set by entering the **show lacp sysid** command.

Related Commands

Command	Description
<code>show lacp internal</code>	Shows the LACP internal information.
<code>show lacp neighbors</code>	Shows the LACP neighbors information.
<code>show lacp sysid</code>	Shows the system identifier used by LACP.

link-state-tracking

link-state-tracking {*groupID*}

no link-state-tracking {*groupID*}

Description

Creates and configures a Link-State Tracking Group (LST)

Syntax

Parameter	Description
<i>groupID</i>	LST group ID (Range: 0-15)

Default

no enable

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a Link-State Tracking Group.

```
DmSwitch(config)#link-state-tracking 0
DmSwitch(config-lst-0)#
```

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show link-state-tracking</code>	Shows Link-State Tracking status.
<code>enable</code>	Enables Link-State Tracking Group.
<code>set-member</code>	Adds an interface to a Link-State Tracking Group.

lldp

lldp

no lldp

Description

Enables the LLDP operation in the DmSwitch.

Inserting **no** as a prefix for this command will disable the LLDP operation.

Syntax

No parameter accepted.

Default

LLDP is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable LLDP operation.

```
DmSwitch(config)#lldp
DmSwitch(config)#
```

You can verify that LLDP operation was enable by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp admin-status	Configures the administratively desired status of the local LLDP agent.

Command	Description
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp notification-interval

lldp notification-interval *seconds*

no lldp notification-interval

Description

Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.

Inserting **no** as a prefix for this command will reset the notification interval to the default value.

Syntax

Parameter	Description
<i>seconds</i>	Specifies the interval at which lldp notifications are sent. (Range: 5-3600)

Default

The default value is 5 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure an interval of 120 seconds for SNMP notifications.

```
DmSwitch(config)#lldp notification-interval 120
DmSwitch(config)#
```

You can verify that the notification interval was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp reinitialize-delay

lldp reinitialize-delay *seconds*

no lldp reinitialize-delay

Description

Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled.

Inserting **no** as a prefix for this command will reset the reinitialize delay to the default value.

Syntax

Parameter	Description
<i>seconds</i>	Specifies the delay that applies to the re-initialization attempt.(Range: 1-10)

Default

The default value is 2 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a re-initialization delay of 10 seconds.

```
DmSwitch(config)#lldp reinitialize-delay 10
DmSwitch(config)#
```

You can verify that the re-initialization delay was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp transmit-delay

```
lldp transmit-delay { auto | seconds }
```

```
no lldp transmit-delay
```

Description

Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB).

Inserting **no** as a prefix for this command will reset the transmit interval to the default value.

Syntax

Parameter	Description
auto	Set delay time to maximum allowed value (25% of transmit-interval).
<i>seconds</i>	Specifies the delay time between successive frame transmissions. Range is (1-8192) but maximum allowed value is 25% of transmit-interval.

Default

The default value is 2 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how automatically to configure the delay time between successive LLDP frame transmissions.

```
DmSwitch(config)#lldp transmit-delay auto
DmSwitch(config)#
```

You can verify that the auto transmit delay was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is transmit-interval * transmit-hold.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp transmit-hold

`lldp transmit-hold value`

`no lldp transmit-hold`

Description

Configures the transmit-hold that is used to calculate the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.

Inserting **no** as a prefix for this command will reset the transmit-hold to the default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the TTL value to transmit. (Range: 2-10)

Default

The default value is 4.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the transmit-hold value of 5.

```
DmSwitch(config)#lldp transmit-hold 5
DmSwitch(config)#
```

You can verify that the the transmit-hold value was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp transmit-interval

```
lldp transmit-interval seconds
```

```
no lldp transmit-interval
```

Description

Configures the periodic transmit interval for LLDP protocol data units (PDUs).

Inserting **no** as a prefix for this command will reset the transmit interval to the default value.

Syntax

Parameter	Description
<i>seconds</i>	Specifies the time duration between LLDP transmissions. Range is (5-32768) but the minimum allowed value is 4 times the transmit-delay.

Default

The default value is 30 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a transmit interval of 10 seconds for LLDP PDUs.

```
DmSwitch(config)#lldp transmit-interval 10
DmSwitch(config)#
```

You can verify that the transmit interval was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp med location-identification coordinate altitude

```
lldp med location-identification coordinate altitude value
```

```
no lldp med location-identification coordinate altitude
```

Description

This command sets the location-identification coordinate altitude parameter.

Inserting **no** as a prefix for this command will reset the altitude to the default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the altitude value. (Range: -4194303 - 4194303)

Default

The default value is 0.0.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

For altitude-type meters, 0.0 indicate unknown altitude. For altitude-type floors, value represent floor-to-floor dimensions, 0.0 represents the floor level associated with ground level at the main entrance. Sub-floors (mezzanine) can be represented by non-integer values. Negative values can be accepted in two types.

Example

This example shows how to configure altitude.

```
DmSwitch(config)#lldp med location-identification coordinate altitude 15.1
DmSwitch(config)#
```

You can verify that the location-identification coordinate altitude was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate altitude-resolution

`lldp med location-identification coordinate altitude-resolution value`

`no lldp med location-identification coordinate altitude-resolution`

Description

This command sets the location-identification coordinate altitude-resolution parameter.

Inserting **no** as a prefix for this command will reset the altitude-resolution to the default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the resolution of altitude. (Range: 0-30)

Default

The default value is 0.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Indicating the number of valid bits in the altitude.

Example

This example shows how to configure altitude-resolution.

```
DmSwitch(config)#lldp med location-identification coordinate altitude-resolution 30
DmSwitch(config)#
```

You can verify that the location-identification coordinate altitude-resolution was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate altitude-type

```
lldp med location-identification coordinate altitude-type { meters|floors }
```

```
no lldp med location-identification coordinate altitude-type
```

Description

This command sets the location-identification coordinate altitude-type parameter.

Inserting **no** as a prefix for this command will reset the altitude-type to the default value.

Syntax

Parameter	Description
<i>meters</i>	Enables representing altitude in meters
<i>floors</i>	Enables representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions.

Default

The default value is meters.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure altitude type.

```
DmSwitch(config)#lldp med location-identification coordinate altitude-type floors
DmSwitch(config)#
```

You can verify that the location-identification coordinate altitude-type was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate datum

```
lldp med location-identification coordinate datum {  
nad83-mlw|nad83-navd|wgs84 }
```

```
no lldp med location-identification coordinate datum
```

Description

This command sets the location-identification coordinate datum parameter.

Inserting **no** as a prefix for this command will reset the datum to the default value.

Syntax

Parameter	Description
<i>nad83-mlw</i>	North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW) This datum pair is to be used when referencing locations on water/sea/ocean
<i>nad83-navd</i>	North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88) This datum pair is to be used when referencing locations on land, not near tidal water.
<i>wgs84</i>	(Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich

Default

The default value is wgs84.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure datum.

```
DmSwitch(config)#lldp med location-identification coordinate datum wgs84
DmSwitch(config)#
```

You can verify that the location-identification coordinate datum was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate latitude

```
lldp med location-identification coordinate latitude value
```

```
no lldp med location-identification coordinate latitude
```

Description

This command sets the location-identification coordinate latitude parameter.

Inserting **no** as a prefix for this command will reset the longitude to the default value.

Syntax

Parameter	Description
<i>value</i>	.Latitude SHOULD be normalized to within +/- 90 degrees. Positive numbers are north of the equator and negative numbers are south of the equator. (Range: -90 - 90)

Default

The default value is 0.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure latitude.

```
DmSwitch(config)#lldp med location-identification coordinate latitude -30.00471
DmSwitch(config)#
```

You can verify that the location-identification coordinate latitude was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate latitude-resolution

`lldp med location-identification coordinate latitude-resolution value`

`no lldp med location-identification coordinate latitude-resolution`

Description

This command sets the location-identification coordinate latitude-resolution parameter.

Inserting **no** as a prefix for this command will reset the latitude to the default value.

Syntax

Parameter	Description
<i>value</i>	Latitude resolution indicating the number of valid bits in the fixed-point value of Latitude. (Range: 0-34)

Default

The default value is 34.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure latitude-resolution.

```
DmSwitch(config)#lldp med location-identification coordinate latitude-resolution 34
DmSwitch(config)#
```

You can verify that the location-identification coordinate latitude-resolution was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate longitude

```
lldp med location-identification coordinate longitude value
```

```
no lldp med location-identification coordinate longitude
```

Description

This command sets the location-identification coordinate longitude parameter.

Inserting **no** as a prefix for this command will reset the longitude to the default value.

Syntax

Parameter	Description
<i>value</i>	Longitude SHOULD be normalized to within +/- 180 degrees. Positive values are East of the prime meridian and negative numbers are West of the prime meridian. (Range: -180 - 180)

Default

The default value is 0.0

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure longitude.

```
DmSwitch(config)#lldp med location-identification coordinate longitude -51.32180
DmSwitch(config)#
```

You can verify that the location-identification coordinate longitude was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification coordinate longitude-resolution

```
lldp med location-identification coordinate longitude-resolution value
```

```
no lldp med location-identification coordinate longitude-resolution
```

Description

This command sets the location-identification coordinate longitude-resolution parameter.

Inserting **no** as a prefix for this command will reset the longitude-resolution to the default value.

Syntax

Parameter	Description
<i>value</i>	Longitude resolution indicating the number of valid bits in the fixed-point value of Longitude. (Range: 0-34)

Default

The default value is 34.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure longitude-resolution.

```
DmSwitch(config)#lldp med location-identification coordinate longitude-resolution 34
DmSwitch(config)#
```

You can verify that the location-identification coordinate longitude-resolution was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
lldp med location-identification coordinate altitude	Configures altitude for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification ecs-elin	Configures ecs-elin for lldp med location-identification.

lldp med location-identification ecs-elin

```
lldp med location-identification ecs-elin string
```

```
no lldp med location-identification ecs-elin
```

Description

This command sets the location-identification ecs-elin parameter.

Inserting **no** as a prefix for this command will reset the latitude to the default value.

Syntax

Parameter	Description
<i>string</i>	Specifies the elin number.(10-25 number characters)

Default

The default value is 0.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure ecs-elin

```
DmSwitch(config)#lldp med location-identification ecs-elin 0123456789
DmSwitch(config)#
```

You can verify that the location-identification ecs-elin was configured by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
show lldp	Shows LLDP configuration information.
clear lldp	Clears LLDP data.
lldp med location-identification coordinate altitude-resolution	Configures altitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate altitude-type	Configures altitude-type for lldp med location-identification coordinate.
lldp med location-identification coordinate datum	Configures datum for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude	Configures latitude for lldp med location-identification coordinate.
lldp med location-identification coordinate latitude-resolution	Configures latitude-resolution for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude	Configures longitude for lldp med location-identification coordinate.
lldp med location-identification coordinate longitude-resolution	Configures longitude-resolution for lldp med location-identification coordinate.

logging commands

```
logging commands { to { flash | mail | ram | syslog } | facility facility-type }
```

```
no logging commands { to { flash | mail | ram | syslog } | facility }
```

Description

This command permits enable and configure the commands logging.

Inserting **no** as a prefix for this command will disable the logs of commands to the given destination or if the **facility** option is specified, will restore his default value.

Syntax

Parameter	Description
to	Specifies destination for the command logging.
flash	Log commands to flash.
mail	Log commands to email.
ram	Log commands to RAM.
syslog	Log commands to remote destination.
facility	Configure facility for commands logging.
<i>facility-type</i>	Specifies the facility type. (Range: 16-23)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable the commands logging to RAM.

```
DmSwitch(config)#logging commands to ram
DmSwitch(config)#
```

Related Commands

Command	Description
logging history	Configures the level of local events.
logging host	Configures a remote syslog server.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
logging on	Enables the logging of events.
logging sendmail	Enables and configures the sending of logs via e-mail.
logging trap	Configures the level of events that will be sent to remote syslog.
show log	Shows log messages.
show logging	Shows logging configuration.

logging debug

```
logging debug { all | apply | arp { protection | rx | tx } | cfm { event |  
packet-decode | packet-hex | state } | cpu { tx | rx } | dhcp snooping [ db | control ]  
| dot1x { event | packet-decode | packet-hex | state } | eaps | egr-mgr | elmi { event  
| packet-decode | packet-hex | state } | erps | gvrp | icmp { tx | rx } | intf-mgr |  
ip-tunnel [ db | fsm | hw ] | l3core [ host ] | lacp | link | link-flap | logs | mpls {  
frr-mgr | hardware | lib { db | hw | proc } } | multicast | stp | vrf | vrrp }
```

```
logging debug port-security { event | mac-sticky | state }
```

```
logging debug { l3proto { ips-log | ldp-mem-dump [ clear ] | mem-log | pd-log [  
clear | detail { full | summary } | filter { exclude | include } text | level { audit |  
exception | none | problem } ] } }
```

```
no logging debug { all | apply | arp | cfm [ event | packet-decode | packet-hex |  
state ] | cpu rx | dhcp snooping [ db | control ] | dot1x [ event | packet-decode |  
packet-hex | state ] | eaps | egr-mgr | elmi [ event | packet-decode | packet-hex |  
state ] | erps | gvrp | icmp | intf-mgr | ip-tunnel [ db | [ fsm | [ hw ] ] | l3core [ host ]  
| lacp | link | link-flap | logs | mpls { frr-mgr | hardware | lib { db | hw | proc } } |  
multicast | stp | vrf | vrrp }
```

```
no logging debug port-security { event | mac-sticky | state }
```

```
no logging debug { l3proto { ips-log | mem-log | pd-log }
```

Description

Configures logging of debug messages related to the selected option.

Inserting **no** as a prefix for this command will disable logging of debug messages related to the selected option.

Syntax

Parameter	Description
all	Enables logging of all debug messages.
apply	Enables logging of APPLY time debug messages.
arp protection	Enables logging of debug messages of ARP protection feature.
arp rx	Enables logging of debug messages of ARP packets received at CPU.
arp tx	Enables logging of debug messages of ARP packets transmitted from CPU.
cfm event	Enables logging of CFM events.

Parameter	Description
<code>cfm packet-decode</code>	Enables logging of decoded CFM packets.
<code>cfm packet-hex</code>	Enables logging of CFM packets in hexadecimal format messages.
<code>cfm state</code>	Enables logging of CFM state machines.
<code>cpu tx</code>	Enables logging of debug messages of packets received at CPU.
<code>cpu rx</code>	Enables logging of debug messages of packets transmitted from CPU.
<code>dhcp snooping</code>	Enables logging of debug messages of DHCP Snooping feature.
<code>dhcp snooping db</code>	Enables logging of debug messages about DHCP Snooping database.
<code>dhcp snooping control</code>	Enables logging of debug messages about sending and receiving DHCP Snooping messages and packet inspection.
<code>dot1x event</code>	Enables logging of 802.1X events.
<code>dot1x packet-decode</code>	Enables logging of decoded 802.1X packets.
<code>dot1x packet-hex</code>	Enables logging of 802.1X packets in hexadecimal format messages.
<code>dot1x state</code>	Enables logging of 802.1X state machines.
<code>eaps</code>	Enables logging of EAPS debug messages.
<code>egr-mgr</code>	Enables logging messages for Egress Manager hardware control block.
<code>elmi event</code>	Enables logging of E-LMI events.
<code>elmi packet-decode</code>	Enables logging of decoded E-LMI packets.
<code>elmi packet-hex</code>	Enables logging of E-LMI packets in hexadecimal format messages.
<code>elmi state</code>	Enables logging of E-LMI state machines.
<code>erps</code>	Enables logging of ERPS debug messages.
<code>gvrp</code>	Enables logging of GVRP debug messages.
<code>icmp tx</code>	Enables logging of debug messages of ICMP packets received at CPU.
<code>icmp rx</code>	Enables logging of debug messages of ICMP packets transmitted from CPU.
<code>intf-mgr</code>	Enables logging messages for INTF Manager hardware control block.
<code>ip-tunnel</code>	Enables debug messages about IPv6/IPv4 tunneling.
<code>ip-tunnel db</code>	Enables debug messages about database informations of the IPv6/IPv4 tunneling module.
<code>ip-tunnel fsm</code>	Enables debug messages about the finite state machine of the IPv6/IPv4 tunneling module.
<code>ip-tunnel hw</code>	Enables debug messages about the IPv6/IPv4 tunneling module at L3 hardware.
<code>l3core</code>	Enables debug messages about routes at L3 hardware interaction subsystem.

Parameter	Description
l3core host	Enables debug messages about hosts at L3 hardware interaction subsystem.
l3proto ips-log	Enables logging of internal messages.
l3proto ldp-mem-dump	Dump LDP/PW/Tunnel internal memory contents.
l3proto ldp-mem-dump clear	Clear all internal memory dump files.
l3proto mem-log	Enables dump of memory statistics.
l3proto pd-log	Enables logging messages for L3 routing protocols.
l3proto pd-log clear	Clear L3 protocols debug log file.
l3proto pd-log detail full	Enables L3 protocols logging fully detailed messages.
l3proto pd-log detail summary	Enables L3 protocols logging summarized messages.
l3proto pd-log filter exclude <i>text</i>	Filter excluding specified <i>text</i> .
l3proto pd-log filter include <i>text</i>	Filter only specified <i>text</i> .
l3proto pd-log level audit	Enables problem, exception and audit logs.
l3proto pd-log level exception	Enables problem and exception logs.
l3proto pd-log level none	Disables all logs.
l3proto pd-log level problem	Enables problem logs.
lACP	Enables logging of LACP debug messages.
link	Enables logging of link state debug messages.
link-flap	Enables logging of link-flap debug messages.
logs	Enables logging messages from system logs.
mpls frr-mgr	Enables logging messages for Fast Re-Route manager hardware control block.
mpls hardware	Enables logging messages for general MPLS hardware interaction.
mpls lib	Enables all logging messages for Label Information Base hardware control block.
mpls lib db	Enables logging messages for Label Information Base database.
mpls lib hw	Enables logging messages for Label Information Base hardware interaction.
mpls lib proc	Enables logging messages for Label Information Base process.
multicast	Enables logging messages for multicast protocols.
port-security	Enables logging of port-security debug messages.
stp	Enables logging of STP debug messages.
vrf	Enables logging messages for VRF events.
vrrp	Enables logging of VRRP debug messages.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
6.0	This command was introduced.
9.4	Replaced BGP, OSPF and RIP by L3PROTO. Introduced L3CORE and MULTICAST messages.
10.0	Updated L3CORE and L3PROTO logging debugs. Introduced MPLS and VRF logging debugs.
11.2	Added "intf-mgr" option in MPLS debug. Update syntax of MPLS debugs. Removed "vrf" logging debugs.
11.2	Introduced l3core host option.
12.0	Added link-flap and E-LMI debugs.
12.2	Added 802.1X debugs.
13.0	Added IP Tunnel debugs.
13.0	Added "tx" and "rx" options for debug arp,cpu and icmp.
13.4	Added port-security debugs.
13.4	Added DHCP Snooping logging debugs.
13.4	Moved options egr-mgr and inft-mgr from logging debug mpls hierarchy to logging debug hierarchy.
13.6	Added ERPS debugs.
13.6	Added ARP Protection logging debugs.
13.0	Added apply time debugs.
14.2	Introduced PW/Tunnel internal memory dump.

Usage Guidelines

This command configures logging of debug messages. To log debug messages in RAM/flash memory, set the level of events to be stored in memory to 7, by using the **logging history** command. To send debug messages to an existing remote syslog server, set the level of events to be sent to 7, by using the **logging trap** command.

The **ldp-mem-dump** command creates a snapshot of control-plane internal memory contents (memory dump) when invoked, becoming inactive a few milliseconds later. For that reason, this debug option is not listed in **show logging debugging** command.

Example

This example shows how to send STP debug messages to a remote syslog server.

```
DmSwitch(config)#logging host 10.11.12.13
DmSwitch(config)#logging trap 7
DmSwitch(config)#logging debug stp
DmSwitch(config)#
```


You can verify the debug messages logging configuration by entering the **show logging debug** privileged EXEC command.

Related Commands

Command	Description
debug	Enables the printing of debug messages.
logging facility	Sets the facility type for remote logging.
logging history	Configures the level of local events.
logging on	Enables the logging of events.
logging trap	Configures the level of events that will be sent to remote syslog.
logging host	Configures a remote syslog server.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
show log	Shows log messages.
show logging	Shows logging configuration.
show running-config	Shows the current operating configuration.

logging facility

logging facility *facility-type*

no logging facility

Description

Sets the facility type for remote logging.

Inserting **no** as a prefix for this command will restore the default facility value for remote logging.

Syntax

Parameter	Description
<i>facility-type</i>	Specifies the facility type. (Range: 16-23)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the facility type 18 for remote logging.

```
DmSwitch(config)#logging facility 18
DmSwitch(config)#
```

You can verify that the facility type was set by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>logging history</code>	Configures the level of local events.
<code>logging host</code>	Configures a remote syslog server.
<code>logging host destination-ipv6</code>	Configures a remote syslog server with IPv6 address.
<code>logging on</code>	Enables the logging of events.
<code>logging sendmail</code>	Enables and configures the sending of logs via e-mail.
<code>logging trap</code>	Configures the level of events that will be sent to remote syslog.
<code>show log</code>	Shows log messages.
<code>show logging</code>	Shows logging configuration.
<code>show running-config</code>	Shows the current operating configuration.

logging history

```
logging history { flash | ram | terminal } log-level
```

```
no logging history { flash | ram | terminal }
```

Description

Configures the level of local events.

Inserting **no** as a prefix for this command will restore the default logging level for the specified destination.

Syntax

Parameter	Description
flash	Configures log level for flash memory.
ram	Configures log level for RAM memory.
terminal	Configures log level for terminal logging.
<i>log-level</i>	Defines the range of log levels that will be saved in the specified memory. (Range: 0-7)

Default

Default level for flash memory is 4.

Default level for RAM memory is 6.

Default level for terminal logging is 6.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.0	Default level for flash memory changed from 3 to 4.
13.0	Added terminal as a destination option for this command.

Usage Guidelines

Not available.

Example

This example shows how to configure a range of 0 to 3 of log levels to be saved in flash memory.

```
DmSwitch(config)#logging history flash 3
DmSwitch(config)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
logging facility	Sets the facility type for remote logging.
logging host	Configures a remote syslog server.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
logging on	Enables the logging of events.
logging sendmail	Enables and configures the sending of logs via e-mail.
logging trap	Configures the level of events that will be sent to remote syslog.
show log	Shows log messages.
show logging	Shows logging configuration.
show running-config	Shows the current operating configuration.

logging host

```
logging host ip-address [ source-iface { loopback number | vlan number | mgmt-eth } ]
```

```
no logging host [ ip-address [ source-iface ] | all ]
```

Description

Configures a remote syslog server.

Inserting **no** as a prefix for this command will remove the configuration of a remote syslog server.

Using the option "all" will remove both, IPv4 and IPv6 entries.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the IP address of the remote syslog server.
source-iface	(Optional) Specifies the host source interface.
loopback number	Select loopback interface as source address. (Range: 0-7)
vlan number	Select VLAN interface as source address. (Range: 1-4094)
mgmt-eth	Select management interface as source address.
all	Remove all remote hosts entries.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
6.6	The option source-iface was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the IP address of the remote syslog server.

```
DmSwitch(config)#logging host 10.11.12.13
DmSwitch(config)#
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
logging facility	Sets the facility type for remote logging.
logging history	Configures the level of local events.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
logging on	Enables the logging of events.
logging sendmail	Enables and configures the sending of logs via e-mail.
logging trap	Configures the level of events that will be sent to remote syslog.
show log	Shows log messages.
show logging	Shows logging configuration.
show running-config	Shows the current operating configuration.

logging host destination-ipv6

```
logging host destination-ipv6 ipv6-address [ scope-iface { vlan number | mgmt-eth } ]
```

```
no logging host destination-ipv6 { ipv6-address }
```

Description

Configures a remote syslog server with IPv6 address.

Inserting **no** as a prefix for this command will remove the configuration of a remote syslog server.

In order to set a IPv6 for remote syslog is needed to have the IPv6 enabled in the scope interface and also an IPv6 address configured.

Syntax

Parameter	Description
<i>ipv6-address</i>	Specifies the IPv6 address of the remote syslog server
scope-iface	(Optional) Specifies the scope resolution interface if non-global scope address is being used.
<i>vlan number</i>	Select VLAN interface as scope resolution interface. (Range: 1-4094)
mgmt-eth	Select management interface as scope resolution interface.

Default

If no interface is specified for IPv6 remote host, default VLAN will be used as scope resolution interface.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the IPv6 address of the remote syslog server with management interface as scope interface.

```
DmSwitch(config)#logging host destination-ipv6 fe80::224:21bf:feaa:e98c scope-iface mgmt-eth
DmSwitch(config)#
```

You can verify that the IPv6 address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
logging facility	Sets the facility type for remote logging.
logging history	Configures the level of local events.
logging host	Configures a remote syslog server.
logging on	Enables the logging of events.
logging sendmail	Enables and configures the sending of logs via e-mail.
logging trap	Configures the level of events that will be sent to remote syslog.
show log	Shows log messages.
show logging	Shows logging configuration.
show running-config	Shows the current operating configuration.

logging on

logging on

no logging on

Description

Enables the logging of events.

Inserting **no** as a prefix for this command will disable the logging of events.

Syntax

No parameter accepted.

Default

Enabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable event logging.

```
DmSwitch(config)#logging on
DmSwitch(config)#
```

You can verify that the logging was enabled by entering the **show logging** privileged EXEC command.

Related Commands

Command	Description
logging facility	Sets the facility type for remote logging.

Command	Description
<code>logging history</code>	Configures the level of local events.
<code>logging host</code>	Configures a remote syslog server.
<code>logging host destination-ipv6</code>	Configures a remote syslog server with IPv6 address.
<code>logging sendmail</code>	Enables and configures the sending of logs via e-mail.
<code>logging trap</code>	Configures the level of events that will be sent to remote syslog.
<code>show log</code>	Shows log messages.
<code>show logging</code>	Shows logging configuration.
<code>show running-config</code>	Shows the current operating configuration.

logging sendmail

```
logging sendmail [ host ip-address | level log-level | source-email email-address |  
destination-email email-address ]
```

```
no logging sendmail [ host ip-address | level | source-email | destination-email  
email-address ]
```

Description

Enables and configures the sending of logs via e-mail.

Inserting **no** as a prefix for this command will disable the sending of logs via e-mail or delete the specified configuration used for sending e-mails.

Syntax

Parameter	Description
host <i>ip-address</i>	(Optional) Specifies the IPv4/IPv6 address of the SMTP server.
level <i>log-level</i>	(Optional) Defines the range of log levels that will be sent by e-mail. (Range: 0-7)
source-email <i>email-address</i>	(Optional) Specifies the e-mail address to use for the "from" field.
destination-email <i>email-address</i>	(Optional) Specifies the recipients e-mail address of messages.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.4	IPv6 address option was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a e-mail to use for the "from" field.

```
DmSwitch(config)#logging sendmail source-email DmSwitch@Datacom.ind.br
DmSwitch(config)#
```

You can verify that the e-mail was configured by entering the **show logging sendmail** privileged EXEC command.

Related Commands

Command	Description
logging facility	Sets the facility type for remote logging.
logging history	Configures the level of local events.
logging host	Configures a remote syslog server.
logging host destination-ipv6	Configures a remote syslog server with IPv6 address.
logging on	Enables the logging of events.
logging trap	Configures the level of events that will be sent to remote syslog.
show log	Shows log messages.
show logging	Shows logging configuration.
show running-config	Shows the current operating configuration.

logging trap

logging trap *log-level*

no logging trap

Description

Configures the level of events that will be sent to remote syslog.

Inserting **no** as a prefix for this command will restore the default facility for remote logging and disable the sending of logs to the remote syslog.

Syntax

Parameter	Description
<i>log-level</i>	Defines the range of log levels that will be sent by trap. (Range: 0-7)

Default

Enabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the range of log levels that will be sent by traps.

```
DmSwitch(config)#logging trap 3
DmSwitch(config)#
```

You can verify that the range of log levels was configured by entering the **show logging trap** privileged EXEC command.

Related Commands

Command	Description
<code>logging facility</code>	Sets the facility type for remote logging.
<code>logging history</code>	Configures the level of local events.
<code>logging host</code>	Configures a remote syslog server.
<code>logging host destination-ipv6</code>	Configures a remote syslog server with IPv6 address.
<code>logging on</code>	Enables the logging of events.
<code>logging sendmail</code>	Enables and configures the sending of logs via e-mail.
<code>show log</code>	Shows log messages.
<code>show logging</code>	Shows logging configuration.
<code>show running-config</code>	Shows the current operating configuration.

loopback-detection action

```
loopback-detection action { block | shutdown }
```

```
no loopback-detection action
```

Description

Configures action taken by Loopback Detection protocol when failure condition is detected.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
block	Block traffic on interface when fail condition is detected
shutdown	Shutdown interface when fail condition is detected

Default

The default action taken by Loopback-Detection protocol is to block the interface.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4.2	This command was introduced.

Usage Guidelines

This command is used to configure action taken when failure condition is detected by Loopback-Detection protocol.

The most common action is to block the interface and let its link state unchanged. However, for some applications a more restrictive action is necessary; the shutdown action changes the link state in the same way as **shutdown** command.

Please note that changes in link state caused by shutdown action will be registered by Link-Flap Detection protocol. Thus, **unblock-time** of Loopback-Detection and Link-Flap Detection parameters must be configured accordingly.

Example

This example shows how to configure loopback-detection action:

```
DmSwitch(config)#loopback-detection action shutdown
DmSwitch(config)#
```

You can verify that the information was configured by entering the **show loopback-detection** privileged EXEC command.

Related Commands

Command	Description
show loopback-detection	Shows loopback-detection status and configuration
show running-config	Shows the current operating configuration.
show loopback-detection	Shows loopback-detection status and configuration
loopback-detection	Configures destination address Loopback Detection PDUs
destination-address	

loopback-detection destination-address

```
loopback-detection destination-address { alternative | interface-mac |  
standard }
```

```
no loopback-detection destination-address
```

Description

Configures destination MAC address of Loopback Detection PDUs.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
alternative	Use slow protocols alternative MAC address: 01:04:DF:00:00:02
interface-mac	Use Ethernet interface MAC address
standard	Use slow protocols standard MAC address: 01:80:C2:00:00:02

Default

The default destination address of Loopback-Detection PDUs the standard address of slow protocols.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4.2	This command was introduced.

Usage Guidelines

This command is used to configure the destination MAC address of Loopback-Detection PDUs.

The most usual destination MAC address is the standard address of slow protocols (multicast). That MAC address is not forwarded by any network element, and is very useful to detect RX/TX loopback on optical links or electrical loopbacks caused by problems on copper links.

An alternative MAC address of slow protocols can be used for applications where PDUs must be commuted by adjacent network elements, to detect issues in other links; that is not possible when using the standard address for slow protocols. The alternative MAC address is also a multicast address.

Finally, Loopback-Detection PDUs can use the interface MAC address, which is an unicast address. Using that address will reduce traffic of multicast frames on the network.

Example

This example shows how to configure loopback-detection destination address:

```
DmSwitch(config)#loopback-detection destination-address interface-mac
DmSwitch(config)#
```

You can verify that the information was configured by entering the **show loopback-detection** privileged EXEC command.

Related Commands

Command	Description
show loopback-detection	Shows loopback-detection status and configuration
show running-config	Shows the current operating configuration.
loopback-detection action	Configures action of Loopback Detection protocol

mac-address-table aging-time

```
mac-address-table aging-time { aging-time | 0 | mode { global | vlan } }
```

```
no mac-address-table aging-time [ mode ]
```

Description

Sets the length of time before removing unused dynamic entries in the MAC address table.

Inserting **no** as a prefix for this command will return the aging time to the default value.

Syntax

Parameter	Description
<i>aging-time</i>	Defines the global aging time in seconds. (Range: 10-1000000)
0	Disables the global aging time.
mode	Selects aging time mode.
global	Selects the global aging time mode.
vlan	Selects the VLAN aging time mode.

Default

300 seconds

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

If you disable the MAC address table aging time, MAC addresses are learned and never removed from the table. When the table is full, packets with unknown source MAC addresses do not cause learning and packets with unknown destination MAC addresses are flooded.

When a specific port change its status to down, all entries on that port are removed from the MAC address table. This is independent of the aging time set to MAC address table entries.

Example

This example shows how to change the global aging time to 1000 seconds.

```
DmSwitch(config)#mac-address-table aging-time 1000
DmSwitch(config)#
```

You can verify the global aging time configuration by entering the **show mac-address-table aging-time** privileged EXEC command.

Related Commands

Command	Description
clear mac-address-table	Erases entries stored in the MAC address table.
mac-address-table static	Adds a static address to MAC address table.
show mac-address-table	Shows the MAC address table.
show running-config	Shows the current operating configuration.

mac-address-table duplication-monitoring

```
mac-address-table duplication-monitoring
```

```
no mac-address-table duplication-monitoring
```

Description

Sets the duplication MAC addresses monitoring.

Inserting **no** as a prefix for this command will disable feature.

Syntax

No parameter accepted.

Default

Disable

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If enable mac-adress-table duplication-monitoring, log and sends out a notification trap announcing that a connected host has moved from one port to another.

Example

This example shows how to enable duplication-monitoring.

```
DmSwitch(config)#mac-address-table duplication-monitoring
DmSwitch(config)#
```

You can verify the duplication-monitoring was enable by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show logging ram</code>	Erases entries stored in the MAC address table.
<code>show running-config</code>	Shows the current operating configuration.

mac-address-table move-monitoring

`mac-address-table move-monitoring`

`no mac-address-table move-monitoring`

Description

Sets the MAC addresses move monitoring.

Inserting **no** as a prefix for this command will disable feature.

Syntax

No parameter accepted.

Default

Disable

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If enable mac-adress-table move-monitoring, log and sends out a notification trap announcing that a connected host has moved from one interface to another.

Example

This example shows how to enable move-monitoring.

```
DmSwitch(config)#mac-address-table move-monitoring
DmSwitch(config)#
```

You can verify the move-monitoring was enable by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mac-address-table move-monitoring	Configure MAC address move monitoring per interface.
show logging ram	Shows logging configuration.
show running-config	Shows the current operating configuration.

mac-address-table static

```
mac-address-table static mac-address { ethernet [ unit-number/ ] port-number |  
port-channel port-channel-number } vlan vlan-id
```

```
no mac-address-table static mac-address vlan vlan-id
```

```
no mac-address-table sticky unit unit-number
```

Description

Adds a static entry to the MAC address table. This will force packets with a specified destination MAC address and VLAN to be always forwarded to the specified interface. If a multicast MAC address is provided, multiple output interfaces can be configured for it.

Inserting **no** as a prefix for this command will remove a static entry from the MAC address table. **sticky** option in this case, will delete all Sticky MACs from the selected unit.

Syntax

Parameter	Description
<i>mac-address</i>	Defines the MAC address.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Defines the ethernet unit (optional) and port to be associated with the static entry.
port-channel <i>port-channel-number</i>	Defines the port channel to be associated with the static entry.
vlan <i>vlan-id</i>	Defines the VLAN ID associated with the static entry. (Range: 1-4094)

Default

By default, no static entries are configured.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Added multicast support.

Usage Guidelines

Not available.

Example

This example shows how to add a static MAC address on ethernet port 1 and VLAN 1.

```
DmSwitch(config)#mac-address-table static 00-01-02-03-04-05 ethernet 1 vlan 1
DmSwitch(config)#
```

You can verify that the static MAC address was added by entering the **show mac-address-table** privileged EXEC command.

Related Commands

Command	Description
clear mac-address-table	Erases entries stored in the MAC address table.
mac-address-table aging-time	Sets the aging time for MAC address table entries.
show mac-address-table	Shows the MAC address table.
show running-config	Shows the current operating configuration.

management

```
management { all-client | http-client | snmp-client | ssh-client |  
telnet-client } { ip-address/mask | ipv6address/prefix-length }
```

```
no management { all-client | http-client | snmp-client | ssh-client |  
telnet-client } ip-address/mask | ipv6address/prefix-length }
```

```
management snmp-client { ip-address/mask | ipv6address/prefix-length } community  
community-name
```

Description

Filters client IP address to access internal servers.

Inserting **no** as a prefix for this command will remove the specified filter.

Syntax

Parameter	Description
all-client	Adds clients IP addresses to HTTP, SNMP, SSH and Telnet internal servers.
http-client	Adds clients IP addresses to HTTP internal server.
snmp-client	Adds clients IP addresses to SNMP internal server.
ssh-client	Adds clients IP addresses to SSH internal server.
telnet-client	Adds clients IP addresses to Telnet internal server.
<i>ip-address/mask</i>	Specifies the clients network.
<i>ipv6address/prefix-length</i>	Specifies the clients IPv6 network.

Default

No filter is configured.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The configuration to filter a different IP address that you are logged in (e.g. Telnet connection), disconnects your current session.

Use the mask /32 to indicate a unique host.

Example

This example shows how to add a client IP address to access all internal servers.

```
DmSwitch(config)#management all-client 11.11.11.11/32
DmSwitch(config)#
```

You can verify that the client IP address was added by entering the **show management all-client** privileged EXEC command.

Related Commands

Command	Description
ip http	Configures the internal HTTP server for external access.
ip snmp	Configures the internal SNMP server.
ip ssh	Configures the internal SSH server for external access.
ip telnet	Configures the internal Telnet server for external access.
show ip http	Shows the HTTP server information.
show ip snmp	Shows the SNMP server information.
show ip ssh	Shows the SSH server information.
show ip telnet	Shows the Telnet server information.
show running-config	Shows the current operating configuration.

memory-external resource ^[5]

```
memory-external resource { vlan entries | disable }
```

Description

Configure resource for using with external memory in RSVP scenarios.

Syntax

Parameter	Description
<code>vlan entries</code>	Sets reserved vlan.
<code>disable</code>	Disable resources.

Default

Default is resources disabled.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command must be used when the switch belongs to RSVP tunnel paths as LSR and it has external memory enabled for routing.

The reserved VLAN cannot be in use.

Example

This example illustrates how to enable the external memory resource.

```
DmSwitch(config)#memory-external resource vlan 4095
DmSwitch(config)#
```

This example illustrates how to disable the external memory resource.

```
DmSwitch(config)#memory-external resource disable
```

```
DmSwitch(config)#
```

Related Commands

Command	Description
<code>show memory external</code>	Shows memory configuration.

chassis load-balance ^[1] ^[5] ^[6] ^[8] ^[9]

```
chassis load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip |  
src-mac | enhanced } unit unit-number
```

```
no chassis load-balance unit unit-number
```

Description

Internally, all units in the chassis are connected to the MPU. Units with more front panel interfaces have more connections to the MPU; usually this number ranges from two to four connections for each unit. In a chassis system, traffic can ingress from a given unit and egress to another unit, flowing through the internal chassis connections of these units with the MPU.

The ingress/egress traffic of a given unit is usually spread among all connections of that unit with the active MPU using a default load balance criteria. This command allows the configuration of the port selection criteria to be used for each unit when traffic flows from/to the unit to/from the MPU through the internal connections of the chassis.

Syntax

Parameter	Description
dst-ip	Use destination IP address to balance traffic between unit and MPU
dst-mac	Use destination MAC address to balance traffic between unit and MPU
src-dst-ip	Use source and destination IP addresses to balance traffic between unit and MPU
src-dst-mac	Use source and destination MAC addresses to balance traffic between unit and MPU
src-ip	Use source IP address to balance traffic between unit and MPU
src-mac	Use source MAC address to balance traffic between unit and MPU
enhanced	Use MPLS labels, MAC addresses, IP addresses and TCP/UDP ports to balance traffic between unit and MPU

Default

The 'src-dst-mac' port selection criteria is used for load balance of the traffic from/to MPU to/from all units.

Command Modes

Privileged EXEC.

Command History

Release	Modification
14.10.10	This command was introduced.

Usage Guidelines

Internally, all units in the chassis are connected to the MPU. Units with more front panel interfaces have more connections to the MPU; usually this number ranges from two to four connections for each unit. The ingress/egress traffic of a given unit is usually spread among all connections of that unit with the active MPU using a default load balance criteria and this command allows the configuration of the port selection criteria to be used for each unit.

This configuration affects only the traffic from/to each unit to/from the MPU as it flows through the internal chassis connections. It is still necessary to configure the port selection criteria of Port-Channels that group front panel interfaces, so the egress traffic will be distributed/balanced correctly. Please refer to the related commands to learn how to configure load balance on Port-Channels.

The current instant value of bandwidth usage of each interface (including Port-Channel members) can be verified using **show interface table utilization bandwidth**. When members of the same Port-Channel have a very asymmetric bandwidth usage, it is probably necessary to configure the load balance of that Port-Channel and/or the internal chassis connections.

Example

This example illustrates how to configure the load balance criteria for a given unit of the chassis:

```
DmSwitch(config)#chassis load-balance enhanced unit 2
(config)#

DmSwitch#show stacking chassis-load-balance

Unit  Load-balance criteria
----  -
  2   Enhanced (MPLS, IP, MAC, TCP/UDP)
  3   Enhanced (MPLS, IP, MAC, TCP/UDP)
  4   Enhanced (MPLS, IP, MAC, TCP/UDP)

DmSwitch#configure
DmSwitch(config)#chassis load-balance dst-ip unit 2
DmSwitch(config)#exit
DmSwitch#show stacking chassis-load-balance

Unit  Load-balance criteria
----  -
  2   Destination IP
  3   Enhanced (MPLS, IP, MAC, TCP/UDP)
  4   Enhanced (MPLS, IP, MAC, TCP/UDP)
```

Related Commands

Command	Description
show units	Shows information about system units.
show chassis-load-balance	Shows load balance information for internal connections of chassis.
load-balance	Configures load distribution method among the ports.
show interfaces table utilization	Shows the interface average utilization table.

meter

```
meter { ingress | egress } { new | id } mode { { flow | hflow } rate-limit rate [
burst-size burst | remark text | ... ] | srtcm color-blind committed CIR CBS excess
EBS [ remark text ] | { trtcm | htrtcm } color-blind committed CIR CBS peak PIRPBS [
remark text ] }
```

```
no meter { ingress | egress } id
```

Description

Configure a meter to be used by a filter.

Inserting **no** as a prefix for this command will remove meter specified.

Syntax

Parameter	Description
ingress	Meter is related to ingress stage.
egress ^[5]	Meter is related to egress stage.
new	Creates a new meter.
id	Selects a meter to edit by ID.
mode flow	Specifies Flow mode.
mode hflow	Specifies Flow mode for hierarchical metering. This mode does not accept editions.
mode srtcm	Specifies Single-Rate Three-Color Marker mode.
mode trtcm	Specifies Two-Rate Three-Color Marker mode.
mode htrtcm	Specifies Two-Rate Three-Color Marker mode for hierarchical metering.
burst <i>burst-size</i>	(Optional) Specifies the maximum burst size in kbyte (power of 2 steps).
rate-limit <i>rate</i>	Specifies the rate-limit in kbit/s (64 kbit/s granularity).
remark <i>text</i>	(Optional) Adds a remark text.
committed	Committed Information Rate (CIR and PIR) and Burst Size (CBS and PBS).
color-blind	Specifies Color-Blind mode. Resulting color is incoming color independent.
excess	Specifies Excess Burst Size.
<i>CIR</i>	Specifies Committed Information Rate (CIR) in kbit/s (64 kbit/s granularity). (Range: 0-10000000)
<i>CBS</i>	Specifies Committed Burst Size (CBS) in kbyte (power of 2). (Range: 4-16384)
<i>EBS</i>	Specifies Excess Burst Size (EBS) in kbyte (power of 2). (Range: 4-16384)
<i>PIR</i>	Specifies Peak Information Rate (PIR) in kbit/s (64 kbit/s granularity). (Range: 0-10000000)

Parameter	Description
<i>PBS</i>	Specifies Peak Burst Size (PBS) in kbyte (power of 2). (Range: 32-131072)

Default

By default, no meter is created and initial parameters are not defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	The options mode flow and mode srtcm were introduced.
9.0	The option mode trtcm was introduced.
11.6	<i>ingress egress</i> parameter was added.
5.0	The options mode hflow and mode htrtcm were introduced.

Usage Guidelines

Using these meters, the filter can perform different actions on packets from a given flow depending on the state of the meter.

Example

This example shows how to create a new meter.

```
DmSwitch(config)#meter ingress new mode flow rate-limit 1536 burst 512 remark tcp_policy
Meter 1 created.
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show meter** privileged EXEC command.

Related Commands

Command	Description
show meter	Shows meters configuration.
filter	Creates or configures a traffic filter
show running-config	Shows the current operating configuration.

monitor

monitor

Description

Enables monitor configuration mode.

Syntax

Parameter	Description
No parameters are defined.	

Default

No default is defined.

Command Modes

Monitor configuration.

Command History

Release	Modification
3.1	This command was introduced.
10.0	RSPAN was introduced.
13.0	The configuration of parameters were moved to inside monitor configuration mode.

Usage Guidelines

Not available.

Example

This example shows how to entry in monitor configuration mode.

```
DmSwitch(config)#monitor
DmSwitch(config-monitor)#
```

Related Commands

Command	Description
---------	-------------

Command	Description
<code>destination (Monitor configuration)</code>	Configures the traffic monitoring destination interface.
<code>rspan (Monitor configuration)</code>	Configures RSPAN over the traffic monitoring.
<code>source (Monitor configuration)</code>	Configures the traffic monitoring filtered sources.
<code>monitor (Interface configuration)</code>	Sets the interface as a monitoring source.
<code>show monitor</code>	Shows traffic monitoring configuration.
<code>show running-config</code>	Shows the current operating configuration.

mpls exp-map egress ^[1] ^[3] ^[6]

mpls exp-map egress prio *priority-level* **exp** *EXP-level*

no exp-map egress prio *priority-level*

Description

Configures the table mapping from COS priority to EXP egress packets.

Inserting **no** as a prefix for this command will return the service to default.

Syntax

Parameter	Description
prio <i>priority-level</i>	COS Priority Level. (Range: 0-7)
EXP <i>EXP-level</i>	EXP Level. (Range: 0-7)

Default

For each priority (0-7) the EXP has the same value (0-7).

```
DmSwitch#show mpls exp-map egress
Priority - EXP
0 - 0
1 - 1
2 - 2
3 - 3
4 - 4
5 - 5
6 - 6
7 - 7
```

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The MPLS experimental bits are used to provide QoS capabilities by using the EXP bits in MPLS header of an ingress/egress packet.

With EXP field is possible to classify and to prioritize the packets traffic. The MPLS EXP table provides the translation from:

- internal priority (0-7) to MPLS EXP (0-7) for egress packets;
- MPLS EXP (0-7) to internal priority (0-7) for ingress packets.

Example

This example shows how to configure an exp-map table field.

```
DmSwitch(config)#mpls exp-map egress prio 0 exp 1
DmSwitch(config)#
```

You can verify that the service was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls exp-map ingress	Configures the table mapping for EXP to COS priority ingress packets.
show mpls exp-map egress	Shows MPLS COS priority to EXP mapping table for egress packets.
show mpls exp-map ingress	Shows MPLS EXP to COS priority mapping table for ingress packets.
show running config	Shows the current operating configuration.

mpls exp-map ingress ^[1] ^[3] ^[6]

mpls exp-map ingress exp *EXP-level* **prio** *priority-level*

no exp-map ingress exp *EXP-level*

Description

Configures the table mapping from EXP to COS priority assigned to ingress packets.

Inserting **no** as a prefix for this command will return the service to default.

Syntax

Parameter	Description
EXP <i>EXP-level</i>	EXP Level. (Range: 0-7)
prio <i>priority-level</i>	COS Priority Level. (Range: 0-7)

Default

For each EXP (0-7) the priority has the same value (0-7).

```
DmSwitch#show mpls exp-map ingress
EXP - Priority
0 - 0
1 - 1
2 - 2
3 - 3
4 - 4
5 - 5
6 - 6
7 - 7
```

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The MPLS experimental bits are used to provide QoS capabilities by using the EXP bits in MPLS header of an ingress/egress packet.

With EXP field is possible to classify and to prioritize the packets traffic. The MPLS EXP table provides the translation from:

- internal priority (0-7) to MPLS EXP (0-7) for egress packets;
- MPLS EXP (0-7) to internal priority (0-7) for ingress packets.

Example

This example shows how to configure an exp-map table field.

```
DmSwitch(config)#mpls exp-map ingress exp 0 prio 1
DmSwitch(config)#
```

You can verify that the service was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls exp-map egress	Configures the table mapping for COS priority to EXP egress packets.
show mpls exp-map ingress	Shows MPLS EXP to COS priority mapping table for ingress packets.
show mpls exp-map egress	Shows MPLS COS priority to EXP mapping table for egress packets.
show running config	Shows the current operating configuration.

mpls expl-path ^[1] ^[3] ^[6]

mpls expl-path

Description

Enters on Explicit Path Configuration Mode.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to enter on the Explicit Path configuration mode.

```
DmSwitch(config)#  
DmSwitch(config)#mpls expl-path  
DmSwitch(config-mpls-expl-path)#
```

Related Commands

Command	Description
explicit-path identifier	Configures an explicit path
tsp-hop	Configures individually each hop that belongs to an explicit path
tunnel mpls traffic-eng path-option explicit-path identifier	Configures the path-option index and the explicit path identifier

mpls ldp control-mode ^[1] ^[3] ^[5]

```
mpls ldp control-mode { independent | ordered }
```

Description

LDP allows flexibility in strategies when to advertising FEC-label bindings. An LSR using independent control mode advertises FEC-label bindings to peers whenever it sees fit, whereas one using ordered control advertises bindings only when it has previously received a label for the FEC from the FEC nexthop or it is an MPLS egress for the FEC.

Syntax

Parameter	Description
independent	Independent label distribution mode.
ordered	Ordered label distribution mode.

Default

The default mode of label distribution is ordered.

Command Modes

Global configuration.

Command History

Release	
12.2	This command was introduced.

Usage Guidelines

To send labels for every active route the router needs to operate in *independent* mode. This mode is particularly useful when used with RFC 3107. To only send labels for previously sent FECs or local FECs the router needs to operate in *ordered* mode.

By entering the **control-mode** command the user can specify the label distribution control mode of LDP.

Example for independent label distribution mode

This example shows how to configure LDP label distribution control mode to independent.

```
DmSwitch#config
DmSwitch(config)#mpls ldp control-mode independent
DmSwitch(config)#exit
```

```
DmSwitch#
```

Example for ordered label distribution mode

This example shows how to configure LDP label distribution control mode to ordered.

```
DmSwitch#config
DmSwitch(config)#mpls ldp control-mode ordered
DmSwitch(config)#exit
DmSwitch#
```

You can verify the label control mode configuration by entering the **show mpls ldp parameters** user EXEC command.

Related Commands

Command	Description
show mpls ldp parameters	Shows current LDP parameters.
show running-config	Shows the current operating configuration.
neighbor send-label	Enables Carrying Label Information in BGP-4.

mpls ldp discovery ^[1] ^[3] ^[6]

```
mpls ldp discovery { hello|targeted-hello } holdtime seconds
```

```
no mpls ldp discovery { hello|targeted-hello } holdtime
```

Description

Specifies the hold timer for a discovered LDP neighbor.

Inserting **no** as a prefix for this command will revert the configuration to the default value.

Syntax

Parameter	Description
hello	Set hello hold time for basic discovery mechanism.
targeted-hello	Set hello hold time for extend discovery mechanism.
holdtime <i>seconds</i>	Discovery hello hold time in seconds - valid range (1-65535).

Default

The default LDP discovery hello hold time for basic discovery mechanism is 15 seconds. For extend discovery the default value is 45 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	Command syntax was modified.

Usage Guidelines

On receipt of a hello message from an allowed peer, the router adds the discovered neighbor into the adjacency list. The router then maintain a hold timer with each hello adjacency which it restarts whenever it receives a new hello from the neighbor. If the timer expires, the router excludes the hello adjacency from the list and terminates the LDP session with the respective peer.

All routers advertises their configured hello hold time on discovery hello messages. The effective hold time is then set to the smallest value of local and proposed hello hold time.

Within the hello hold time period the router sends 3 discovery hello messages.

Example

This examples shows how to configure the discovery hello and targeted hello hold time.

```
DmSwitch#config
DmSwitch(config)#mpls ldp discovery hello holdtime 20
DmSwitch(config)#exit
DmSwitch#

DmSwitch#config
DmSwitch(config)#mpls ldp discovery targeted-hello holdtime 50
DmSwitch(config)#exit
DmSwitch#
```

You can verify the current discovery hello hold time selected by an adjacency entering the **show mpls ldp discovery detail** user EXEC command. Also, you can verify its current local configuration entering the **show mpls ldp parameters** user EXEC command.

Related Commands

Command	Description
show mpls ldp discovery	Shows the status of LDP discovery process.
show mpls ldp parameters	Shows current LDP parameters.
show running-config	Shows the current operating configuration.

mpls ldp holdtime ^[1] ^[3] ^[6]

```
mpls ldp holdtime seconds [ force ]
```

```
no mpls ldp holdtime [ force ]
```

Description

Specifies the maximum time all LDP sessions are maintained without receipt of any LDP messages from the session peer. This command also indirectly specifies the periodicity of LDP KeepAlive messages when there is no need to exchange LDP messages between LDP peers, maintaining the session alive.

Inserting **no** as a prefix for this command will revert the hold time to the default value.

Syntax

Parameter	Description
<i>seconds</i>	KeepAlive hold time in seconds - valid range (1-65535).
<i>force</i>	Force new timer value on both link and targeted current LDP sessions (all sessions will be restarted). Without this option, the new timer value will only be employed on link sessions established after its configuration. Targeted sessions are always restarted, whether this option is used or not.

Default

The default value for LDP KeepAlive hold time is 40 seconds. The router will send keepAlive messages every 6,66 seconds in absence of LDP protocol messages.

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	Command syntax was modified.
13.0	Option 'force' was implemented.

Usage Guidelines

To maintain LDP sessions and verify its integrity, the router uses a KeepAlive Timer that is reset on receipt of any LDP protocol message (except discovery hello messages). If this timer expires, the router consider that the

session is not operational and terminates it.

By entering the **holdtime** command the user can specify the KeepAlive hold time, in seconds. To guarantee that the session will not be terminate in absence of LDP protocol messages, the router sends a KeepAlive message every $k/6$ seconds, where k is the configured KeepAlive hold time value.

Example

This example shows how to configure LDP KeepAlive hold time to 50 seconds.

```
DmSwitch#config
DmSwitch(config)#mpls ldp holdtime 50
DmSwitch(config)#exit
DmSwitch#
```

You can verify the LDP KeepAlive hold time configuration by entering the **show mpls ldp parameters** user EXEC command.

When there are both targeted and link sessions configured for an entity, the change will not be applied. In this case, it is necessary to use the **force** option.

This example shows how to configure LDP KeepAlive hold time to 50 seconds with **force** option.

```
DmSwitch#config
DmSwitch(config)#mpls ldp holdtime 50 force
DmSwitch(config)#exit
DmSwitch#
```

When LDP *graceful restart* is enabled, the new holdtime value will only be applied once *graceful restart* procedures have been finished.

You can verify the LDP KeepAlive hold time configuration by entering the **show mpls ldp parameters** user EXEC command.

Related Commands

Command	Description
show mpls ldp neighbor	Shows the status of LDP sessions.
show mpls ldp parameters	Shows current LDP parameters.
show running-config	Shows the current operating configuration.

mpls ldp neighbor ^[1] ^[3] ^[6]

```
mpls ldp neighbor { ip-address [ password password ] | advertise-labels }
```

```
no mpls ldp neighbor { ip-address [ password ] | advertise-labels }
```

Description

Sets up an LDP targeted session with the specified neighbor, with an optional password for message authentication. A policy that dictates whether labels for prefix FEC's should be distributed to targeted neighbors can also be configured.

Inserting **no** as a prefix for this command will remove the LDP neighbor, unset its password, or disable distribution of labels for prefix FEC's to targeted neighbors.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of LDP neighbor.
<i>password</i>	Password for LDP neighbor authentication using MD5 encryption. At most 32 characters in length.
advertise-labels	Configure distribution of labels for prefix FEC's to targeted neighbors policy.

Default

Distribution of labels for prefix FEC's to targeted neighbors is enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	Command syntax was modified.
11.0	password option was introduced.
14.4	advertise-labels option was introduced.
15.2.8	The default value for the option advertise-labels has been changed to disable.

Usage Guidelines

There are some cases where it's necessary to establish an LDP session between non-directly connected routers. The user should create one LDP entity in order to set up an LDP targeted session.

Instead of using basic discovery mechanism, a targeted session is established via extended discovery mechanism. In basic discovery mechanism, routers exchange hello messages sending them to a well-known multicast group address. Each router is then capable to build a list of adjacencies which contains all reachable LDP peer directly connected.

Extended discovery mechanism supports LDP sessions between non-directly connected routers since LDP discovery hello messages have as destination the peer's address. Hence, these LDP targeted hello messages are forwarded through the network as an ordinary IP packet.

The **mpls ldp neighbor ip-address** command also allows the router to accept LDP targeted hello messages from the specified peer and to establish LDP targeted session after accomplishing the extended discovery process.

When a password is specified, messages received from the given LDP neighbor are only accepted if they are signed with the TCP MD5 option and the specified password. Outgoing messages to that LDP neighbor are also signed with the same password. This mechanism exists to thwart spoofing attacks by authenticating the source router (which must also have been configured to use the same password).

In most scenarios it is not necessary to advertise FEC labels from host prefixes to targeted neighbors. Only the labels for FECs of infrastructure are required.

It reduces the amount of LDP messages exchanged among routers and also the memory used for the LDP database. Besides that, the convergence timing after LDP target sessions flapping will be improved due to the smaller LDP database.

However, this option must be enabled in LDPoRSVP scenarios, where labels for all types of FECs must be advertised between two targeted peers to allow the tunneled LSP establishment.

Through the command **advertise-labels** it is possible to enable the distribution of such labels to the neighbors.

Example

This example shows how to set up an LDP targeted session between the local host and remote host 100.100.100.3.

```
DmSwitch#config
DmSwitch(config)#mpls ldp neighbor 100.100.100.3
DmSwitch(config)#exit
DmSwitch#
```

The following example shows how to define a password for authenticated message exchange with remote host 100.100.100.3.

```
DmSwitch#config
DmSwitch(config)#mpls ldp neighbor 100.100.100.3 password b4c0n
DmSwitch(config)#exit
DmSwitch#
```

The following example shows how to disable the distribution of labels for prefix FEC's to targeted neighbors.

```
DmSwitch#config
DmSwitch(config)#no mpls ldp neighbor advertise-labels
% Warning:
LSP's may not be established and tunneled over RSVP in some scenarios upon this
operation.
LDP stack will be restarted upon this operation.
Confirm this command? <y/N> y
DmSwitch(config)#exit
DmSwitch#
```

You can verify the LDP targeted session configuration by entering the **show mpls ldp parameters** user EXEC command.

Related Commands

Command	Description
mpls ldp discovery	Specifies the global discovery hold timer for LDP sessions.
mpls ldp holdtime	Specifies the global hold time for all LDP sessions.
show mpls ldp database	List LSP database
show mpls ldp discovery	Shows the status of LDP discovery process.
show mpls ldp neighbor	Shows the status of LDP sessions.
show mpls ldp parameters	Shows current LDP parameters.
show running-config	Shows the current operating configuration.

mpls ldp logging

mpls ldp logging

no mpls ldp logging

Description

Enable LDP event logging. LDP events such as session state up/down and Graceful Restart timer expiration will be logged.

Inserting **no** as a prefix for this command will disable LDP event logging.

Syntax

No parameters accepted.

Default

LDP logging enabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command enables or disables the LDP event logging. The following events are logged:

LDP session state: A message is logged when a session state transition occurs, indicating whether the session has gone up or down. In the case of a session that has gone down, it's also indicated what caused the session state transition (session/adjacency timer expiration, or LDP signaling admin shutdown).

LDP-GR timer expiration: A message is logged indicating that a LDP Graceful Restart timer has expired (LDP-GR has finished). The expiration of the "MPLS Forwarding State Holding timer", "Neighbor Liveness timer" and "Adjacency Down Hold timer" are logged. In the case of expiration of the "Adjacency Down Hold timer", it's also indicated which adjacency had its timer expired (neighbor's uplink interface IP address).

The log can be viewed through the command **show log ram**.

Example

This example shows how to enable the LDP event logging.

```
DmSwitch(config)#mpls ldp logging
DmSwitch(config)#
```

You can verify whether LDP event logging is enabled by entering the command **show running-config**.

Once enabled you can view LDP event logging messages through the command **show log ram**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show log ram	Shows log messages.

mpls ldp igp sync holddown ^[1] ^[3] ^[6]

```
mpls ldp igp sync holddown seconds
```

```
no mpls ldp igp sync holddown
```

Description

Specifies how long an Interior Gateway Protocol (IGP) should wait for Label Distribution Protocol (LDP) Synchronization to be achieved.

Inserting **no** as a prefix for this command will disable the holddown timer for IGP-LDP Synchronization.

Syntax

Parameter	Description
<i>seconds</i>	The number of seconds an IGP should wait for an LDP session to be established. The valid range is from 1 to 2,147,483,647.

Default

An IGP will wait indefinitely for LDP synchronization to be achieved.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command enables you to limit the amount of time an IGP waits for LDP synchronization to be achieved.

The behavior once the timer is expired is to restore the IGP max-metric independently of the LDP session status.

Example

This example shows how to configure the holddown timer to 10 seconds.


```
DmSwitch(config)#mpls ldp igp sync holddown 10
```

You can verify the configuration by issuing the **show mpls ldp igp sync** privileged EXEC command.

Related Commands

Command	Description
show mpls ldp igp sync	Shows the LDP-IGP Synchronization

mpls ldp graceful-restart [1] [3] [6]

```
mpls ldp graceful-restart [ timers { reconnect-time | forwarding-holding |  
neighbor-liveness | max-recovery | adj-down-hold-time } milliseconds ]
```

```
no mpls ldp graceful-restart [ timers { reconnect-time | forwarding-holding  
| neighbor-liveness | max-recovery | adj-down-hold-time } ]
```

Description

Enable and configure LDP Graceful Restart, according to RFC3478.

Inserting **no** as a prefix for this command will revert the configuration to the default value.

Syntax

Parameter	Description
timers reconnect-time	(Optional) Configure the value of FT Reconnect Timeout advertised in FT Session TLV in Initialization message. (Range: 1-2147483647).
timers forwarding-holding	(Optional) Configure the time that the local node is willing to retain its MPLS forwarding state, if any, that it preserved across the restart. (Range: 0-2147483647).
timers neighbor-liveness	(Optional) Configure the maximum time that LDP should wait for a restart capable neighbor to restore an LDP session. (Range: 0-2147483647).
timers max-recovery	(Optional) Configure the maximum period of time that LDP should wait for a restart capable neighbor to refresh Label Mappings previously received from that neighbor. After this time, all stale bindings should be deleted. (Range: 0-2147483647).
timers adj-down-hold-time	(Optional) Configure the time to hold a failed LDP Hello adjacency. The value should be large enough for the LDP session to fail if the LDP peer has failed. Otherwise, the LSP will be teared down. (Range: 0-2147483647).
<i>milliseconds</i>	Respective timer interval in milliseconds.

Default

LDP Graceful Restart is disabled by default. The default value for adj-down-hold-time is 60000 ms. For the remaining of the timers the default value is 240000 ms.

Command Modes

Global configuration.

Command History

Release	Modification
10.0	This command was introduced.
11.0	Changed default values.

Usage Guidelines

LDP Graceful Restart functionality allows control plane to restart and recover its previous state, without affecting data plane and minimizing the impact in service availability.

Changes in LDP Graceful Restart configuration requires LDP to restart in order to make changes effective. If the feature is being activated, such restart shall not affect data plane (i.e. established LSP's are maintained across the restart).

The **reconnect-time** should be large enough for LDP to be terminated and restarted. This time is advertised to neighbors in the FT Session TLV in Initialization messages. There are no restrictions for the value of this timer. However, values lower than 50000 are not recommended because of the risk of LDP not be active at time.

The **forwarding-holding**, also known as recovery-time, should NEVER be zero. When the LDP is up again, after the restart procedure, the forwarding-holding indicates the time that the MPLS forwarding table will be retained. This timer is advertised to neighbors in the FT Session TLV in Initialization messages after restart procedure. Forwarding-holding zero value indicates that any MPLS forwarding information has been retained and all LSP's will be released. When forwarding-holding time expires, it means that the graceful restart procedure for LDP has finished.

The **neighbor-liveness** is an internal timer that is used together with the reconnect-time received from a restart capable neighbor. The neighbor-liveness timer starts when the LSR detects that its LDP session with the neighbor went down. LDP waits for the minimum of this time and the reconnect-time advertised in the FT Session TLV in the Initialization message from the neighbor. There are no restrictions for the value of this timer.

The **max-recovery** is an internal timer that is used together with the forwarding-holding (recovery-time) received from a restart capable neighbor. LDP waits for the minimum of this time and the recovery-time advertised in the FT Session TLV in the Initialization message from the neighbor. There are no restrictions for the value of this timer.

The **adjacency-down-hold-time** helps to distinguish between LDP peer failure and interface failure. This timer ensure that LDP retains adjacency multilink LSPs during peer restart recovery in both cases: when the peer restarts and when an LDP Hello adjacency goes down before the LDP session. The value chosen should be large enough for the LDP session to fail if the LDP peer has failed. For DATACOM products, it is suggested to use values equal or greater than the reconnect-time (50000 ms).

Example

This example illustrates how to enable and configure LDP Graceful Restart.

```
DmSwitch#config
DmSwitch(config)#mpls ldp graceful-restart
DmSwitch(config)#mpls ldp graceful-restart timers reconnect-time 50000
DmSwitch(config)#mpls ldp graceful-restart timers forwarding-holding 30000
DmSwitch(config)#mpls ldp graceful-restart timers max-recovery 30000
DmSwitch(config)#mpls ldp graceful-restart timers adj-down-hold-time 50000
DmSwitch(config)#exit
DmSwitch#
```

You can verify LDP-GR configuration by entering the **show running-config** privileged EXEC command, and the **show mpls ldp parameters** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls ldp parameters	Shows current LDP parameters.
show mpls ldp graceful-restart	Shows LDP Graceful Restart recovery status.

mpls l2vpn logging

```
mpls l2vpn logging { pw-status | redundancy }
```

```
no mpls l2vpn logging { pw-status | redundancy }
```

Description

Enable L2VPN events logging pseudowire status (pw-status) and pseudowire redundancy (redundancy).

Inserting **no** as a prefix for this command will disable L2VPN event logging.

Syntax

Parameter	Description
pw-status	Enable logging pseudowire status (up/down).
redundancy	Enable logging pseudowire redundancy (primary/standby).

Default

Enabled L2VPN events logging pseudowire status and redundancy.

Command History

Release	Modification
14.10	This command was introduced.

Usage Guidelines

To get events logging pseudowire status needs to enable *pw-status*. To get events logging pseudowire redundancy needs to enable *redundancy*.

Example for pseudowire status events logging

This example shows how to enable L2VPN pseudowire status events logging.

```
DmSwitch#config
DmSwitch(config)#mpls l2vpn logging pw-status
DmSwitch(config)#exit
DmSwitch#
```

Example for pseudowire redundancy events logging

This example shows how to enable L2VPN redundancy events logging.

```
DmSwitch#config
DmSwitch(config)#mpls l2vpn logging redundancy
DmSwitch(config)#exit
DmSwitch#
```

By default the L2VPN events logging pseudowire status and redundancy are enabled. You can verify whether events logging are enabled by entering the command **show running-config**.

Once enabled you can view L2VPN events logging messages through the command **show log ram**.

```
DmSwitch#show log ram
Apr 12 09:17:03 DM4001-16 : [Master] <5> Interface Ethernet 1/4 changed state to up
Apr 12 09:17:07 DM4001-16 : [Master] <5> Interface Ethernet 1/3 changed state to up
Apr 12 09:17:23 DM4001-16 : [Master] <5> Redundancy vpn 1701: Activating primary pw 70
Nbr 200.200.200.1
Apr 12 09:17:23 DM4001-16 : [Master] <5> MPLS L2VPN : Neighbor 200.200.200.1 (PWID 70),
on VPN 1701, changed state to UP
Apr 12 09:17:38 DM4001-16 : [Master] <5> MPLS L2VPN : Neighbor 200.200.200.3 (PWID 1500),
on VPN 1500, changed state to UP
Apr 12 09:18:02 DM4001-16 : [Master] <5> MPLS L2VPN : Neighbor 200.200.200.3 (PWID 1600),
on VPN 1600, changed state to UP
Apr 12 09:18:02 DM4001-16 : [Master] <5> MPLS L2VPN : Neighbor 200.200.200.3 (PWID 80),
on VPN 1701, changed state to UP
Apr 12 09:19:06 DM4001-16 : [Master] <5> Interface Ethernet 1/4 changed state to down
(shutdown)
Apr 12 09:19:43 DM4001-16 : [Master] <5> MPLS L2VPN : Neighbor 200.200.200.1 (PWID 70),
on VPN 1701, changed state to DOWN
Apr 12 09:19:43 DM4001-16 : [Master] <5> Redundancy vpn 1701: Activating standby pw 80
Nbr 200.200.200.3
DmSwitch#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show log ram	Shows log messages.

mpls rsvp ^[1] ^[3] ^[6]

mpls rsvp

Description

Enters on RSVP global configuration mode.

Syntax

No parameter accepted.

Default

No default is defined.

Command Mode

Privileged EXEC.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to enter in RSVP Global Configuration Mode.

```
DmSwitch#configure
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#
```

Related Commands

Command	Description
rsvp enable	Enables RSVP protocol
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

mpls rsvp logging

```
mpls rsvp logging { tunnel-status }
```

```
no mpls rsvp logging { tunnel-status }
```

Description

Enable events logging RSVP tunnel status (up/down).

Inserting **no** as a prefix for this command will disable RSVP event logging.

Syntax

No parameters accepted.

Default

RSVP events logging enabled.

Command History

Release	Modification
14.10	This command was introduced.

Usage Guidelines

This command enables or disables the RSVP events logging. A message is logged when the tunnel goes up or goes down.

The log can be viewed through the command **show log ram**.

Example

This example shows how to enable the RSVP events logging.

```
DmSwitch(config)#mpls rsvp logging tunnel-status
DmSwitch(config)#
```

By default the RSVP events logging is enabled. You can verify whether events logging is enabled by entering the command **show running-config**.

Once enabled you can view RSVP events logging messages through the command **show log ram**.

```
DmSwitch#show log ram
Apr 12 09:51:38 DM4001-16 : [Master] <5> RSVP-ADJCHG - Tunnel (20) to destination
200.200.200.3 is UP
```

```
Apr 12 09:54:27 DM4001-16 : [Master] <5> Interface Ethernet 1/3 changed state to down
(shutdown)
Apr 12 09:54:27 DM4001-16 : [Master] <5> RSVP-ADJCHG - Tunnel (20) to destination
200.200.200.3 is DOWN
DmSwitch#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show log ram	Shows log messages.

mpls te ^[1] ^[3] ^[6]

mpls te

Description

Enters on Traffic Engineering (TE) Configuration Mode in order to configure RSVP tunnels.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to enter on the Traffic Engineering Mode.

```
DmSwitch(config)#  
DmSwitch(config)#mpls te  
DmSwitch(config-mpls-te)#
```

Related Commands

Command	Description
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel name	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity

Command	Description
<code>tunnel mpls traffic-eng autoroute announce</code>	Configures RSVP tunnel to be announced into IGP
<code>tunnel mpls traffic-eng autoroute metric</code>	Configures the autoroute metric
<code>tunnel mpls traffic-eng bandwidth bw_value</code>	Configures the bandwidth associated to the RSVP tunnel
<code>tunnel mpls traffic-eng bypass</code>	Configures the RSVP Tunnel as a bypass tunnel
<code>tunnel mpls traffic-eng fast-reroute</code>	Enables the creation of alternative paths for Fast-Reroute
<code>tunnel mpls traffic-eng path-option po_number explicit identifier ei_number</code>	Configures the path-option index and the explicit path identifier
<code>tunnel mpls traffic-eng record-route</code>	Enables the Record-Route Object
<code>shutdown</code>	Disables administratively an RSVP tunnel
<code>show mpls rsvp</code>	Show counters of RSVP messages
<code>show mpls te traffic-eng tunnels</code>	Shows Traffic Engineering Tunnel Information

mpls vpws ^[1] ^[3] ^[6]

mpls vpws

Description

Enables VPWS configuration mode.

Syntax

Parameter	Description
-----------	-------------

No parameters are defined.

Default

No default is defined.

Command Modes

VPWS configuration.

Command History

Release	Modification
---------	--------------

9.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To use this command, the equipment must support MPLS feature.

Example

This example shows how to entry in vpws configuration mode.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-vpws)#
```

Related Commands

No related command.

mpls vpls ^[1] ^[3] ^[6]

mpls vpls

Description

Enables VPLS configuration mode.

Syntax

Parameter	Description
-----------	-------------

No parameters are defined.

Default

No default is defined.

Command Modes

VPLS configuration.

Command History

Release	Modification
---------	--------------

9.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To use this command, the equipment must support MPLS/VPLS feature.

Example

This example shows how to entry in vpls configuration mode.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#
```

Related Commands

No related command.

mpls vpls mac-address limit global ^[1] ^[3] ^[6]

```
mpls vpls mac-address limit global number
```

```
no mpls vpls mac-address limit global
```

Description

Set the global default mac-address limit for VPLS VPNs.

Inserting **no** as prefix for this command will unset the global default mac-address limit for VPLS VPNs.

Syntax

Parameter	Description
<i>number</i>	The global default mac-address limit for the current VPLS VPN.(Range: It has board and external memory dependencies)

Default

Global limit is defined 1024.

Command Modes

Global configuration.

Command History

Release	Modification
10.0	The global default mac-address limit value for VPLS VPN's was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS/VPLS feature. This command set the global default value for mac-address limit when a VPLS VPN is created.

If the specific mac-address limit command is executed inside VPN configuration, that value overrides this global one.

If the global default mac-addres limit is not set and and the specfic mac-addres limit is not set in VPN configuration too, the mac-address limit for VPLS VPNs is shared with total L2 table.

Example

This example shows how to set the mac-address limit for the VPLS VPN.

```
DmSwitch(config)#mpls vpls mac-address limit global 200
DmSwitch(config)#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

mpls audit l2vpn ^[1] ^[3] ^[6]

```
mpls audit l2vpn { guard-time | interval-time } seconds
```

```
mpls audit l2vpn { enable | disable }
```

```
no mpls audit l2vpn
```

Description

MPLS audit to L2VPN allows scheduling checks over MPLS L2VPN's configured on system after some events over the system. These events could be network changes, unit reboots and redundancy switchover.

Inserting **no** as a prefix for this command will revert the configuration to the default value.

Syntax

Parameter	Description
guard-time	Set a delay time on audit, to avoid immediately start after a event occurrence.
interval-time	Configure the interval time between audit executions.
enable	Enable audit to work.
disable	Disable audit functionality, but preserve configurations.

Default

MPLS audit L2VPN is disabled by default. The default value for guard-time is 7200 seconds and for interval-time is 15 seconds.

Command Modes

Global configuration.

Command History

Release	
13.0	This command was introduced.

Usage Guidelines

The MPLS audit L2VPN provides scheduling of periodic audits to correct possible hardware inconsistencies presents on installed MPLS L2VPNs. This audits are carried out based on the values of *guard-time* and *interval-time*, which control the initial delay after event ocurrence and the interval between audits respectively.

Example of MPLS Audit L2VPN configuration

This example shows how to configure MPLS audit L2VPN.

```
DmSwitch#config
DmSwitch(config)#mpls audit l2vpn guard-time 60
DmSwitch(config)#mpls audit l2vpn interval-time 10
DmSwitch(config)#mpls audit l2vpn enable
DmSwitch(config)#exit
DmSwitch#
```

Example for disable MPLS Audit L2VPN functionality

This example shows how to disable MPLS Audit L2VPN

```
DmSwitch#config
DmSwitch(config)#mpls audit l2vpn disable
DmSwitch(config)#exit
DmSwitch#
```

This commands disable audit functionality, but preserve configurations.

Example for unconfigure MPLS Audit L2VPN

This example shows how to unconfigure MPLS Audit L2VPN

```
DmSwitch#config
DmSwitch(config)#no mpls audit l2vpn
DmSwitch(config)#exit
DmSwitch#
```

This command will revert the configuration to the default values.

Related Commands

Command	Description
show mpls audit l2vpn	Shows the status of MPLS audit L2VPN.
show running-config	Shows the current operating configuration.

mvr

```
mvr { source-vlan vlan-number | group-range { ip ip-address | ipv6 ipv6-address } }
```

```
no mvr [ group-range { ip | ipv6 } ]
```

Description

Configures the Multicast Vlan Registration protocol. Its possible to replicate multicast traffic from a source vlan to a previously configured receiver vlan

Inserting **no** as a prefix for this command will disable the MVR and reset parameters to the default value or delete the MVR Group Range IPs.

Note: Packets must have TTL greater than 2 in order to be replicated to destination VLAN.

Syntax

Parameter	Description
source-vlan <i>vlan-number</i>	Enables the MVR Source Vlan.
group-range ip <i>ip-address</i>	Sets the IP range of Multicast Group used by the MVR.
group-range ipv6 <i>ipv6-address</i>	Sets the IPv6 range of Multicast Group used by the MVR.

Default

MVR is disabled

Command Modes

Global configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The MVR allows to configure a VLAN as a source of multicast traffic data and replicates it to the receivers VLANs. Its also possible to limit a range of multicast groups set in MVR.

To avoid replicating toward a traffic source a VLAN can be configured as source or receiver but never both. Furthermore, a port cannot belong at the same time to the source and receiver VLANs.

Example

This example shows how to enable MVR source vlan.

```
DmSwitch(config)#mvr source-vlan 580
DmSwitch(config)#
```

You can verify that the MVR was enabled by entering the **show running-config** command.

This example shows how to set the MVR to acts only in given multicast group range.

```
DmSwitch(config)#mvr group-range ip 224.0.0.0/8
DmSwitch(config)#
```

You can verify that the MVR was set by entering the **show running-config** command.

Related Commands

Command	Description
mvr receiver	Sets a VLAN as receiver of multicast traffic from Multicast Vlan Registration protocol.

network-policy

network-policy profile *profile-number*

no network policy { **all** | **profile** *profile-number* }

Description

Enters on Network Policy configuration mode.

Syntax

Parameter	Description
profile <i>profile-number</i>	Enters on a specific profile configuration mode. Inserting no as a prefix, removes a specific profile.
all	Remove all profiles.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enter on configuration mode for network policy profile 1.

```
DmSwitch#network-policy profile 1
DmSwitch(config-net-pol-prof) #
```

You can verify that the information was configured by entering the **show network-policy** in the new prompt.

Related Commands

Command	Description
<code>voice vlan</code>	Configure Voice VLAN feature.
<code>voice-signaling vlan</code>	Configure Voice-Signaling VLAN feature.
<code>show network-policy</code>	Shows Network Policy settings.
<code>network-policy mac-list</code>	Configure Network Policy MAC List settings.
<code>show running-config</code>	Shows the current operating configuration.

network-policy mac-list

```
network-policy mac-list
```

```
entry entry-number address mac-address mask mac-address-mask [ description text
```

```
no entry { all | entry-number }
```

Description

Configure Network Policy MAC List settings.

Syntax

Parameter	Description
network-policy mac-list	Enters on Network Policy MAC List configuration mode.
entry <i>entry-number</i>	Specify an index in the network-policy MAC list
address <i>mac-address</i>	Specify MAC address of entry
mask <i>mac-address</i>	Specify MAC address mask of entry
description <i>text</i>	Specify an optional description for this entry

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

It is possible to configure a network-policy profile that associates traffic from a given MAC address range to a specific VLAN and 802.1p priority to implement Voice VLANs.

First, a network-policy profile must be created and associated with MAC list:

```
DmSwitch#network-policy profile 1
```

```
DmSwitch(config-net-pol-prof)#voice-vlan 1983 cos 7 mac-list
```

Then it is necessary to configure a list of ranges of MAC addresses from which traffic will be associated with that profile. The MAC address range is usually specified to match the OUI of vendors of VoIP phones, but is also possible to use an arbitrary pair of MAC address and mask.

```
DmSwitch(config)#network-policy mac-list
DmSwitch(config-net-pol-mac-list)#entry 1 address 00:04:DF:00:00:00 mask FF:FF:FF:00:00:00 description Grandst
```

Finally, the created profile must be associated with the Ethernet interfaces where that traffic is expected.

```
DmSwitch(config)#interface ethernet all
DmSwitch(config-if-eth-1/1-to-1/24)#network-policy profile 1
```

Now all incoming traffic whose source MAC address is 00:04:DF:XX:XX:XX will be associated with VLAN 1983 and 802.1p priority 7.

Example

This example shows how to enter on configuration mode for network policy profile 1.

```
DmSwitch#network-policy profile 1
DmSwitch(config-net-pol-prof)#
```

You can verify that the information was configured by entering the **show network-policy** in the new prompt.

Related Commands

Command	Description
voice vlan	Configure Voice VLAN feature.
voice-signaling vlan	Configure Voice-Signaling VLAN feature.
show network-policy	Shows Network Policy settings.
show running-config	Shows the current operating configuration.

openflow

openflow

no openflow

Description

Enables global OpenFlow on the router and enter OpenFlow configuration mode.

The **no** command removes the global OpenFlow configuration from the router.

Syntax

To enable global OpenFlow no additional parameter is needed, but to work properly, some additional configurations must be inserted.

Default

Global OpenFlow protocol is not enabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

This command must be used in global Configuration mode.

Example

This example shows how to enable global OpenFlow on the router.

```
DmSwitch(config)#openflow
DmSwitch(config)#
```

You can verify if global OpenFlow is enabled by entering the **show openflow** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
show openflow	Shows global OpenFlow configuration.
clear-flows	Clear all OpenFlow flows.
controller	Configure OpenFlow controller.
filter-group-prio	Reserve a Filter Group Priority for OpenFlow.
mode	Configure OpenFlow mode.
native-vlan	Configure the OpenFlow native vlan.
rem-ssl-file	Remove certificate files used by OpenFlow when connecting to a controller using SSL.
strip-fcs	Enables the strip of FCS (Frame Check Sequence) from OpenFlow packets.

port-channel nuc-load-balance ^[1]

```
port-channel nuc-load-balance { dst-addr | src-addr | src-dst-ip | src-port }
```

```
no port-channel nuc-load-balance
```

Description

Configures non-unicast load distribution method in port channels.

Inserting **no** as a prefix for this command will return to default configuration.

Syntax

Parameter	Description
dst-addr	Uses destination MAC address.
src-addr	Uses source MAC address.
src-dst-ip	Uses source or destination IP address.
src-port	Uses source port.

Command Modes

Global configuration.

Command History

Release	Modification
7.6	This command was introduced.
13.8.4	Option src-dst-ip was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a non-unicast load distribution method.

```
DmSwitch(config)#port-channel nuc-load-balance dst-addr
DmSwitch(config)#
```

You can verify that the configuration was created by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ptp unit domain

```
ptp unit { all | unit-number | { range first-unit-number last-unit-number } } domain  
domain-id
```

```
no ptp unit { all | unit-number | range { first-unit-number last-unit-number } }  
domain
```

Description

Configure PTP domain or set default value if "no" is given.

Syntax

Parameter	Description
all	Configure PTP domain for all units.
<i>unit-number</i>	Configure PTP domain for a specific unit.
range <i>first-unit-number last-unit-number</i>	Configure PTP domain for a range of specific units.
domain <i>domain-id</i>	Specify PTP domain id. (Range: 0-127)

Default

By default it is used domain 0.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

PTP must be disabled before domain configuration, otherwise an error message is displayed.

Example

This example show how set ptp to use domain 4.

```
DM4000(config)#ptp unit 1 domain 4
```

You can verify that the configuration was well done by entering the **show ptp unit 1**

Related Commands

Command	Description
<code>show ptp unit</code>	Shows precision time protocol information of an unit.

ptp unit enable

```
[ no ] ptp unit { all | unit-number | { range first-unit-number last-unit-number } }  
enable
```

Description

Enable precision time protocol or disable it if "no" is given.

Syntax

Parameter	Description
all	Enables PTP for all units.
<i>unit-number</i>	Enables PTP for a specific unit.
range <i>first-unit-number last-unit-number</i>	Enables PTP for a range of specific units.

Default

By default, global PTP is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Some coherency are checked when this command is used. To set up some other PTP configurations it must be disabled, otherwise a message is displayed: "Interface is enabled. Please disable before changing this parameter". If "no" is used, it configures the default value, which is global PTP disabled.

Example

This example show how to enable ptp at unit 1.

```
DM4000(config)#ptp unit 1 enable
```

You can verify that the configuration was well done by entering the **show ptp unit 1**

Related Commands

Command	Description
<code>show ptp unit</code>	Shows precision time protocol information of an unit.

ptp unit mode

```
ptp unit { all | unit-number | { range first-unit-number last-unit-number } } mode { {  
ordinary { master | slave } } | boundary }
```

```
no ptp unit { all | unit-number | range { first-unit-number last-unit-number } } mode
```

Description

Configure precision time protocol mode of operation.

Syntax

Parameter	Description
all	Set mode for all units.
<i>unit-number</i>	Set mode for a specific unit.
range <i>first-unit-number last-unit-number</i>	Set mode for a range of specific units.
mode ordinary { <i>master</i> <i>slave</i> }	Select PTP as ordinary master or slave clock device.
mode boundary	Select PTP as boundary clock device.

Default

By default PTP work on **ordinary master** mode.

Command Modes

Global configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

PTP must be disabled to set up this configuration.

Example

This example show how to set unit 1 to use ptp as ordinary slave.

```
DM4000(config)#ptp unit 1 mode ordinary slave
```

You can verify that the configuration was well done by entering the **show ptp unit 1**

Related Commands

Command	Description
<code>show ptp unit</code>	Shows precision time protocol information of an unit.

queue cos-map

```
queue cos-map { queue-id priority 1st_queue_prio } [ 2nd_queue_prio ... 8th_queue_prio ]
```

```
no queue cos-map
```

Description

Configure the map of CoS priorities to queues.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
<i>queue-id</i>	Selects a meter to edit by ID
priority <i>1st_queue_prio</i>	1st CoS Priority of 8 possible
<i>2nd_queue_prio</i>	2nd CoS Priority of 8 possible
...	...
<i>8th_queue_prio</i>	8th CoS Priority of 8 possible

Default

Queue	802.1P Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced. Before this was called qos cos-map .

Usage Guidelines

Not available.

Example

This example shows how to map CoS priorities 0, 3 and 6 to queue 5.

```
DmSwitch(config)#queue cos-map 5 priority 0 3 6
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue cos-map** privileged EXEC command.

Related Commands

Command	Description
show queue cos-map	Shows priority mappings
queue max-bw	Configures the maximum bandwidth allocation per queue
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
show running-config	Shows the current operating configuration.

radius-server acct-port

radius-server acct-port *port-number*

no radius-server acct-port

Description

Configures the default RADIUS server accounting port.

Inserting **no** as a prefix for this command will return to the default port number.

Syntax

Parameter	Description
<i>port-number</i>	Specifies the port number. (Range: 1-65535)

Default

Port number: 1813.

Command Modes

Global Configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

The accounting by a RADIUS server uses this default server port if no port is configured to a specific RADIUS host.

Example

This example shows how to change the default RADIUS accounting port number.

```
DmSwitch(config)#radius-server acct-port 6500
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server key</code>	Configures the default RADIUS server key string.
<code>radius-server retries</code>	Configures the RADIUS server retries.
<code>radius-server timeout</code>	Configures the RADIUS server timeout.
<code>show running-config</code>	Shows the current operating configuration.
<code>show radius-server</code>	Shows RADIUS server information.

radius-server auth-port

radius-server auth-port *port-number*

no radius-server auth-port

Description

Configures the default RADIUS server authentication port.

Inserting **no** as a prefix for this command will return to the default port number.

Syntax

Parameter	Description
<i>port-number</i>	Specifies the port number. (Range: 1-65535)

Default

Port number: 1812.

Command Modes

Global Configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

The authentication login by a RADIUS server uses this default server port if no port is configured to a specific RADIUS host.

Example

This example shows how to change the default RADIUS authentication port number.

```
DmSwitch(config)#radius-server auth-port 6500
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>radius-server acct-port</code>	Configures the default RADIUS server accounting port.
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server key</code>	Configures the default RADIUS server key string.
<code>radius-server retries</code>	Configures the RADIUS server retries.
<code>radius-server timeout</code>	Configures the RADIUS server timeout.
<code>show running-config</code>	Shows the current operating configuration.
<code>show radius-server</code>	Shows RADIUS server information.

radius-server host

```
radius-server host index { accounting | acct-port acct-port-number |  
authentication | auth-port auth-port-number | address ip-address | key key-text |  
source-iface { loopback number | vlan number } }
```

```
no radius-server host index [ accounting | authentication | source-iface ]
```

Description

Configures a specific RADIUS server.

Inserting **no** as a prefix for this command will remove the configuration for the specified host.

Syntax

Parameter	Description
<i>index</i>	Specifies the server index. (Range: 1-5)
accounting	Enables RADIUS accounting.
acct-port	Specifies RADIUS server accounting port.
<i>acct-port-number</i>	Specifies the server accounting port number. (Range: 1-65535)
authentication	Enables RADIUS authentication.
auth-port	Specifies RADIUS server authentication port.
<i>auth-port-number</i>	Specifies the RADIUS server port number. (Range: 1-65535)
address	Specifies RADIUS server IPv4/IPv6 address.
<i>ip-address</i>	Specifies the server IP address.
key	Specifies RADIUS server key.
<i>key-text</i>	Specifies the server key string.
source-iface	Specifies the RADIUS source interface.
loopback <i>number</i>	Select loopback interface as source address. (Range: 1-4094)
vlan <i>number</i>	Select VLAN interface as source address. (Range: 0-7)

Default

No host is configured.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.

Release	Modification
6.6	The option source-iface was introduced.
13.4	IPv6 address option was introduced.

Usage Guidelines

It configures the IP address, port and key for authentication and accounting in a specific RADIUS server.

It is possible to define until five RADIUS hosts.

Example

This example shows how to define a RADIUS server.

```
DmSwitch(config)#radius-server host 1 address 10.10.50.70
DmSwitch(config)#radius-server host 1 auth-port 4050
DmSwitch(config)#radius-server host 1 authentication
DmSwitch(config)#radius-server host 1 key key_for_this_host
DmSwitch(config)#radius-server host 1 acct-port 4051
DmSwitch(config)#radius-server host 1 accounting
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
authentication login	Defines the login authentication method and its precedence.
radius-server acct-port	Configures the default RADIUS server accounting port.
radius-server auth-port	Configures the default RADIUS server authentication port.
radius-server key	Configures the default RADIUS server key string.
radius-server retries	Configures the RADIUS server retries.
radius-server timeout	Configures the RADIUS server timeout.
show running-config	Shows the current operating configuration.
show radius-server	Shows RADIUS server information.

radius-server key

radius-server key *key-text*

no radius-server key

Description

Configures the default RADIUS server key string.

Inserting **no** as a prefix for this command will remove the configured key.

Syntax

Parameter	Description
<i>key-text</i>	Specifies the key string.

Default

No key is configured.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The authentication login by a RADIUS server uses this default server key if no key string is configured to a specific RADIUS host.

Example

This example shows how to define the default RADIUS key string.

```
DmSwitch(config)#radius-server key this_is_a_test
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>radius-server acct-port</code>	Configures the default RADIUS server accounting port.
<code>radius-server auth-port</code>	Configures the default RADIUS server authentication port.
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server retries</code>	Configures the RADIUS server retries.
<code>radius-server timeout</code>	Configures the RADIUS server timeout.
<code>show running-config</code>	Shows the current operating configuration.
<code>show radius-server</code>	Shows RADIUS server information.

radius-server retries

radius-server retries *retries*

no radius-server retries

Description

Configures the RADIUS server retries.

Inserting **no** as a prefix for this command will return to the default retries value.

Syntax

Parameter	Description
<i>retries</i>	Specifies the server retries. (Range: 1-5)

Default

Retries: 2.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

It defines the number of login attempts in the RADIUS server.

Example

This example shows how to change the RADIUS server retries.

```
DmSwitch(config)#radius-server retries 1
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>radius-server acct-port</code>	Configures the default RADIUS server accounting port.
<code>radius-server auth-port</code>	Configures the default RADIUS server authentication port.
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server key</code>	Configures the default RADIUS server key string.
<code>radius-server timeout</code>	Configures the RADIUS server timeout.
<code>show running-config</code>	Shows the current operating configuration.
<code>show radius-server</code>	Shows RADIUS server information.

radius-server timeout

radius-server timeout *timeout*

no radius-server timeout

Description

Configures the RADIUS server timeout.

Inserting **no** as a prefix for this command will return to the default timeout value.

Syntax

Parameter	Description
<i>timeout</i>	Specifies the server timeout (in seconds). (Range: 1-65535)

Default

Timeout: 5.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

It defines the number of login attempts in the RADIUS server.

Example

This example shows how to change the RADIUS server timeout.

```
DmSwitch(config)#radius-server timeout 10
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>radius-server acct-port</code>	Configures the default RADIUS server accounting port.
<code>radius-server auth-port</code>	Configures the default RADIUS server authentication port.
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server key</code>	Configures the default RADIUS server key string.
<code>radius-server retries</code>	Configures the RADIUS server retries.
<code>show running-config</code>	Shows the current operating configuration.
<code>show radius-server</code>	Shows RADIUS server information.

remote-devices devices-vlan

remote-devices devices-vlan *vlan-id ip ipaddress/mask*

no remote-devices devices-vlan

Description

Configure a VLAN to manage remote devices locally.

Inserting **no** as a prefix for this command will clear VLAN's created to manage remote devices.

Syntax

Parameter	Description
<i>vlan-id</i>	Specifies the vlan id. (Range: 1-4094)
ip	Configures an IP address to manage remote devices.
<i>ipaddress/mask</i>	Specifies the ip address/mask. (mask: /16)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a VLAN and a IP address to manage remote devices.

```
DmSwitch(config)#remote-devices devices-vlan 3 ip 192.163.255.254/16
DmSwitch(config)#
```

You can verify that the VLAN was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>remote-devices enable</code>	Enable remote devices management.
<code>remote-devices force</code>	Force configuration of remote devices with configuration conflict.
<code>remote-devices rate-limit</code>	Configure maximum number of packets per second sent to remote devices.
<code>remote-devices service</code>	Configure services available on remote devices.
<code>show remote devices</code>	Remote device management configuration and status.
<code>show running config</code>	Shows the current operating configuration.

remote-devices enable

```
remote-devices enable [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no remote-devices enable
```

Description

Enable remote devices management.

Inserting **no** as a prefix for this command will disable remote devices management.

Syntax

Parameter	Description
all	Enables for all ports.
[unit-number/] port-number	Enables for a specific unit and port. (Range:1-1/1-28)
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Enables for a range of specific units and ports. (Range:1-1/1-28)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable remote devices management to unit 1 port ethernet 1.

```
DmSwitch(config)#remote-devices enable ethernet 1/1
```

```
DmSwitch(config)#
```

You can verify that the remote devices management was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
remote-devices devices-vlan	Configure a VLAN to manage remote devices locally.
remote-devices force	Force configuration of remote devices with configuration conflict.
remote-devices rate-limit	Configure maximum number of packets per second sent to remote devices.
remote-devices service	Configure services available on remote devices.
show remote devices	Remote device management configuration and status.
show running config	Shows the current operating configuration.

remote-devices force

`remote-devices force`

`no remote-devices force`

Description

Force configuration of remote devices with configuration conflict.

Inserting **no** as a prefix for this command will not force configuration of remote devices with configuration conflict.

Syntax

No parameter accepted.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to force configuration of remote devices with configuration conflict.

```
DmSwitch(config)#remote-devices force
DmSwitch(config)#
```

You can verify that the force configuration was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
remote-devices devices-vlan	Configure a VLAN to manage remote devices locally.
remote-devices enable	Enable remote devices management.

Command	Description
<code>remote-devices rate-limit</code>	Configure maximum number of packets per second sent to remote devices.
<code>remote-devices service</code>	Configure services available on remote devices.
<code>show remote devices</code>	Remote device management configuration and status.
<code>show running config</code>	Shows the current operating configuration.

remote-devices rate-limit

remote-devices rate-limit *packets/seconds*

no remote-devices rate-limit

Description

Configure maximum number of packets per second sent to remote devices.

Inserting **no** as a prefix for this command will reset maximum number of packets per second sent to remote devices.

Syntax

Parameter	Description
<i>packets/seconds</i>	Packets per second sent to remote devices. (Range: 10-10000)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a maximum number of 100 packets per second to send for remote devices.

```
DmSwitch(config)#remote-device rate-limit 100
DmSwitch(config)#
```

You can verify that the rate-limit was configured by entering the **show remote-devices** privileged EXEC command.

Related Commands

Command	Description
remote-devices devices-vlan	Configure a VLAN to manage remote devices locally.
remote-devices enable	Enable remote devices management.
remote-devices force	Force configuration of remote devices with configuration conflict.
remote-devices service	Configure services available on remote devices.
show remote devices	Remote device management configuration and status.
show running config	Shows the current operating configuration.

remote-devices service

```
remote-devices service index { tcp port-number | udp port-number }
```

```
no remote-devices service index
```

Description

Configure services available on remote devices.

Inserting **no** as a prefix for this command will delete service index.

Syntax

Parameter	Description
<i>index</i>	Service index. (Range: 1-20)
tcp <i>port-number</i>	TCP port number. (Range: 1-1024)
udp <i>port-number</i>	UDP port number. (Range: 1-1024)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a service available on remote devices.

```
DmSwitch(config)#remote-device service 1 tcp 100
DmSwitch(config)#
```

You can verify that the service was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>remote-devices devices-vlan</code>	Configure a VLAN to manage remote devices locally.
<code>remote-devices enable</code>	Enable remote devices management.
<code>remote-devices force</code>	Force configuration of remote devices with configuration conflict.
<code>remote-devices rate-limit</code>	Configure maximum number of packets per second sent to remote devices.
<code>show remote devices</code>	Remote device management configuration and status.
<code>show running config</code>	Shows the current operating configuration.

rmon

```
rmon [ alarm { parameters } | event { parameters } ]
```

```
no rmon [ alarm { parameters } | event { parameters } ]
```

Description

Configures an RMON.

Inserting **no** as a prefix for this command will remove the specified RMON configuration.

Syntax

Parameter	Description
alarm <i>parameters</i>	Configures an RMON alarm. Click here to see the alarm parameters description.
event <i>parameters</i>	Configures an RMON event. Click here to see the event parameters description.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to remove all RMON configuration for the switch.

```
DmSwitch(config)#no rmon
DmSwitch(config)#
```

You can verify that all RMON configuration was removed by entering the **show running-config** privileged EXEC command.

Related Commands

No related command.

rmon alarm

```
rmon alarm index oid-variable sample-interval { absolute | delta } { rising-threshold  
value } { [ event-number ] falling-threshold value } [ event-number ] [ owner string ]
```

```
no rmon alarm index
```

Description

Configures an RMON alarm.

Inserting **no** as a prefix for this command will removes the specified RMON alarm.

Syntax

Parameter	Description
<i>index</i>	Specifies the RMON alarm index. (Range: 1-65535)
<i>oid-variable</i>	Specifies the MIB object to monitor.
<i>sample-interval</i>	Specifies the interval to monitor.
absolute	Tests each MIB variable directly.
delta	Tests the change between samples of a MIB variable.
rising-threshold <i>value</i>	Specified the rising threshold value. (Range: -2147483648 - 2147483648)
falling-threshold <i>value</i>	Specified the falling threshold value. (Range: -2147483648 - 2147483648)
<i>event-number</i>	Specifies the event number to trigger when the rising or falling threshold exceeds its limit.
owner <i>string</i>	Specifies the owner of the alarm.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

You can set an alarm on any MIB object. The specified MIB must be an existing SNMP MIB object in standard dot notation (.1.3.6.1.2.1.2.2.1.14.5 for ifInErrors.5). The falling threshold must be lower than the rising threshold.

Example

This example shows how to configure a RMON alarm index 1 that monitors the MIB variable ifInErrors.5 once every 30 seconds. If the ifInErrors.5 increase 10 or more, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the RMON event command. If the MIB value changes by 0, the alarm is reset and can be triggered again.

```
DmSwitch(config)#rmon alarm 1 .1.3.6.1.2.1.2.2.1.14.5 30 delta rising-threshold 10 1
falling-threshold 0 owner test
DmSwitch(config)#
```

You can verify that the RMON alarm was configured by entering the **show rmon alarm** privileged EXEC command.

Related Commands

Command	Description
rmon	Configures an RMON.
rmon collection history	Configures a RMON history group of statistics.
rmon collection stats	Configures a RMON collection of statistics.
rmon event	Configures an RMON event.
show rmon alarm	Shows the RMON alarm table.
show rmon event	Shows the RMON event table.
show rmon history	Shows the RMON history table.
show running-config	Shows the current operating configuration.
show rmon statistics	Shows the RMON statistics table.

rmon event

rmon event *index* [**batch** *index*] [**description** *string*] [**log**] [**owner** *string*] [**trap** *community*]

no rmon event *index*

Description

Configures an RMON event.

Inserting **no** as a prefix for this command will remove the specified RMON event.

Syntax

Parameter	Description
<i>index</i>	Specifies the RMON event index. (Range: 1-65535)
batch <i>index</i>	(Optional) Specifies a batch to be executed when the event is triggered. (Range: 1-16)
description <i>string</i>	(Optional) Specifies a description of the event.
log	(Optional) Generates an RMON log entry when the event is triggered.
owner <i>string</i>	(Optional) Specifies the owner of the event.
trap <i>community</i>	(Optional) Generates a trap when the event is triggered using the specified community.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a RMON event index 1 to define HighErrors. The event generates a log entry and a SNMP trap when the event is triggered by the alarm. The commands specified in batch 1 are executed in background when the event is triggered.

```
DmSwitch(config)#rmon event 1 description HighErrors log trap eventtrap batch 1 owner test
DmSwitch(config)#
```

You can verify that the RMON alarm was configured by entering the **show rmon event** privileged EXEC command.

Related Commands

Command	Description
rmon	Configures an RMON.
rmon alarm	Configures an RMON alarm.
rmon collection history	Configures a RMON history group of statistics.
rmon collection stats	Configures a RMON collection of statistics.
show rmon alarm	Shows the RMON alarm table.
show rmon event	Shows the RMON event table.
show rmon history	Shows the RMON history table.
show running-config	Shows the current operating configuration.
show rmon statistics	Shows the RMON statistics table.

route-map

```
route-map tag { deny number | permit number }
```

```
no route-map tag { deny number | permit number }
```

Description

Create route-map and/or enter route-map command mode.

Inserting **no** as a prefix for this command will delete the route map.

Syntax

Parameter	Description
<i>tag</i>	Specifies a route map tag.
deny	Specifies route map denies set operations.
permit	Specifies route map permits set operations.
<i>number</i>	Specifies sequence to insert to route-map entry. (Range: 1-65535)

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add a route-map named tag.

```
DmSwitch(config)#route-map tag permit 1
```

```
DmSwitch(config-route-map)#
```

You can verify that route-map was added by entering the **show runnig-config** privileged EXEC command.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running config	Shows the current operating configuration.

router bgp

```
router bgp AS
```

```
router bgp [AS]
```

```
no router bgp
```

Description

Enables the BGP process with the specified *AS number* (which can be entered either via *AS_DOT* or *AS_PLAIN* notation - RFC4893 and RFC5396) and provides access to its configuration.

Inserting **no** as a prefix for this command will disable BGP routing process.

Syntax

Parameter	Description
AS	The Autonomous System (AS) number, which can have the size of 32-bits. This is a optional parameter when the BGP AS number is already configured. (Range: 0.1-65535.65535 (AS_DOT) or 1-4294967295 (AS_PLAIN))

Default

BGP process is disabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
10.0	AS size has been increased to 32-bits (AS_DOT and AS_PLAIN notation).
5.0	This command was introduced.

Usage Guidelines

After enabling the BGP process, you can not create different BGP process under different AS number.

Example

This example shows how to enable the protocol, configuring a BGP process for autonomous system 5.100 in *AS_DOT* notation, which corresponds to 327780 in *AS_PLAIN* notation.

```
DmSwitch(config)#router bgp 5.100
DmSwitch(config-router-bgp)#
```

Enter the **show ip bgp** privileged EXEC command to verify if the protocol was enabled.

Related Commands

Command	Description
show_ip_bgp	

router isis

```
router isis area-name
```

```
no router isis area-name
```

Description

Enables the IS-IS process with a specified *area-name* and provides access to its configuration.

Inserting **no** as a prefix for this command will disable IS-IS routing process.

Syntax

Parameter	Description
<i>area-name</i>	Identifies the router IS-IS instance. Area names of up to 12 characters are allowed.

Default

ISIS process is disabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command is used to enable routing for an area. A network entity title (NET) must be configured to specify the area address and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

Example

This example shows how to enable the protocol.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#
```

Enter the **show isis** privileged EXEC command to verify if the protocol was enabled.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
net	Configure the IS-IS network entity title (NET)
show isis	Shows the IS-IS routing table entries.

router ospf

`router ospf`

`no router ospf`

Description

Enables the OSPF process and provides access to its configuration.

Inserting **no** as a prefix for this command will disable OSPF routing process.

Syntax

No parameter accepted.

Default

OSPF process is disabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The OSPF process only act when a network is associated by the **network** router ospf command.

Example

This example shows how to enable the protocol.

```
DmSwitch(config)#router ospf
DmSwitch(config-router-ospf)#
```

Enter the **show ip ospf** privileged EXEC command to verify the protocol was enabled.

Related Commands

No related command.

router ospfv3

```
router ospfv3
```

```
no router ospfv3
```

Description

Enables the OSPFv3 process and provides access to its configuration.

Inserting **no** as a prefix for this command will disable OSPFv3 routing process.

Syntax

No parameter accepted.

Default

OSPFv3 process is disabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The OSPFv3 process only act when a vlan is associated by the **instance-id** vlan ospfv3 command.

Example

This example shows how to enable the protocol.

```
DmSwitch(config)#router ospfv3
DmSwitch(config-router-ospfv3)#
```

Enter the **show ipv6 ospfv3** privileged EXEC command to verify the protocol was enabled.

Related Commands

No related command.

router rip

router rip

no router rip

Description

Enables the RIP process and provides access to its configuration.

Inserting **no** as a prefix for this command will disable RIP routing process.

Syntax

No parameter accepted.

Default

RIP process is disabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The RIP process only act when a network is associated by the **network** router rip command.

Example

This example shows how to enable the protocol.

```
DmSwitch(config)#router rip
DmSwitch(config-router-rip)#
```

Enter the **show ip rip** privileged EXEC command to verify the protocol was enabled.

Related Commands

Command	Description
<code>clear ip rip process</code>	Clear RIP routing data.
<code>default-metric</code>	Defines the default metric of RIP protocol.
<code>distance</code>	Defines the administrative distance of RIP protocol.
<code>network</code>	Associates a network with a RIP routing process.
<code>passive-interface</code>	Suppresses RIP routing updates on specified VLAN interfaces.
<code>redistribute</code>	Redistributes routes with a metric of RIP protocol.
<code>show ip rip</code>	Shows the RIP process parameters.
<code>show ip rip neighbor</code>	Shows RIP neighbors
<code>show running-config</code>	Shows the current operating configuration.
<code>timers basic</code>	Defines the basic timers of RIP protocol.

router ripng

`router ripng`

`no router ripng`

Description

Enables the RIPng process and provides access to its configuration.

Inserting **no** as a prefix for this command will disable RIPng routing process.

Syntax

No parameter accepted.

Default

RIPng process is disabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The RIPng process only act when an interface is associated by the **interface** within the interface vlan or interface loopback command.

Example

This example shows how to enable the protocol.

```
DmSwitch(config)#router ripng
DmSwitch(config-router-ripng)#
```

Enter the **show ipv6 ripng** privileged EXEC command to verify the protocol was enabled.

Related Commands

Command	Description
<code>clear ipv6 ripng process</code>	Clear RIPng routing data.
<code>default-metric</code>	Defines the default metric of RIPng protocol.
<code>distance</code>	Defines the administrative distance of RIPng protocol.
<code>ipv6 ripng</code>	Enable the RIPng routing process on the specified interface.
<code>passive-interface</code>	Suppresses RIPng routing updates on specified VLAN interfaces.
<code>redistribute</code>	Redistributes routes with a metric of RIPng protocol.
<code>show ipv6 ripng</code>	Shows the RIPng process parameters.
<code>show ipv6 ripng database</code>	Shows the RIPng database parameters.
<code>show ipv6 ripng neighbors</code>	Shows the RIPng neighbors parameters.
<code>show running-config</code>	Shows the current operating configuration.
<code>timers basic</code>	Defines the basic timers of RIPng protocol.

sdh-map

```
sdh-map unit [ unit-id ] { new | id xc-id } new | id xc-id { e1c e1c-id | sdh
sdh-id vc4 vc4-id vc12 klm } to { e1c e1c-id | sdh sdh-id vc4 vc4-id vc12 klm
}
```

```
no sdh-map unit unit-id id xc-id
```

Description

Use this command to cross-connect e1c to vc12 or vc12 to vc12.

Syntax

Parameter	Description
new id xc-id	Select on which map index will be configured. If <i>new</i> is selected it will choose the first available index.
e1c e1c-id	Select one e1c for mapping.
sdh sdh-id vc4 vc4-id vc12 klm	Select one vc12 for mapping, which value is given on <i>klm</i> parameter.
no sdh-map unit unit-id id xc-id	Delete the mapping identified by the index <i>xc-id</i> .
no sdh-map unit unit-id all	Delete all mappings on the given unit.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

It's not possible to map one e1c to another. When mapping, both interfaces (e1c or sdh) must be enabled for it properly work. There cannot be two mappings using the same vc12.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to map one vc12 (373) to a elc.

```
DM4000(config)#sdh-map unit 4 new sdh 1 vc4 1 vc12 373 to elc 20
DM4000(config)#
```

You can verify that the command was executed by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show interfaces elc	the Section called <i>show interfaces elc</i> in Chapter 2
show interfaces sdh	Shows sdh interface configuration.
interfaces elc	Enables the interface configuration mode.
interfaces sdh	Enables the interface configuration mode.
show sdh-map	Show the mappings of SDH interfaces.

rpu power-sharing

rpu power-sharing unit *number*

no rpu power-sharing unit *number*

Description

Enable RPU Power Sharing, which allows RPU to supply power to increase PoE power sourcing capabilities.

Inserting **no** as a prefix for this command makes RPU works as backup power source.

Syntax

Parameter	Description
unit <i>number</i>	Enable/Disable RPU power-sharing of the unit specified by number. (Range: 1-8)[1]

Default

Disabled.

Command Modes

User EXEC.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable RPU Power Sharing.

```
DmSwitch#config
DmSwitch(config)#rpu power-sharing unit 1
DmSwitch(config)#
```

You can verify that the RPU Power Sharing is working by inserting an RPU and reserving more power than internal PSU power.

Related Commands

Command	Description
<code>show poe</code>	Shows the PoE current configuration.
<code>poe</code>	Configure interface port to transmit both data and electrical energy.

Notes

[1] - Range 1-8 available only to DM4000 Switches.

sniffer

sniffer *id*

no sniffer *id*

Description

Accesses the sniffer instance.

Inserting **no** as a prefix for this command will reset with default configuration the specified sniffer instance.

Syntax

Parameter	Description
new <i>index</i>	Specifies the sniffer id. (Range: 1-1)

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to access the sniffer instance 1.

```
DmSwitch(config)#sniffer 1
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture files	Shows a list of files containing packet captures.
show capture realtime	Show packets captured in realtime.
accepted	Sets the type of packet (accepted/discarded) being filtered by sniffer.
direction	Sets the direction of the packet to be filtered by sniffer.
enable	Enables the sniffer.
interface-ethernet	Setse an ethernet interface over which packets are filtered by sniffer.
max-packets	Sets the limit of packets to be captured by the sniffer.
protocol	Sets the protocol of the packets to be filtered by sniffer.
show-config	Shows the settings of sniffer.
vlan	Sets a vlan for the sniffer filter.

sntp

```
sntp { client | poll interval | server { ip-address key key-number } | authenticate |  
authentication-key { key-number md5 string } }
```

```
no sntp { client | poll | server ip-address | authenticate | authentication-key key-  
number }
```

Description

Configures the Simple Network Time Protocol.

Inserting **no** as a prefix for this command will disable the SNTP configuration.

Syntax

Parameter	Description
client	Enables the SNTP protocol, accepting time from specified time servers.
poll	Sets the interval at which the client polls for time.
<i>interval</i>	Seconds number of SNTP poll interval. (Range: 16-16384).
server	Specifies a time server.
<i>ip-address</i>	Specifies the IP address.
key	Associates a key to a SNTP server.
<i>key-number</i>	Specifies the key-number. Range(1-4294967295).
authenticate	Enables the authentication feature.
authentication-key	Specifies a key-number.
md5	MD5.
<i>string</i>	String up to eight characters for the key.

Default

SNTP is disabled.

Poll interval: 30 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

You can configure one or more time servers.

Example

This example shows how to changes the poll interval.

```
DmSwitch(config)#sntp poll 10000
DmSwitch(config)#
```

You can verify the SNTP configuration by entering the **show sntp** privileged EXEC command.

Related Commands

Command	Description
show sntp	Shows Simple Network Time Protocol information.
show running-config	Shows the current operating configuration.

spanning-tree

```
spanning-tree { instance [ instance-parameters ] | bpduguard | mode {  
mode-parameters } | mst { mst-parameters } }
```

```
no spanning-tree { instance [ instance-parameters ] | bpduguard | mode {  
mode-parameters } | mst { mst-parameters } }
```

Description

Configures Spanning-tree parameters.

Inserting **no** as a prefix for this command will disable the specified spanning-tree parameters.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
instance-parameters	Specifies the spanning-tree instance parameters. Click here to see the "instance-parameters" description.
bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard. Click here to see the "bpduguard" command description.
mode mode-parameters	Configures the spanning-tree mode. Click here to see the "mode-parameters" description.
mst mst-parameters	Defines parameters of Multiple Spanning-Tree (MST) configuration. Click here to see the "mst-parameters" description.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

Not available.

Example

This example shows how to enable a Spanning-Tree instance.

```
DmSwitch(config)#spanning-tree 1
DmSwitch(config)#
```

You can verify that the instance was enabled by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpduguard	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree bpdufilter

spanning-tree bpdufilter

no spanning-tree bpdufilter

Description

Globally enables Bridge Protocol Data Unit (BPDU) filter for edge ports.

Inserting **no** as a prefix for this command will globally disable the BPDU filter.

Syntax

No parameter accepted.

Default

The BPDU filter is globally disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.
13.0	BPDU filter acting only in edge ports.

Usage Guidelines

The global BPDU filter is used to prevent edge ports from sending BPDUs. Interfaces operating as edge-ports will still send a few BPDUs at link up before start filtering outgoing BPDUs.

If an edge port receives a BPDU, it loses the edge status and global BPDU filter will no longer be applied to that port. Configuring BPDU filter directly in the interface force the feature to be enabled independently from edge configuration.

Example

To globally enable BPDU filter for edge ports:

```
DmSwitch#configure
DmSwitch(config)#spanning-tree bpdufilter
DmSwitch(config)#
```

To verify that BPDU filter was globally enabled:

```
DmSwitch#show spanning-tree configuration
```

```
Spanning-tree information
```

```
-----
Spanning tree mode:      RSTP
BPDU filter status:      Enabled   <==
BPDU guard status:       Disabled
MST name:
MST revision:            0
MST configuration digest: 0xE13A80F11ED0856ACD4EE3476941C73B
```

```
Instance      Protected VLAN groups
-----
1 (RSTP01)    1
```

When a port has edge operation enabled, you can see BPDU filter is active for that interface.

```
DmSwitch#configure
```

```
DmSwitch(config)#interface ethernet 1
```

```
DmSwitch(config-if-eth-1/1)#spanning-tree edge-port
```

```
DmSwitch(config-if-eth-1/1)#show spanning-tree interface ethernet 1
```

```
Eth 1/ 1 information
```

```
-----
Edge port:      admin: enabled, oper: enabled
Link type:      admin: auto, oper: point-to-point
BPDU Filter:    enabled (global)   <==
BPDU Guard:     disabled
Restricted role: disabled
Restricted TCN:  disabled
```

```
DmSwitch#
```

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree bpdupfilter (Interface configuration)	Enables the Bridge Protocol Data Unit (BPDU) filter on the interface.
spanning-tree bpduguard (Interface configuration)	Enables the Bridge Protocol Data Unit (BPDU) guard on the interface.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree bpduguard

spanning-tree bpduguard

no spanning-tree bpduguard

Description

Globally enables Bridge Protocol Data Unit (BPDU) guard for edge ports.

Inserting **no** as a prefix for this command will globally disable the BPDU guard.

Syntax

No parameter accepted.

Default

The BPDU guard is globally disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.
13.0	BPDU guard has lower priority than BPDU filter configured on interface.

Usage Guidelines

The BPDU guard is used to prevent BPDU attacks from spanning-tree edge ports.

If an edge port receives a BPDU when BPDU guard is enabled, that port is administratively disabled.

Configuring BPDU guard on a BPDU filtered interface has no effect. This is not the case when the BPDU filter was enabled only by global configuration.

Example

To globally enable BPDU guard for edge ports:

```
DmSwitch#configure
DmSwitch(config)#spanning-tree bpduguard
DmSwitch(config)#
```

To verify that BPDU guard was globally enabled:

```
DmSwitch#show spanning-tree configuration

Spanning-tree information
-----
Spanning tree mode:          RSTP
BPDU filter status:          Disabled
BPDU guard status:           Enabled   <==
MST name:
MST revision:                0
MST configuration digest:     0xE13A80F11ED0856ACD4EE3476941C73B

Instance      Protected VLAN groups
-----
1 (RSTP01)    1
```

When a port has edge operation enabled, you can see BPDU guard is active for that interface.

```
DmSwitch#configure
DmSwitch(config)#interface ethernet 1
DmSwitch(config-if-eth-1/1)#spanning-tree edge-port
DmSwitch(config-if-eth-1/1)#show spanning-tree interface ethernet 1
Eth 1/ 1 information
-----
Edge port:          admin: enabled, oper: enabled
Link type:          admin: auto, oper: point-to-point
BPDU Filter:        disabled
BPDU Guard:         enabled (global)   <==
Restricted role:     disabled
Restricted TCN:      disabled
DmSwitch#
```

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree bpdupfilter	Enables the Bridge Protocol Data Unit (BPDU) filter.
spanning-tree instance	Configure the default STP BPDU tag mode in the DmSwitch.
bpdu-tag	
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree bpdupfilter (Interface configuration)	Enables the Bridge Protocol Data Unit (BPDU) filter on the interface.
spanning-tree bpduguard (Interface configuration)	Enables the Bridge Protocol Data Unit (BPDU) guard on the interface.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree *instance*

spanning-tree *instance*

spanning-tree *instance* [**forward-delay** *forward-delay-parameters* | **hello-time** *hello-time-parameters* | **max-age** *max-age-parameters* | **max-hops** *max-hops-parameters* | **priority** *priority-parameters* | **root** *root-parameters* | **vlan-group** *vlan-group-parameters* | **bpdu-tag** *bpdu-tag-parameters*]

no spanning-tree *instance* [**forward-delay** | **hello-time** | **max-age** | **max-hops** | **priority** | **vlan-group** *vlan-group-parameters* | **bpdu-tag**]

Description

Enables a Spanning-tree instance and its configuration.

Inserting **no** as a prefix for this command will disable the specified spanning-tree instance.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
forward-delay <i>forward-delay-parameters</i>	(Optional) Configures the Spanning-Tree Algorithm forwarding delay time. Click here to see the "forward-delay-parameters" description.
hello-time <i>hello-time-parameters</i>	(Optional) Configures the Spanning-Tree Algorithm hello time. Click here to see the "hello-time-parameters" description.
max-age <i>max-age-parameters</i>	(Optional) Configures the Spanning-Tree Algorithm maximum age. Click here to see the "max-age-parameters" description.
max-hops <i>max-hops-parameters</i>	(Optional) Configures the Spanning-Tree Algorithm maximum hops. This is the maximum number of hops in a MSTP region before a BPDU is discarded. Click here to see the "max-hops-parameters" description.
priority <i>priority-parameters</i>	(Optional) Specifies the spanning-tree priority in the DmSwitch. Click here to see the "priority-parameters" description.
root <i>root-parameters</i>	(Optional) Configures the spanning-tree priority so that the equipment becomes the root bridge or a backup for the root bridge. Click here to see the "root-parameters" description.
vlan-group <i>vlan-group-parameters</i>	(Optional) Adds VLAN groups to a spanning-tree instance. Click here to see the "vlan-group-parameters" description.
bpdu-tag <i>bpdu-tag-parameters</i>	(Optional) Configure the default STP BPDU tag mode. Click here to see the "bpdu-tag-parameters" description.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

Not available.

Example

This example shows how to enable a Spanning-Tree instance.

```
DmSwitch(config)#spanning-tree 1
DmSwitch(config)#
```

You can verify that the instance was enabled by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.

Command	Description
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* forward-delay

spanning-tree *instance* **forward-delay** *delay*

no spanning-tree *instance* **forward-delay**

Description

Configures the Spanning-Tree Algorithm forwarding delay time.

Inserting **no** as a prefix for this command will return forwarding delay time to the default value.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>delay</i>	Specifies the forwarding delay time in seconds. (Range: 4-30)

Default

Delay: 15 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

Not available.

Example

This example shows how to configure the forwarding delay time.

```
DmSwitch(config)#spanning-tree 1 forward-delay 30
DmSwitch(config)#
```


You can verify that the delay time was configured by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* hello-time

spanning-tree *instance* **hello-time** *time*

no spanning-tree *instance* **hello-time**

Description

Configures the Spanning-Tree Algorithm hello time.

Inserting **no** as a prefix for this command will return hello time to the default value.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>time</i>	Specifies the hello time in seconds. (Range: 1-10)

Default

Hello time: 2 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

Not available.

Example

This example shows how to configure the hello time.

```
DmSwitch(config)#spanning-tree 1 hello-time 5
DmSwitch(config)#
```

You can verify that the hello time was configured by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* max-age

spanning-tree *instance* **max-age** *max-age-time*

no spanning-tree *instance* **max-age**

Description

Configures the Spanning-Tree Algorithm maximum age.

Inserting **no** as a prefix for this command will return the maximum age to the default value.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>max-age</i>	Specifies the maximum age in seconds. (Range: 6-40)

Default

Maximum age: 20 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

The value of maximum age must be less than: $2 * (\text{forward_delay} - 1)$.

Example

This example shows how to configure the maximum age.

```
DmSwitch(config)#spanning-tree 1 max-age 28
DmSwitch(config)#
```

You can verify that the maximum age was configured by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* max-hops

spanning-tree *instance* **max-hops** *max-hops-number*

no spanning-tree *instance* **max-hops**

Description

Configures the Spanning-Tree Algorithm maximum hops. This is the maximum number of hops in a MSTP region before a BPDU is discarded.

Inserting **no** as a prefix for this command will return the maximum hops to the default value.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>max-hops-number</i>	Specifies the maximum number of hops. (Range: 1-40)

Default

Maximum hops: 20.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter only applies to MSTP mode of spanning-tree protocol.

Example

This example shows how to configure the maximum hops.

```
DmSwitch(config)#spanning-tree 1 max-hops 25
DmSwitch(config)#
```

You can verify that the maximum hops was configured by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* priority

spanning-tree *instance* **priority** *priority-value*

no spanning-tree *instance* **priority**

Description

Specifies the spanning-tree priority in the DmSwitch.

Inserting **no** as a prefix for this command will return the priority value to the default value.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>priority-value</i>	Specifies the priority value in steps of 4096. (Range: 0-61440)

Default

Priority value: 32768.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

The spanning-tree priority is used by Spanning-Tree Algorithm in order to elect the spanning-tree root bridge. Lower values represents higher priorities to become the root bridge. If all devices on the network use the same priority, the one with the lowest MAC address will be elected the root bridge.

Example

This example shows how to configure the spanning-tree priority.

```
DmSwitch(config)#spanning-tree 1 priority 40960
DmSwitch(config)#
```


You can verify that the maximum age was configured by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* root

```
spanning-tree instance root { primary | secondary }
```

Description

Configures the spanning-tree priority so that the equipment becomes the root bridge or a backup for the root bridge.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
primary	Configures a new priority that would cause the equipment to become the root bridge.
secondary	Configures a new priority would cause the equipment to become the root bridge after a failure in the current root bridge.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This is a helper command to automatically set a lower spanning-tree priority in order to turn the equipment into the root bridge. This is not a configuration itself, but it changes the spanning-tree priority configuration instead.

Using **primary** as parameter, the command will set the priority to the minimum value between 24576 and the current root bridge priority minus 4096. After that, the spanning-tree protocol will elect this equipment as the new root bridge. This command will not change the priority value if this is already the root bridge for the spanning-tree instance.

Using **secondary** as parameter, the command will set the priority to 28762. After a failure in another equipment elected as the root bridge, it is likely that this equipment becomes the new root bridge. However this could not be true depending on priority values manually configured on other equipments in the network.

Example

This example shows how to force the equipment to be the root bridge for spanning-tree instance 1.

```
DmSwitch(config)#spanning-tree 1 root primary
DmSwitch(config)#
```

You can verify that the priority was configured by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* vlan-group

spanning-tree *instance* **vlan-group** { *index* | **all** | **range** *first-index last-index* }

no spanning-tree *instance* **vlan-group** { *index* | **all** | **range** *first-index last-index* }

Description

Adds VLAN groups to a spanning-tree instance.

Inserting **no** as a prefix for this command will remove the specified VLAN groups from spanning-tree instance.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>index</i>	Specifies a VLAN group ID. (Range: 0-31)
all	Specifies all VLAN groups.
range <i>first-index last-index</i>	Specifies a range of VLAN group IDs.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
5.0	This command was introduced. It replaces the command spanning-tree instance vlan .

Usage Guidelines

Not available.

Example

This example shows how to add a range of VLAN groups to a spanning-tree instance.

```
DmSwitch(config)#spanning-tree 1 vlan-group range 1 10
```

```
DmSwitch(config)#
```

You can verify that the VLAN groups were added by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree *instance* bpdu-tag

spanning-tree *instance* **bpdu-tag** *bpdu-tag-value*

no spanning-tree *instance* **bpdu-tag**

Description

Configure the default STP BPDU tag mode in the DmSwitch.

Inserting **no** as a prefix for this command will return the bpdu-tag value to the default value.

Syntax

Parameter	Description
<i>first-vlan</i>	Send BPDUs with first vlan tag of the protected vlan-group
<i>untagged</i>	Send untagged BPDUs
<i>1-4094</i>	VLAN ID

Default

Priority value: *first-vlan*.

Command Modes

Global configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The spanning-tree bpdu-tag is used by Spanning-Tree Algorithm in order to select the VLAN of the BPDU's. It is possible to leave it untagged, by choosing the option *untagged* .

Example

This example shows how to configure the spanning-tree bpdu-tag.

```
DmSwitch(config)#spanning-tree 1 bpdu-tag 1-4094
DmSwitch(config)#
```

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree mode

```
spanning-tree mode { mstp | rstp | stp }
```

```
no spanning-tree mode
```

Description

Configures the spanning-tree mode.

Inserting **no** as a prefix for this command will return the spanning-tree mode to the default value.

Syntax

Parameter	Description
mstp	Selects the Multiple Spanning-Tree Protocol mode.
rstp	Selects the Rapid Spanning-Tree Protocol mode.
stp	Selects the Spanning-Tree Protocol mode.

Default

Spanning-tree mode: rstp.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to select the MSTP mode.

```
DmSwitch(config)#spanning-tree mode mstp
DmSwitch(config)#
```


You can verify that the information was deleted by entering the **show spanning-tree** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

spanning-tree mst

```
spanning-tree mst { name name | revision revision-number }
```

```
no spanning-tree mst { name | revision }
```

Description

Defines parameters of Multiple Spanning-Tree (MST) configuration.

Inserting **no** as a prefix for this command will remove the records from the specified parameters.

Syntax

Parameter	Description
name <i>name</i>	Specifies the MST configuration name.
revision <i>revision-number</i>	Specifies the MST configuration revision number.

Default

Name is empty and revision is zero.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a name to MST configuration.

```
DmSwitch(config)#spanning-tree mst name test
DmSwitch(config)#
```

You can verify that the name was saved by entering the **show spanning-tree** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

storm-control

storm-control action

no storm-control action

Description

This option enables at global level the storm-control action options, which then must be fine-grained controlled by interface.

Inserting **no** as a prefix for this command will disable any action other action than limit on all interfaces.

Syntax

Parameter	Description
action	Confirm intention on enabling or disable actions for storm-control.

Default

Defaults to be disabled.

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Not available.

Not available.

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.
storm-control	Configures packet storm control.

sync-source bits-clock-mode

```
sync-source unit { all | { range first-unit-id last-unit-id } | unit-number }
bits-clock-mode { 2MHz | 2Mbps }
```

Description

Selects the BITS clock synchronization mode.

Syntax

Parameter	Description
all	Configures all units.
range <i>first-unit last-unit</i>	Configures a range of units, defined from <i>first-unit</i> to <i>last-unit</i> .
<i>unit-number</i>	Configures an specific unit.
bits-clock-mode 2MHz	Set external clock operation mode to 2Mhz
bits-clock-mode 2Mbps	Set BITS clock operation mode to 2Mbps unframed (HDB3)

Default

By default BITS port uses 2MHz mode.

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example configures the BITS port to operate at 2Mbps unframed (HDB3) mode.

```
DM4000(config)#sync-source unit 1 bits-clock-mode 2Mbps
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show sync-source bits-clock-mode</code>	Shows synchronization bits clock mode source configuration

sync-source hierarchy ack-out-of-limits

```
sync-source unit unit-number hierarchy { all | { range first-hierarchy  
level last-hierarchy level } | hierarchy-level } ack-out-of-limits
```

Description

Acknowledges and clear out of limits alarm on selected hierarchy, returning from internal to configured clock source.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

No default is defined.

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

```
DM4000(config)#sync-source unit 1 hierarchy 1 ack-out-of-limits
```

Related Commands

Command	Description
<code>show sync-source status</code>	Shows synchronization clock source status

sync-source hierarchy enable

```
sync-source unit unit-number hierarchy { all | { range first-hierarchy
level last-hierarchy level } | hierarchy-level } enable
```

Description

Enables selected hierarchy.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

Default is defined to enable to first hierarchy and disable to others.

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

```
DM4000(config)#sync-source unit 1 hierarchy 1 enable
```

Related Commands

Command	Description
<code>show sync-source status</code>	Shows synchronization clock source status

sync-source hierarchy transmit-clock-source bits

```
sync-source unit    unit-number hierarchy { all | { range first-hierarchy
level last-hierarchy level } | hierarchy-level } transmit-clock-source external

no sync-source unit    unit-number hierarchy hierarchy-level [
transmit-clock-source ]
```

Description

Select external clock input as the source used to keep clock synchronization.

Inserting **no** as a prefix for this command will remove the records from the specified parameters. Depending on the point where the command is called one or more hierarchies will be set to default.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

By default the hierarchies use internal sync-source with no switch-criteria (Fail).

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example configure to transmit clock signal through external clock input.

```
DM4000(config)#sync-source unit 1 hierarchy 1 transmit-clock-source bits
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
show sync-source hierarchy	Shows synchronization clock source hierarchy configuration

sync-source hierarchy transmit-clock-source g704

```
sync-source unit unit-number hierarchy { all | { range first-hierarchy  
level last-hierarchy level } | hierarchy-level } transmit-clock-source g704 g704-id [  
switch-criteria { ais | crc | lof | lom }]
```

```
no sync-source unit unit-number hierarchy hierarchy-level [  
transmit-clock-source [ switch-criteria ]]
```

Description

Select g704 physical interface as the source used to keep clock synchronization. Then the switch-criteria. If a source fails in the specified switch-criteria, the next sync-source on hierarchy is used. By last it uses internal signal.

Inserting **no** as a prefix for this command will remove the records from the specified parameters. Depending on the point where the command is called one or more hierarchies will be set to default.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

By default the hierarchies use internal sync-source with no switch-criteria (Fail).

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example configure to transmit clock signal through interface g704 1 using lom alarm as switch criteria.

```
DM4000(config)#sync-source unit 1 hierarchy 1 transmit-clock-source g704 1 switch-criteria lom
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
show sync-source hierarchy	Shows synchronization clock source hierarchy configuration

sync-source hierarchy transmit-clock-source internal

```
sync-source unit    unit-number hierarchy { all | { range first-hierarchy
level last-hierarchy level } | hierarchy-level } transmit-clock-source internal

no sync-source unit    unit-number hierarchy hierarchy-level [
transmit-clock-source ]
```

Description

Select internal clock input as the source used to keep clock synchronization.

Inserting **no** as a prefix for this command will remove the records from the specified parameters. Depending on the point where the command is called one or more hierarchies will be set to default.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

By default the hierarchies use internal sync-source with no switch-criteria (Fail).

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example configure to transmit clock signal using internal clock.

```
DM4000(config)#sync-source unit 1 hierarchy 1 transmit-clock-source internal
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
show sync-source hierarchy	Shows synchronization clock source hierarchy configuration

sync-source hierarchy transmit-clock-source ptp

```
sync-source unit    unit-number hierarchy { all | { range first-hierarchy
level last-hierarchy level } | hierarchy-level } transmit-clock-source ptp ptp-id [
switch-criteria { freerun | holdover } ]

no sync-source unit    unit-number hierarchy hierarchy-level [
transmit-clock-source [ switch-criteria ] ]
```

Description

Select ptp interface as the source used to keep clock synchronization. Then the switch-criteria. If a source fails in the specified switch-criteria, the next sync-source on hierarchy is used. By last it uses internal signal.

Inserting **no** as a prefix for this command will remove the records from the specified parameters. Depending on the point where the command is called one or more hierarchies will be set to default.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

By default the hierarchies use internal sync-source with no switch-criteria (Fail).

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example configure to transmit clock signal through interface ptp 1 using holdover switch-criteria.

```
DM4000(config)#sync-source unit 1 hierarchy 1 transmit-clock-source ptp 1 switch-criteria holdover
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
show sync-source hierarchy	Shows synchronization clock source hierarchy configuration

sync-source hierarchy transmit-clock-source sdh

```
sync-source unit    unit-number hierarchy { all | { range first-hierarchy
level last-hierarchy level } | hierarchy-level } transmit-clock-source sdh sdh-id [
switch-criteria { ms-ais | ms-exc | rs-lof | rs-tim } ]

no sync-source unit    unit-number hierarchy hierarchy-level [
transmit-clock-source [ switch-criteria ] ]
```

Description

Select ptp interface as the source used to keep clock synchronization. Then the switch-criteria. If a source fails in the specified switch-criteria, the next sync-source on hierarchy is used. By last it uses internal signal.

Inserting **no** as a prefix for this command will remove the records from the specified parameters. Depending on the point where the command is called one or more hierarchies will be set to default.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.

Default

By default the hierarchies use internal sync-source with no switch-criteria (Fail).

Command Modes

Configuration.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example configure to transmit clock signal through interface sdh 1 using ms-ais switch-criteria.

```
DM4000(config)#sync-source unit 1 hierarchy 1 transmit-clock-source sdh 1 ms-ais
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
show sync-source hierarchy	Shows synchronization clock source hierarchy configuration

sync-source hierarchy wtr

```
sync-source unit unit-number hierarchy { all | { range first-hierarchy  
level last-hierarchy level } | hierarchy-level } wtr seconds
```

Description

Acknowledges and clear out of limits alarm on selected hierarchy, returning from internal to configured clock source.

Syntax

Parameter	Description
<i>unit-number</i>	Configures an specific unit.
hierarchy range <i>first-hier last-hier</i>	Shows information about a range of clock synchronization hierarchies.
hierarchy all	Shows information about all clock synchronization hierarchies.
hierarchy <i>hierarchy-level</i>	Shows information about a specific clock synchronization hierarchy.
wtr <i>seconds</i>	Configures wait to restore time in seconds. Source status has to be ok for this period before being used again.

Default

No default is defined.

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example set time to wait after OK status on a higher level hierarchy before restore clock source to it.

```
DM4000(config)#sync-source unit 1 hierarchy 1 wtr 2
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
show sync-source status	Shows synchronization clock source status

sync-source revertive

```
sync-source unit { all | { range first-unit-id last-unit-id } | unit-number }  
revertive
```

Description

Enables revertive operation. Allows sync-source to return to a better hierarchy.

Syntax

Parameter	Description
all	Configures all units.
range <i>first-unit last-unit</i>	Configures a range of units, defined from <i>first-unit</i> to <i>last-unit</i> .
<i>unit-number</i>	Configures an specific unit.

Default

By default synchronization source selection is revertive.

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example enables the revertive operation to a better hierarchy.

```
DM4000(config)#sync-source unit 1 revertive
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show sync-source</code>	Shows synchronization clock source configuration

sync-source switch-enable

```
sync-source unit { all | { range first-unit-id last-unit-id } | unit-number }
switch-enable
```

Description

Enables globally switch between interfaces.

Syntax

Parameter	Description
all	Configures all units.
range <i>first-unit last-unit</i>	Configures a range of units, defined from <i>first-unit</i> to <i>last-unit</i> .
<i>unit-number</i>	Configures an specific unit.

Default

By default switching between hierarchies is enabled.

Command Modes

Configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example enables the switching between synchronization sources.

```
DM4000(config)#sync-source unit 1 switch-enable
```

You may check that the configuration was applied by the command **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show sync-source</code>	Shows synchronization clock source configuration

tacacs-server acct-port

tacacs-server acct-port *port-number*

no tacacs-server acct-port

Description

Configures the TACACS default server accounting port.

Inserting **no** as a prefix for this command will return to the default port value.

Syntax

Parameter	Description
<i>port-number</i>	Specify TACACS server accounting port. (Range: 1-65535)

Default

Port number: 49.

Command Modes

Global configuration.

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

The accounting login by a TACACS server depends on this configuration.

Example

This example shows how to define a different TACACS server accounting port.

```
DmSwitch(config)#tacacs-server acct-port 8380
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server acct-timeout

`tacacs-server acct-timeout time`

`no tacacs-server acct-timeout`

Description

Configure timeout in seconds for TACACS accounting operations.

Inserting **no** as a prefix for this command will return to default timeout value.

Syntax

Parameter	Description
<i>timeout</i>	Specify TACACS timeout in seconds for accounting operations. (Range: 3-60)

Default

Timeout: 10.

Command Modes

Global configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command is used to configure the timeout waiting for the answer from a TACACS accounting server. When timeout occurs the next server is used.

Example

This example shows how to set TACACS timeout for accounting operations.

```
DmSwitch(config)#tacacs-server acct-timeout 3
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server acct-type

```
tacacs-server acct-type { pap | ascii }
```

```
no tacacs-server acct-type
```

Description

Configures the TACACS default server accounting type.

Inserting **no** as a prefix for this command will return to the default type value.

Syntax

Parameter	Description
pap	Specify PAP accounting type.
ascii	Specify ASCII accounting type.

Default

Type: PAP.

Command Modes

Global configuration.

Command History

Release	Modification
6.6	This command was introduced.

Usage Guidelines

The accounting login by a TACACS server depends on this configuration.

Example

This example shows how to define a different TACACS server accounting type.

```
DmSwitch(config)#tacacs-server acct-type ascii  
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server authe-port

tacacs-server authe-port *port-number*

no tacacs-server authe-port

Description

Configures the TACACS default server authentication port.

Inserting **no** as a prefix for this command will return to the default port value.

Syntax

Parameter	Description
<i>port-number</i>	Specify TACACS server authentication port. (Range: 1-65535)

Default

Port number: 49.

Command Modes

Global configuration.

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

The authentication login by a TACACS server depends on this configuration.

Example

This example shows how to define a different TACACS server authentication port.

```
DmSwitch(config)#tacacs-server authe-port 8380
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server auth-timeout

`tacacs-server auth-timeout time`

`no tacacs-server auth-timeout`

Description

Configure timeout in seconds for TACACS authentication operations.

Inserting **no** as a prefix for this command will return to default timeout value.

Syntax

Parameter	Description
<i>timeout</i>	Specify TACACS timeout in seconds for authentication operations. (Range: 3-60)

Default

Timeout: 10.

Command Modes

Global configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command is used to configure the timeout waiting for the answer from a TACACS authentication server. When timeout occurs the next server is used.

Example

This example shows how to set TACACS timeout for authentication operations.

```
DmSwitch(config)#tacacs-server auth-timeout 5
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server auth-type

```
tacacs-server auth-type { pap | ascii }
```

```
no tacacs-server auth-type
```

Description

Configures the TACACS default server authentication type.

Inserting **no** as a prefix for this command will return to the default type value.

Syntax

Parameter	Description
pap	Specify PAP accounting type.
ascii	Specify ASCII accounting type.

Default

Type: PAP.

Command Modes

Global configuration.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The authentication login by a TACACS server depends on this configuration.

Example

This example shows how to define a different TACACS server authentication type.

```
DmSwitch(config)#tacacs-server auth-type ascii  
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server autho-port

tacacs-server autho-port *port-number*

no tacacs-server autho-port

Description

Configures the TACACS default server authorization port.

Inserting **no** as a prefix for this command will return to the default port value.

Syntax

Parameter	Description
<i>port-number</i>	Specify TACACS server authorization port. (Range: 1-65535)

Default

Port number: 49.

Command Modes

Global configuration.

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

The authorization login by a TACACS server depends on this configuration.

Example

This example shows how to define a different TACACS server authorization port.

```
DmSwitch(config)#tacacs-server autho-port 8380
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server autho-timeout

`tacacs-server autho-timeout time`

`no tacacs-server autho-timeout`

Description

Configure timeout in seconds for TACACS authorization operations.

Inserting **no** as a prefix for this command will return to default timeout value.

Syntax

Parameter	Description
<i>timeout</i>	Specify TACACS timeout in seconds for authorization operations. (Range: 3-60)

Default

Timeout: 3.

Command Modes

Global configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command is used to configure the timeout waiting for the answer from a TACACS authorization server. When timeout occurs the next server is used.

Example

This example shows how to set TACACS timeout for authorization operations.

```
DmSwitch(config)#tacacs-server autho-timeout 5
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.
<code>tacacs-server key</code>	Configures the TACACS server key string.

tacacs-server host

```
tacacs-server host index { accounting | acct-port number | authentication |  
autho-port number | address ip-address | key text | source-iface { loopback number |  
vlan number } }
```

```
no tacacs-server host index [ accounting | authorization | authentication |  
source-iface ]
```

Description

Configures the TACACS server IP address.

Inserting **no** as a prefix for this command will remove the configuration for the specified host.

Syntax

Parameter	Description
<i>index</i>	Specifies the server index. (Range: 1-5)
accounting	Enables TACACS accounting.
acct-port <i>number</i>	Specifies TACACS server accounting port. (Range: 1-65535)
authentication	Enables RADIUS authentication.
autho-port <i>number</i>	Specifies TACACS server authentication port. (Range: 1-65535)
authorization	Enable TACACS authorization.
autho-port <i>number</i>	Specifies TACACS server authorization port. (Range: 1-65535)
address <i>ip-address</i>	Specifies TACACS server IPv4/IPv6 address.
key <i>text</i>	Specifies TACACS server key. (text up to 32 characters)
source-iface	Specifies the TACACS source interface.
loopback <i>number</i>	Select loopback interface as source address. (Range: 1-4094)
vlan <i>number</i>	Select VLAN interface as source address. (Range: 0-7)

Default

No host is configured.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.4	IPv6 address option was introduced.

Usage Guidelines

The authentication login by a TACACS server depends on this configuration.

Example

This example shows how to define the TACACS server IP address.

```
DmSwitch(config)#tacacs-server host 10.10.11.20
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
authentication login	Defines the login authentication method and its precedence.
show running-config	Shows the current operating configuration.
show tacacs-server	Shows global TACACS information and all configured servers.
tacacs-server key	Configures the TACACS server key string.

tacacs-server key

tacacs-server key *text*

no tacacs-server key

Description

Configures the TACACS server key string.

Inserting **no** as a prefix for this command will remove the configured key.

Syntax

Parameter	Description
<i>text</i>	Specifies the key string. (up to 32 characters)

Default

No key is configured.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The authentication login by a TACACS server depends on this configuration.

Example

This example shows how to define the TACACS key string.

```
DmSwitch(config)#tacacs-server key this_is_a_test
DmSwitch(config)#
```

The configuration can be verified by entering the **show tacacs-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>show running-config</code>	Shows the current operating configuration.
<code>show tacacs-server</code>	Shows global TACACS information and all configured servers.
<code>tacacs-server host</code>	Configures the TACACS server IP address.

terminal login-timeout

terminal login-timeout *seconds*

no terminal login-timeout

Description

Allows to set a login timeout for terminal. This is the maximum time for login operations including all authentication methods: local database, TACACS+ servers or RADIUS servers.

Inserting **no** as a prefix for this command will reset login-timeout to its default value.

Syntax

Parameter	Description
<i>seconds</i>	Specifies maximum time for login operations . (Range: 10-600)

Default

Disabled.

Command Modes

User EXEC.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the login timeout.

```
DmSwitch(config)#terminal login-timeout 50
DmSwitch(config)#
```

You can verify that the login timeout was configured by entering the **show terminal** privileged EXEC configuration command.

Related Commands

Command	Description
<code>show terminal</code>	Shows terminal information.

terminal paging

terminal paging

no terminal paging

Description

Allows to set a filter for paging through text one screenful at a time.

Inserting **no** as a prefix for this command makes terminal screen to roll continuously.

Syntax

No parameter accepted.

Default

Enabled.

Command Modes

User EXEC.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable paging.

```
DmSwitch(config)#no terminal paging
DmSwitch(config)#
```

You can verify that the paging was configured by entering the **show running-config** privileged EXEC configuration command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

terminal timeout

terminal timeout *seconds*

no terminal timeout

Description

Allows to set an idle timeout for terminal. When the timeout is reached the system issues an auto-logout.

Inserting **no** as a prefix for this command will disable the terminal timeout feature.

Syntax

Parameter	Description
<i>seconds</i>	Specifies the number of seconds until timeout. (Range: 15-3600)

Default

Disabled.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set an idle timeout for terminal.

```
DmSwitch(config)#terminal timeout 600
DmSwitch(config)#
```

You can verify that the timeout was configured by entering the **show running-config** privileged EXEC configuration command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

username

```
username username { access-level { 0 | 1 | 15 } | nopassword | password { 0 plain-text-password | 7 encrypted-password } }
```

```
no username username
```

Description

Creates users and configures its access to the DmSwitch.

Inserting **no** as a prefix for this command will remove the specified username.

Syntax

Parameter	Description
<i>username</i>	Specifies a user name. (Maximum: 32 characters)
access-level	Specifies the privilege level for the user.
0	Defines the normal user access.
1	Defines the normal user access, with access to more visualization commands.
15	Defines the privileged user access.
nopassword	Defines that the user do not have password.
password	Defines a user password.
0 <i>plain-text-password</i>	Specifies a password in plain text.
7 <i>encrypted-password</i>	Specifies a password in encrypted form.

Default

Username: admin; access-level: 15.

Username: guest; access-level: 0.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.0	New user level (1) was introduced.

Usage Guidelines

Creating a **nopassword** user, it configures **access-level 0**. Use the **username username access-level** command to change it.

Example

This example shows how to create a new user with normal access.

```
DmSwitch(config)#username test access-level 0
DmSwitch(config)#
```

You can verify that the user was created by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show managers	Shows the connected managers using terminals.
show running-config	Shows the current operating configuration.
show users	Shows the users information.

vlan-group

vlan-group *instance* [**vlan** { *index* | **all** | **range** *first-index last-index* }]

no vlan-group *instance* [**vlan** { *index* | **all** | **range** *first-index last-index* }]

Description

Create a VLAN group and manage its members in case of VLAN group already exists.

Inserting **no** as a prefix for this command will remove the specified VLAN group or VLAN group member.

Syntax

Parameter	Description
<i>instance</i>	Specifies the VLAN group instance. (Range: 0-31)
vlan	Adds VLANs to the specified VLAN group.
<i>index</i>	Specifies a VLAN ID. (Range: 1-4094)
all	Specifies all VLANs.
range <i>first-index last-index</i>	Specifies a range of VLAN IDs.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a VLAN group, and add a range of VLANs to this group.

```
DmSwitch(config)#vlan-group 5
```

```
DmSwitch(config)#vlan-group 5 vlan range 1 100
DmSwitch(config)#
```

You can verify that the VLAN groups were added by entering the **show running-config** *instance* privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

vlan link-detect

vlan link-detect

no vlan link-detect

Description

Enables the VLAN link detect mode.

Inserting **no** as a prefix for this command will disable the VLAN link detect.

Syntax

No parameter accepted.

Default

The VLAN link detect mode is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

Use the VLAN link detect mode to put vlan link down when all member ports are down.

Example

This example shows how to enable the VLAN link detect.

```
DmSwitch(config)#vlan link detect
DmSwitch(config)#
```

You can verify that this function was disabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>link-detect</code>	Enables link detect on the selected VLAN.
<code>show running-config</code>	Shows the current operating configuration.

vlan-mac-table source-mac ^[1]

```
vlan-mac-table source-mac mac-address vlan vlan-id priority number [ unit { all |  
unit-number } [ remark text ] | remark text ]
```

```
no vlan-mac-table [ source-mac mac-address ] [ unit unit-number ]
```

Description

Add an association from MAC address to VLAN to use for assigning a VLAN tag to untagged packets.

Inserting **no** as a prefix for this command will remove the entire VLAN MAC table.

Syntax

Parameter	Description
<i>mac-address</i>	Specifies the MAC address.
vlan <i>vlan-id</i>	Specifies the VLAN ID. (Range: 1-4094)
priority <i>number</i>	Defines the priority number. (Range: 0-7)
unit <i>unit-number</i>	Specifies the unit number.
unit <i>all</i>	Selects all units.
remark <i>text</i>	Adds a remark text.

Default

By default, the table is empty.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

When inserting a new entry with the same MAC address of an existing entry, data will be overwritten.

Example

This example shows how to add a entry on the VLAN MAC table.

```
DmSwitch(config)#vlan-mac-table source-mac 00-01-02-03-04-05 vlan 1 priority 2 unit 1
DmSwitch(config)#
```

You can verify that the static MAC address was added by entering the **show vlan-mac-table** privileged EXEC command.

Related Commands

Command	Description
show vlan-mac-table	Shows the VLAN MAC table.
show running-config	Shows the current operating configuration.

vlan qinq

vlan qinq

no vlan qinq

Description

Enables the QinQ VLAN mode, also known as "Double Tagging".

Inserting **no** as a prefix for this command will disable the QinQ VLAN.

Syntax

No parameter accepted.

Default

The QinQ mode is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Use the QinQ mode in order to implement a second level of VLAN tagging on a core or service provider network.

Example

This example shows how to enable the QinQ VLAN.

```
DmSwitch(config)#vlan qinq
DmSwitch(config)#
```

You can verify that the information was deleted by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

vlan-translate

```
vlan-translate egress-table { ethernet { all | [ unit-number/ ] port-number | range  
{ [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } | port-channel  
port-channel-number } source-vlan { source-vlan ID | range first-source-vlan ID last-source-vlan  
ID } new-vlan new-vlan ID [ priority CoS-Priority ]
```

```
vlan-translate ingress-table { add | replace } { ethernet { all | [ unit-number/ ] port-  
number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } |  
port-channel port-channel-number } source-vlan { source-vlan ID | range first-source-vlan  
ID last-source-vlan ID } new-vlan new-vlan ID [ priority CoS-Priority ]
```

Description

Adds a VLAN tag or replaces an associated VLAN tag with another, on a given interface. Can be used to change the priority of a VLAN on certain interfaces.

Syntax

Parameter	Description
<i>egress-table</i>	Replace the new VLAN tag after the package is processed by switch.
<i>ingress-table</i>	Adds/Replaces the new VLAN tag before the package is processed by switch.
<i>add</i>	Sets vlan-translation ingress-table to add a new VLAN tag. Needed Q-in-Q enabled.
<i>replace</i>	Sets vlan-translation ingress-table to replace the original VLAN tag with a new VLAN tag.
<i>ethernet/portchannel</i>	Select the interface for vlan-translation.
<i>source-vlan ID</i>	Choose the vlan to apply vlan-translation.
<i>new-vlan ID</i>	New VLAN to add/replace to the package.
<i>CoS-Priority</i>	Sets the new VLAN CoS-Priority.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a VLAN translate that replaces a VLAN 5 tag with VLAN 7 tag with CoS priority 7. The VLAN tag is replaced after the package is processed.

```
DmSwitch(config)#vlan-translate egress-table ethernet range 2/10 2/15 source-vlan 5 new-vlan 10 priority 7
DmSwitch(config)#
```

You can verify that the VLAN translate were added by entering the **show running-config**

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
switchport vlan-translate	Adds a new VLAN tag or replaces an associated VLAN tag with another tag

wred

wred

no wred

Description

Enable Weighted Random Early Detection (WRED).

Inserting **no** as a prefix for this command will disable WRED.

Syntax

No parameter accepted.

Default

The default configuration to wred is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable wred

```
DmSwitch#wred
DmSwitch#
```

You can verify that the configuration was created by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
wred averaging-time	Configures the queue size averaging time for Ethernet interface
wred cng-drop-start-point	Configures the start point to drop CNG marked packets for Ethernet interface
wred cng-slope	Configures the slope of drop probability function for CNG marked packets for Ethernet interface
wred drop-start-point	Configures the start point to drop for Ethernet interface
wred slope	Configures the slope of drop probability function for Ethernet interface
show wred	Shows wred information

Chapter 4. CFM MA Commands

ais alarm-suppression

ais alarm-suppression

no ais alarm-suppression

Description

Enables Alarm Indication Signal (AIS) alarm suppression.

Inserting **no** as a prefix for this command will disable the AIS alarm suppression.

Syntax

No parameter accepted.

Default

Enabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable AIS alarm suppression.

```
DmSwitch(config-cfm-ma)#ais alarm-suppression
DmSwitch(config-cfm-ma)#
```

You can verify that the AIS alarm suppression was configured by entering the **show cfm md** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.

ais enable

ais enable

no ais enable

Description

Enables Alarm Indication Signal (AIS) transmission.

Inserting **no** as a prefix for this command will disable AIS transmission.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable AIS alarm suppression.

```
DmSwitch(config-cfm-ma) #ais enable
DmSwitch(config-cfm-ma) #
```

You can verify that the AIS was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.

ais level

ais level *number*

no ais level

Description

The maintenance level to send AIS frames for MEPs that belongs to MA.

Inserting **no** as a prefix for this command will reset the AIS level.

Syntax

Parameter	Description
<i>number</i>	Insert a level number. (Range: 0-7)

Default

The same level of the current MD.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change AIS level.

```
DmSwitch(config-cfm-ma)#ais level 7
DmSwitch(config-cfm-ma)#
```

You can verify that the MEP ID was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

ais period

```
ais period { 1min | 1s }
```

```
no ais period
```

Description

Transmission periodicity of frames.

Inserting **no** as a prefix for this command will reset the AIS period.

Syntax

Parameter	Description
1min	Insert 1 minute period.
1s	Insert 1 second period.

Default

1 second.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change AIS level.

```
DmSwitch(config-cfm-ma) #ais period 1min
DmSwitch(config-cfm-ma) #
```

You can verify that the AIS period was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

ais priority

ais priority *number*

no ais priority

Description

Transmission periodicity of frames.

Inserting **no** as a prefix for this command will reset the AIS priority.

Syntax

Parameter	Description
<i>number</i>	Insert priority for AIS frames transmitted by MEPS. (Range: 0-7)

Default

priority 0.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change AIS priority.

```
DmSwitch(config-cfm-ma) #ais priority 7
DmSwitch(config-cfm-ma) #
```

You can verify that the AIS period was configured by entering the **show runnig-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

ais recovery-limit

ais recovery-limit *number*

no ais recovery-limit

Description

AIS alarm suppression recovery limit.

Inserting **no** as a prefix for this command will reset the AIS alarm suppression recovery limit.

Syntax

Parameter	Description
<i>number</i>	Insert AIS recovery limit. (Range: 1.0-10.0)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change AIS recovery limit.

```
DmSwitch(config-cfm-ma)#ais recovery-limit 1.0
DmSwitch(config-cfm-ma)#
```

You can verify that the AIS recovery limit was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ais vlan-notify

ais vlan-notify *vlan-id-list*

no ais vlan-notify

Description

Create a list of VLANs to send AIS message.

Inserting **no** as a prefix for this command will empty AIS VLAN list.

Syntax

Parameter	Description
<i>vlan-id-list</i>	Add list of VIDs. (Range list: 1-16, Range vid: 1-4094)

Default

The list of VIDs is empty by default.

Commands Modes

CFM configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a list of VLANs that will be notified with AIS frames.

```
DM4000(config-cfm-ma)#ais vlan-notify 1 2 3
DM4000(config-cfm-ma)#
```

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ccm-interval

`ccm-interval { 1s | 10s | 1min | 10min }`

Description

Configure time between Continuity Check Messages transmissions.

Syntax

Parameter	Description
<code>1s 10s 1min 10min</code>	Specifies a time between Continuity Check Messages transmissions.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a time interval for Continuity Check Messages transmissions.

```
DmSwitch(config-cfm-ma)#ccm-interval 10s
DmSwitch(config-cfm-ma)#
```

You can verify that the time was configured to the list by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

fault-alarm-address

fault-alarm-address *ip-address*

no fault-alarm-address

Description

Configures IP address of the Fault Alarms recipient.

Inserting **no** as a prefix for this command will remove the IP address of the Fault Alarms recipient.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies a IP address for the Fault Alarms recipient.

Default

Not transmitted.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the IP address "10.1.1.1" for the Fault Alarms recipient.

```
DmSwitch(config-cfm-ma)#fault-alarm-address 10.1.1.1
DmSwitch(config-cfm-ma)#
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

mep

```
mep id mep-id [ direction { down | up } { ethernet { [ unit-number/ ] port-number } |  
local-tunnel endpoint {1|2} } ]
```

```
no mep id mep-id
```

Description

Maintenance End Point configuration.

Inserting **no** as a prefix for this command will delete the mep id reported.

Syntax

Parameter	Description
id <i>mep-id</i>	Insert a source MEP ID value. (Range: 1-8191)
direction down	Specifies the sending Continuity Check Messages away from the MAC Relay Entity.
direction up	Specifies the sending Continuity Check Messages towards the MAC Relay Entity.
ethernet [<i>unit-number/</i>] <i>port-number</i>	Entry Unit number/Ethernet interface number. (Range: 1-1/1-28)
local-tunnel endpoint {1 2}	Entry a local tunnel endpoint number. The endpoint must be specified in accordance with the endpoints available in the switch. (Range: 1-2)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.
13.0	The local-tunnel endpoint parameter was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure Maintenance End Point (MEP).

```
DmSwitch(config-cfm-ma)#mep id 1 direction down ethernet 10  
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the MEP ID was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

mep-list

mep-list *id-list*

no mep-list *id-list*

Description

List of Maintenance End Points for this Association.

Inserting **no** as a prefix for this command will delete the mep id reported of the mep id's list.

Syntax

Parameter	Description
<i>id-list</i>	Insert a list of Maintenance End Point (MEP) identifier. (Range: 1-8191)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure Maintenance End Point (MEP) List.

```
DmSwitch(config-cfm-ma) #mep-list 1 2 3
DmSwitch(config-cfm-ma) #
```

You can verify that the MEP ID was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

mip

mip ethernet [*unit-number/*] *port-number*

no mip ethernet [*unit-number/*] *port-number*

Description

Maintenance Intermediate Point configuration.

Inserting **no** as a prefix for this command will delete the mip ethernet port reported.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	Entry Unit number/Ethernet interface number. (Range: 1-1/1-28)

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure Maintenance Intermediate Point (MIP).

```
DmSwitch(config-cfm-ma) #mip ethernet 16
DmSwitch(config-cfm-ma) #
```

You can verify that the MEP ID was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

sender-id-tlv

sender-id-tlv { none | chassis | manage | chassis-manage defer }

Description

Configure the inclusion of Sender ID TLV transmitted by Maintenance Points.

Syntax

Parameter	Description
none	Specifies that sender ID TLV is not to be sent.
chassis	Specifies that chassis ID fields of the Sender ID TLV are to be sent.
manage	Specifies that Management Address Length and Address of the Sender ID TLV are to be sent.
chassis-manage	Specifies that both Chassis ID fields Management Address Length and Address of the Sender ID TLV are to be sent.
defer	Specifies that sender ID TLV control variable corresponds to the one set on its parent Maintenance Domain.

Default

sender-id-tlv none.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the inclusion of Sender ID TLV transmitted by Maintenance Points.

```
DmSwitch(config-cfm)#sender-id-tlv chassis-manage
DmSwitch(config-cfm)#
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

Chapter 5. CFM MD Commands

fault-alarm-address

fault-alarm-address *ip-address*

no fault-alarm-address

Description

Configures IP address of the Fault Alarms recipient.

Inserting **no** as a prefix for this command will remove the IP address of the Fault Alarms recipient.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies a IP address for the Fault Alarms recipient.

Default

Not transmitted.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the IP address "10.1.1.1" for the Fault Alarms recipient.

```
DmSwitch(config-cfm)#fault-alarm-address 10.1.1.1
```

```
DmSwitch(config-cfm) #
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

ma

ma *ma-name* [**vlan-list** *vlan-id* | **none**]

no **ma**

Description

Create a Maintenance Association and configure its parameters.

Inserting **no** as a prefix for this command will remove the Maintenance Association (MA).

Syntax

Parameter	Description
<i>ma-name</i>	Specifies Maintenance Association (MA) name.
vlan-list <i>vlan-id</i>	Specifies a MA primary VLAN ID. (Range: 1-4094)
none	Specifies a empty vlan-list.

Default

No default MA is configured.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a Maintenance Association.

```
DmSwitch(config-cfm) #ma MA_1 vlan-list 1
DmSwitch(config-cfm-ma) #
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

sender-id-tlv

`sender-id-tlv { none | chassis | manage | chassis-manage }`

Description

Configure the inclusion of Sender ID TLV transmitted by Maintenance Points.

Syntax

Parameter	Description
none	Specifies that sender ID TLV is not to be sent.
chassis	Specifies that chassis ID fields of the Sender ID TLV are to be sent.
manage	Specifies that Management Address Length and Address of the Sender ID TLV are to be sent.
chassis-manage	Specifies that both Chassis ID fields Management Address Length and Address of the Sender ID TLV are to be sent.

Default

sender-id-tlv none.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the inclusion of Sender ID TLV transmitted by Maintenance Points.

```
DmSwitch(config-cfm)#sender-id-tlv chassis-manage
DmSwitch(config-cfm)#
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

Chapter 6. CFM MEP Commands

action shutdown event

action shutdown

no action shutdown

Description

Enable action shutdown in response to CFM fail-events (when MEP lost connectivity to some remote MEP or when some remote interface link is down).

Inserting **no** as a prefix for this command will disable the action shutdown when an event occur.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.8	This command was introduced.

Usage Guidelines

This option is only available on MEPs with direction up.

Example

This example shows how to enable action shutdown

```
DmSwitch(config-cfm-ma-mep)#action shutdown
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the action was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

enable

enable

no enable

Description

Enables Maintenance End Point (MEP).

Inserting **no** as a prefix for this command will disable MEP.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable MEP.

```
DmSwitch(config-cfm-ma-mep)#enable
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the MEP was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

fault-alarm-address

fault-alarm-address *ip-address*

no fault-alarm-address

Description

Configures IP address of the Fault Alarms recipient.

Inserting **no** as a prefix for this command will remove the IP address of the Fault Alarms recipient.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies a IP address for the Fault Alarms recipient.

Default

Not specified.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the IP address "10.1.1.1" for the Fault Alarms recipient.

```
DmSwitch(config-cfm-ma-mep)#fault-alarm-address 10.1.1.1
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the IP address was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

fault-alarm-priority

```
fault-alarm-priority { all | mac-status | remote-ccm | error-ccm |  
cross-connect-ccm | none }
```

Description

Configure the lowest priority defect that is allowed to generate a fault alarm.

Syntax

Parameter	Description
all	Specifies all defects.
mac-status	Specifies CCM received reports that MEP's MAC is reporting error and set: remote-ccm, error-ccm and cross-connect-ccm.
remote-ccm	Specifies that this MEP is not receiving CCMs from remotes and set: error-ccm and cross-connect-ccm.
error-ccm	Specifies that this MEP is not receiving CCMs from remotes and set: cross-connect-ccm.
cross-connect-ccm	Specifies that this MEP is receiving CCMs that should be from some other MA.
none	Specifies no defects are to be reported.

Default

MAC Status, Remote CCM, Error CCM and Cross Conect CCM .

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the Fault Alarm Priority.


```
DmSwitch(config-cfm-ma-mep)#fault-alarm-priority cross-connect-ccm
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the fault alarm priority was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.
show running-config	Shows the current operating configuration.

fault-alarm-time

fault-alarm-time { **absent** *time* | **present** *time* }

Description

Configure the time that defects generate/reset a fault alarm.

Syntax

Parameter	Description
absent <i>time</i>	Configure the time that defects must be absent to reset a fault alarm. (Range: 1-2500 milliseconds)
present <i>time</i>	Configure the time that defects must be present to generate a fault alarm.(Range: 1-10000 milliseconds)

Default

absent: 2500 ms , present: 10000 ms.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure 10ms for the Fault Alarm Time Absent.

```
DmSwitch(config-cfm-ma-mep)#fault-alarm-time absent 10
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the fault alarm time was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

generate-ccm

generate-ccm

no generate-ccm

Description

Enable the MEP's generation of Continuity Check Messages (CCMs).

Inserting **no** as a prefix for this command will disable CCM generation.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable CCM generation.

```
DmSwitch(config-cfm-ma-mep)#generate-ccm
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the CCM generation was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cfm md</code>	Maintenance Domain (MD) information.
<code>show running-config</code>	Shows the current operating configuration.

primary-vid

primary-vid *vlan-id*

Description

Configure the Primary VID of the MEP. Must be one of the MEP's MA VIDs.

Syntax

Parameter	Description
<i>vlan-id</i>	Specifies the primary VID of the MEP. Must be one of the MEP's MA vlan-list.

Default

The first VID of the MEP's MA vlan-list.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure VID 1 for the primary vid of the MEP.

```
DmSwitch(config-cfm-ma-mep)#primary-vid 1
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the primary VID was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

priority

priority *number*

Description

Configure priority for CCMs and LTMs transmitted by the MEP.

Syntax

Parameter	Description
<i>number</i>	Specifies the priority for CCMs and LTMs transmitted by MEP. (Range: 0-7)

Default

Priority 7.

Command Modes

Global configuration.

Command History

Release	Modification
7.8	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure priority 3 for for CCMs and LTMs transmitted by MEP.

```
DmSwitch(config-cfm-ma-mep)#priority 3
DmSwitch(config-cfm-ma-mep)#
```

You can verify that the priority was changed by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show cfm md	Maintenance Domain (MD) information.

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

Chapter 7. CFM Probe Commands

delay-measurement

delay-measurement *probe id*

no delay-measurement *probe id*

Description

Create/Edit CFM delay-measurement probe instance.

Syntax

Parameter	Description
<i>probe id</i>	Specifies the probe identifier.

Command Modes

Global configuration.

Command History

Release	Modification
11.2.10	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create/edit the delay-measurement for probe 3.

```
DmSwitch(config-cfm-probe)#delay-measurement 3
DmSwitch(config-cfm-probe-dm)#
```

You can verify that the CFM probe was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show cfm probe delay-measurement</code>	CFM Probe Delay Measurement (DM) information.
<code>show running-config</code>	Shows the current operating configuration.

Chapter 8. CFM Probe DM Commands

interval

interval *minutes*

Description

Configure the interval between 2 delay-measurement probes.

Syntax

Parameter	Description
<i>minutes</i>	Specifies the interval in minutes.(Range 1-1440)

Command Modes

Global configuration.

Command History

Release	Modification
11.2.10	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a interval between 2 delay-measurement probes.

```
DmSwitch(config-cfm-probe-dm)#interval 1
DmSwitch(config-cfm-probe-dm)#
```

You can verify that the interval was configured by entering the **show cfm probe delay-measurement** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show cfm probe delay-measurement</code>	CFM Probe Delay Measurement (DM) information.
<code>show running-config</code>	Shows the current operating configuration.

ma

```
ma ma-name mep id mep-id remote-mep { id mep-id } [ count number [ interval { 1s | 10s | 1min | 10min } ]
```

Description

Configure.

Syntax

Parameter	Description
ma <i>ma-name</i>	Specifies Maintenance Association (MA) name.
mep id <i>mep-id</i>	Insert a source MEP ID value. (Range: 1-8191)
remote-mep id <i>mep-id</i>	Insert a destination MEP ID. (Range: 1-8191)
count <i>number</i>	(Optional) Insert a frame count number. (Range: 1-65535)
interval	(Optional) Specifies a time between frames transmission. (1s 10s 1min 10min)

Default

Not transmitted.

Command Modes

Global configuration.

Command History

Release	Modification
11.2.10	This command was introduced.

Usage Guidelines

Within a given Maintenance Association and MEP, there are some time constraints for configuration of Delay Measurement Probes.

Each Probe takes some time to be executed, which is determined by **interval** and **count** parameters. A given MEP might have several probes configured.

The sum of the necessary time for all Probes of a given MEP must be smaller than the lowest Probe periodicity. For instance, suppose the following running configuration:

```
(...)
delay-measurement 1
  interval 3
  ma MyMaName mep id 1 remote-mep id 2 count 6 interval 10
delay-measurement 2
  interval 10
  ma MyMaName mep id 1 remote-mep id 3 count 6 interval 10
(...)
```

The necessary time for each configured probe is 1 minute, so the total time is 2 minutes. Probe 1 has the lowest probe periodicity: 3 minutes.

So it is not possible to add a new Probe with periodicity lower than 2 minutes.

Example

This example shows how to configure delay-measurement parameters to the probe.

```
DmSwitch(config-cfm-probe-dm)#ma ma mep id 1 remote-mep id 2 count 2
DmSwitch(config-cfm-probe-dm)#
```

You can verify that was configured by entering the **show cfm probe delay-measurement** privileged EXEC command.

Related Commands

Command	Description
show cfm probe delay-measurement	CFM Probe Delay Measurement (DM) information.
show running-config interval	Shows the current operating configuration. Configure the interval between 2 delay-measurement probes.

Chapter 9. CFM Test Commands

cfm-test-tst

cfm-test-tst mac-swap src-mac *source MAC* **dst-mac** *destination MAC* **vlan** *VLAN id*

no cfm-test-tst

Description

Enable/Disable CFM test mode.

This command allows performance tests using CFM TST packets.

Packets sent in configured VLAN will have their source and destination MACs swapped.

Entering **no cfm-test-tst** command, test mode is disabled.

Syntax

Parameter	Description
<i>source MAC</i>	Specifies the source MAC used in CFM TST packets.
<i>destination MAC</i>	Specifies the destination MAC used in CFM TST packets.
<i>VLAN id</i>	Specifies the VLAN used during the test.

Command Modes

Global configuration.

Command History

Release	Modification
14.10.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable CFM test mode.

```
DmSwitch(config)#cfm-test-tst swap-mac src-mac 00:04:DF:6C:78:A5 dst-mac 00:00:00:00:00:01 vlan 1000
DmSwitch(config)#
```

You can verify that the CFM test mode was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
loopback internal	Configures Loopback Internal for Ethernet port.

Chapter 10. E-LMI Commands

uni-c

uni-c interface ethernet [*unit-number/*] *port-number*

no uni interface ethernet [*unit-number/*] *port-number*

Description

Configures a User Network Interface (UNI) on Customer Edge device for a specific interface.

Inserting **no** as a prefix for this command will disable the UNI configuration.

Syntax

Parameter	Description
interface ethernet [<i>unit-number/</i>] <i>port-number</i>	Creates/Edits an UNI instance.

Default

No default is defined.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create/edit an User Network Interface (UNI) on the customer equipment for the

interface ethernet 5.

```
DmSwitch(config-elmi)#uni-c interface ethernet 5
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was set by entering the **show elmi interface ethernet 5** privileged EXEC command.

Related Commands

Command	Description
show elmi	Shows Ethernet Local Management Interface settings.
show running-config	Shows the current operating configuration.
elmi	Enters on Ethernet Local Management Interface protocol configuration mode.

uni-n

uni-n interface ethernet [*unit-number/*] *port-number*

no uni interface ethernet [*unit-number/*] *port-number*

Description

Configures a User Network Interface (UNI) on Provider Edge devices.

Inserting **no** as a prefix for this command will disable the UNI configuration.

Syntax

Parameter	Description
interface ethernet [<i>unit-number/</i>] <i>port-number</i>	Creates/Edits an UNI instance.

Default

No default is defined.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create/edit an User Network Interface (UNI) on provider equipment for interface ethernet 5.

```
DmSwitch(config-elmi)#uni-n interface ethernet 5
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was set by entering the **show elmi interface ethernet 5** privileged EXEC command.

Related Commands

Command	Description
show elmi	Shows Ethernet Local Management Interface settings.
show running-config	Shows the current operating configuration.
elmi	Enters on Ethernet Local Management Interface protocol configuration mode.

Chapter 11. E-LMI UNI-C Commands

polling-counter

polling-counter *value*

no polling-counter

Description

Configures polling counter value on Customer Edge devices.

Inserting **no** as a prefix for this command will reset the polling counter value to its default.

Syntax

Parameter	Description
<i>value</i>	Value for polling counter. (Range: 1-65535).

Default

The default polling counter value is 360.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set a polling-counter.

```
DmSwitch(config-elmi-uni-c)#polling-counter 100
```

```
DmSwitch(config-elmi-uni-c) #
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
show elmi	Shows Ethernet Local Management Interface settings.
show running-config	Shows the current operating configuration.
elmi	Enters on Ethernet Local Management Interface protocol configuration mode.

polling-timer

polling-timer *value*

no polling-timer

Description

Configures polling timer value on Customer Edge devices.

Inserting **no** as a prefix for this command will reset the polling timer to its default value.

Syntax

Parameter	Description
<i>value</i>	Value for polling timer. (Range: 5-30)

Default

The default polling timer value is 10 seconds.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the polling timer for an UNI instance on the customer equipment.

```
DmSwitch(config-elmi-uni-c)#polling-timer 20
DmSwitch(config-elmi-uni-c)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>elmi</code>	Enters on Ethernet Local Management Interface protocol configuration mode.

status-counter

status-counter *value*

no status-counter

Description

Configures status counter value on Customer Edge devices.

Inserting **no** as a prefix for this command will reset the status counter to its default value.

Syntax

Parameter	Description
<i>value</i>	Value for status counter. (Range: 2-10)

Default

The default status counter value is 4.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the status counter on customer equipment.

```
DmSwitch(config-elmi-uni-c)#status-counter 5
DmSwitch(config-elmi-uni-c)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>elmi</code>	Enters on Ethernet Local Management Interface protocol configuration mode.

Chapter 12. E-LMI UNI-N Commands

evc

```
evc name customer-vlan-list { any | [ default-evc ] [ untagged ] { vlan-id | range first-vlan-id last-vlan-id } [ vlan-id | range first-vlan-id last-vlan-id ] }
```

```
no evc name
```

Description

Assigns an existing EVC to an existing UNI-N.

Syntax

Parameter	Description
<i>name</i>	EVC identifier of an existing EVC (up to 32 characters).
any	All VLANs and untagged frames.
default-evc	(Optional) Default EVC.
untagged	(Optional) Untagged frames.
<i>vlan-id</i>	VLAN Identifier. (Range: 1-4094).
range <i>first-vlan-id last-vlan-id</i>	VLAN range. (Range: 1-4094)

Default

No default is defined.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Parameter **any** can be configured only if EVC map type is all to one bundling.

Parameter **default-evc** can be configured only if EVC map type is bundling.

Example

This example shows how to assign an existing EVC to an existing UNI-N.

```
DmSwitch(config-elmi-uni-n)#evc EVC_NAME customer-vlan-list any
DmSwitch(config-elmi-uni-n)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
show elmi	Shows Ethernet Local Management Interface settings.
show running-config	Shows the current operating configuration.
elmi	Enters on Ethernet Local Management Interface protocol configuration mode.
evc	Creates an Ethernet Virtual Circuit.
cfm	Enables Connectivity Fault Management (CFM) and create a Maintenance Domain (MD).
evc-map-type	Configures EVC map type on an UNI-N.

evc-map-type

```
evc-map-type { all-to-one-bundling | bundling | service-multiplexing }
```

```
no evc-map-type
```

Description

Configures EVC map type for an UNI-N instance on Provider Edge devices.

Inserting **no** as a prefix for this command will reset the EVC map type to its default value.

Syntax

Parameter	Description
all-to-one-bundling	Configures EVC map type to all to one bundling.
bundling	Configures EVC map type to bundling.
service-multiplexing	Configures EVC map type to all to service multiplexing.

Default

The default EVC map type is bundling.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure an EVC map type.

```
DmSwitch(config-elmi-uni-n)#evc-map-type bundling
DmSwitch(config-elmi-uni-n)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>elmi</code>	Enters on Ethernet Local Management Interface protocol configuration mode.
<code>evc</code>	Creates an Ethernet Virtual Circuit.

polling-verification-timer

polling-verification-timer *value*

no polling-verification-timer

Description

Configures polling verification timer value on Provider Edge devices.

Inserting **no** as a prefix for this command will reset the polling verification timer to its default value.

Syntax

Parameter	Description
<i>value</i>	Value for polling verification timer. (Range: 5-30)

Default

15 seconds.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

UNI-N polling-verification-timer should be greater than polling-timer configured in UNI-C.

Example

This example shows how to set the polling verification timer on provider equipment.

```
DmSwitch(config-elmi-uni-n)#polling-verification-timer 15
DmSwitch(config-elmi-uni-n)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>elmi</code>	Enters on Ethernet Local Management Interface protocol configuration mode.

status-counter

status-counter *value*

no status-counter

Description

Configures status counter value on Provider Edge devices.

Inserting **no** as a prefix for this command will reset the status counter to its default value.

Syntax

Parameter	Description
<i>value</i>	Value for status counter. (Range: 2-10)

Default

The default status counter value is 4.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set a status counter.

```
DmSwitch(config-elmi-uni-n)#status-counter 5
DmSwitch(config-elmi-uni-n)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>elmi</code>	Enters on Ethernet Local Management Interface protocol configuration mode.

id

id *name*

no id

Description

Configures UNI identifier on Provider Edge devices.

Inserting **no** as a prefix for this command will reset the identifier.

Syntax

Parameter	Description
<i>name</i>	UNI identifier. (Up to 64 characters)

Default

No default is defined.

Command Modes

E-LMI configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure UNI identifier text on customer equipment.

```
DmSwitch(config-elmi-uni-n)#id UNI_ID
DmSwitch(config-elmi-uni-n)#
```

You can verify that the information was set by entering the **show elmi** privileged EXEC command.

Related Commands

Command	Description
<code>show elmi</code>	Shows Ethernet Local Management Interface settings.
<code>show running-config</code>	Shows the current operating configuration.
<code>elmi</code>	Enters on Ethernet Local Management Interface protocol configuration mode.

Chapter 13. HQoS Commands

service

```
service { new | id } { 802.1p priority | dscp dscp-value } committed CIR CBS peak PIR PBS [  
action parameters | remark text ]
```

```
no service id
```

Description

Create or configure an HQoS service. HQoS service is used to assure that a determined traffic type (VoIP, multimedia, internet, etc.) will respect their attributed bandwidth.

Inserting **no** as a prefix for this command will delete the HQoS service specified.

Syntax

Parameter	Description
new	Create a new HQoS service
<i>id</i>	Select an HQoS service to edit by ID
Action parameters	Add an action to the service
802.1p <i>priority</i>	Change packet and internal 802.1p priority value
dscp <i>ip-dscp-value</i>	Change Differentiated Services Code Point
green-802.1p <i>priority</i>	Change packet and internal 802.1p priority of green packet
green-dscp <i>ip-dscp-value</i>	Change Differentiated Services Code Point of green packet
green-int-802.1p <i>priority</i>	Change internal 802.1p priority of green packet
int-802.1p <i>priority</i>	Change internal 802.1p priority value
yellow-dscp <i>ip-dscp-value</i>	Change Differentiated Services Code Point of yellow packet
yellow-802.1p <i>priority</i>	Change packet and internal 802.1p priority of yellow packet
yellow-int-802.1p <i>priority</i>	Change internal 802.1p priority of yellow packet
Other parameters	Description
802.1p <i>priority</i>	802.1p priority related to the service
dscp <i>dscp-value</i>	DSCP related to the service
committed <i>CIR CBS</i>	CIR in kbit/s (64 kbit/s granularity) and CBS in kbyte (power of 2)
peak <i>PIR PBS</i>	PIR in kbit/s (64 kbit/s granularity) and PBS in kbyte (power of 2)
remark <i>text</i>	Add a remark text

Default

By default, no service is created.

A new service has no actions if no action is specified.

Command Modes

Privileged EXEC.

Global configuration.

Command History

Release	Modification
11.4	This command was introduced.
12.0	Added the possibility to add actions to service.

Usage Guidelines

The HQoS services derives from domains. Therefore a domain must exist to create a new service.

The service classifies the packets according to its CIR and PIR values. Next discards the packets that not respect the service rules.

The sum of the CIR of all domain's services must not exceed it's rate limit. And also, the service's PIR must be under the domain's rate-limit.

Services are indentified by an unique DSCP or 802.1p.

Optionally, an action could be added to the service. The marking of 802.1p, internal 802.1p or DSCP of packets not discarded by HQoS is responsibility of this action. This can be done aiming an internal reorganization of the traffic.

Example

This example shows how to create an HQoS service that guarantees a CIR of 1024kbit/s and PIR of 512kbit/s for the service identified by DSCP 2.

```
DmSwitch(config-hqos-domain-1)#service new dscp 2 committed 1024 4 peak 512 4
DmSwitch(config-hqos-domain-1)#
```

Another example, showing how to edit the HQoS with id 1 and DSCP 10, changing its CIR to 2048kbit/s and PIR to 10048kbit/s, and also adding an action to change the yellow packets' DSCP to 15.

```
DmSwitch(config-hqos-domain-1)#service 1 dscp 10 committed 2048 4 peak 10048 4 action yellow-dscp 15
DmSwitch(config-hqos-domain-1)#
```

You can verify that the configuration was created by entering the **show hqos 1 service** privileged EXEC command.

Related Commands

Command	Description
hqos	Creates or configures an HQoS domain
show hqos	Shows HQoS information.
show running-config	Shows the current operating configuration.

Chapter 14. Interface Bundle Commands

bundle circuit-name

circuit-name [*text*]

no circuit-name

Description

This command is used to define a label for the interface.

Inserting **no** as a prefix for this command will remove the configured circuit name.

Syntax

Parameter	Description
text	"text" Circuit name

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The circuit name cannot be longer than 127 characters.

Example

This example shows how to set a circuit name for an interface.

```
DM4000(config)#interface bundle 1
```

```
DM4000(config-if-bundle-1/1)#circuit-name abc001
```

You can verify that the command was executed by entering the **show interface bundle 1** user EXEC command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface

bundle destination-bundle

destination-bundle [*bundle-id*]

no destination-bundle

Description

Use this command to define a destination bundle id for current bundle.

Inserting **no** as a prefix for this command will remove the configured destination bundle.

Syntax

Parameter	Description
bundle-id	1-8063 Destination Bundle ID.

Default

Default destination bundle is 1.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to set destination bundle for a given bundle.

```
DM4000(config)#interface bundle 5
DM4000(config-if-bundle-1/5)#destination-bundle 6
```

You can verify that the information was modified by entering the **show interface bundle 5** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle destination-ip-address

destination-ip-address [*ip-address*]

no destination-ip-address

Description

Use this command to define a destination ip address for current interface.

Inserting **no** as a prefix for this command will remove the configured destination-ip-address.

Syntax

Parameter	Description
ip-address	destination ip address

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to set a destination address for interface bundle 2.

```
DM4000(config)#interface bundle 2
DM4000(config-if-bundle-1/2)#destination-ip-address 10.0.0.254
```

You can verify that the command was executed by entering the **show interface bundle 1** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface
<code>ip-next-hop</code>	Defines bundle ip-next-hop

bundle destination-mac

destination-mac [*mac address*]

no destination-mac

Description

Use this command to define a destination mac address for current bundle.

Inserting **no** as a prefix for this command will remove the configured destination mac.

Syntax

Parameter	Description
mac address	destination MAC address (XX:XX:XX:XX:XX:XX)

Default

Default destination mac is 00:00:00:00:00:00.

Command Modes

Interface configuration.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to set destination mac for a given bundle.

```
DM4000(config)#interface bundle 5
DM4000(config-if-bundle-1/5)#destination-mac 00:04:DF:63:AE:B5
```

You can verify that the information was modified by entering the **show interface bundle 5** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle dscp

dscp [*value*]

no dscp

Description

Used to classify the traffic, setting the Differentiated Services Codepoint.

Inserting **no** as a prefix for this command will remove the configured dscp.

Syntax

Parameter	Description
dscp <i>value</i>	0-63 Specifies the Differentiated Services Codepoint.

Default

Default value is 0.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to configure dscp on the current interface.

```
DM4000(config)#interface bundle 1
DM4000(config-if-bundle-1/1)#dscp 25
```

You can verify that the command was executed by entering the **show interface bundle 1** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle ecid

```
ecid { remote } ecid-id
```

```
no ecid remote
```

Description

Use the command `ecid remote` to define a ECID value to be transmitted for current bundle.

Inserting **no** as a prefix for this command will remove the configured `ecid remote`.

Syntax

Parameter	Description
<code>remote</code>	0-1048575 ECID value limits.

Default

Default `ecid remote` is 0.

Command Modes

Interface configuration.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to set `ecid remote`.

```
DM4000(config)#interface bundle 5
DM4000(config-if-bundle-1/5)#ecid remote 4
DM4000(config-if-bundle-1/5)#no shutdown
```

You can verify that the command was executed by entering the **show interface bundle 5** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle ip-next-hop

ip-next-hop [*ip-address*]

no ip-next-hop

Description

Define an address of next hop of the network. If none is defined, it use destination-ip-address for ARP requests.

Inserting **no** as a prefix for this command will remove the configured ip-next-hop.

Syntax

Parameter	Description
ip-address	ip address of next hop.

Default

Destination IP address is used if ip-next-hop is not configured.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to define a next hop address.

```
DM4000(config)#interface bundle 10
DM4000(config-if-bundle-1/10)#ip-next-hop 10.10.10.10
```

You can verify that the command was executed by entering the **show interface bundle 10** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface
<code>destination-ip-address</code>	Defines bundle destination ip address

bundle jitter-buffer

jitter-buffer [*size*]

no jitter-buffer

Description

Use the jitter-buffer command to define how long is the jitter buffer of the current interface. Its used to attenuate the jitter caused by the ethernet network.

Inserting **no** as a prefix for this command will remove the configured jitter-buffer.

Syntax

Parameter	Description
size	1.00-496.00 (Max. Range) Jitter buffer size in ms.

Default

Default is 10.000 ms.s

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The value of *jitter-buffer* must be multiple of *packet-delay* . $packet-delay * 2 =$ minimum jitter. $packet-delay * (124/2) =$ maximum jitter. $(2 * jitter\ buffer) / packet-delay$ must be equal to zero. To configure bundle interface must be disabled.

Example

This example shows how to set jitter-buffer size of bundle 1 to 15 ms.

```
DM4000(config)#interface bundle 1
DM4000(config-if-bundle-1/1)#jitter-buffer 15
```

You can verify that the command was executed by entering the **show interface bundle 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface
packet-delay	Defines a value for packet-delay

bundle jitter-buffer-history

[no] jitter-buffer-history

Description

Use the jitter-buffer-history command to enable Jitter-Buffer occupation level monitoring.
Inserting **no** as a prefix for this command will disable recording.

Syntax

No parameter accepted.

Default

Enabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Example

This example shows how to disable interface bundle 10 jitter-buffer-history recording.

```
DM4000(config)#interface bundle 10
DM4000(config-if-bundle-1/10)#no jitter-buffer-history
```

You can verify that the parameter has been disabled by entering the **show this** privileged EXEC command.

Related Commands

Command	Description
jitter-buffer-history interval	Configure jitter-buffer-history sample interval.

bundle jitter-buffer-history interval

`jitter-buffer-history interval seconds`

`no jitter-buffer-history interval`

Description

Use the jitter-buffer-history interval command to configure interval to sample Jitter-Buffer-History.

Inserting **no** as a prefix for this command will restore default interval value.

Syntax

Parameter	Description
<i>seconds</i>	Specifies the interval to sample Jitter-Buffer value. (Range: 10-21600)

Default

The default value is 1200 seconds (20 minutes).

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Example

This example shows how to configure interface bundle 10 jitter-buffer-history interval to sample each 100 seconds.

```
DM4000 (config)#interface bundle 10
DM4000 (config-if-bundle-1/10)#jitter-buffer-history interval 100
```

You can verify that the parameter has been configured by entering the **show this** privileged EXEC command.

Related Commands

Command	Description
<code>jitter-buffer-history</code>	Enable/Disable jitter-buffer-history recording.

bundle lost-pkt-fill

```
lost-pkt-fill { automatic | idle-byte | repeat-last-data }
```

```
no lost-pkt-fill
```

Description

Configures lost packet fill.

Inserting **no** as a prefix for this command, it will resets lost packet fill to its default value.

Syntax

Parameter	Description
automatic	Automatically choose how to fill lost packets.
idle-byte	Fill lost packet with idle byte.
repeat-last-data	Fill lost packet with last valid data received.

Default

Lost-pkt-fill default value is repeat-last-data.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Bundle interface must be disabled before using lost-pkt-fill command.

Example

This example shows how to set lost packet fill in the bundle interface 1.

```
DM4000(config)#interface bundle 1/1
DM4000(config-if-bundle-1/1)#lost-pkt-fill automatic
DM4000(config-if-bundle-1/1)#
```

You can verify which test are enable by entering the **show interfaces bundle** user EXEC configuration command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface
show interfaces status	Shows interface configuration status.
show running-config	Shows the current operating configuration.

bundle lops-limits

lops-limits *entry value exit value*

no lops-limits

Description

Use this command to define the quantity of loss packets per frame that trigger the alarm of bundle fail (entry) and recovery (exit).

Inserting **no** as a prefix for this command will set lops-limits to its default value.

Syntax

Parameter	Description
entry	Specifies entry LOPS limits. (Range: 1-255)
exit	Specifies exit LOPS limits. (Range: 1-255)

Default

Default is entry limit 10 and exit limit 2.

Command Modes

Interface configuration.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled.

Example

This example shows how to configure interface bundle 1 of unit 2 to use lops-limits entry 20 and exit 5.

```
DM4000(config)#interface bundle 2/1
DM4000(config-if-bundle-2/1)#lops-limits entry 20 exit 5
```

You may check the configuration using the command *show interfaces bundle 2/1*

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle r-bit-send-rai

[no] r-bit-send-rai

Description

Use the r-bit-send-rai command to enable RAI sending when R bit enabled is received in the CESoP Ethernet packet.

Inserting **no** as a prefix for this command will disable RAI sending.

Syntax

No parameter accepted.

Default

Enabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Example

This example shows how to enable interface bundle 10 r-bit-send-rai.

```
DM4000(config)#interface bundle 10
DM4000(config-if-bundle-1/10)#r-bit-send-rai
```

You can verify that the parameter has been disabled by entering the **show this** privileged EXEC command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface

bundle packet-delay

packet-delay *delay*

no packet-delay

Description

Use this command to define how long bundle interface takes to switch data from TDM to packets.

Inserting **no** as a prefix for this command will remove the configured packet-delay.

Syntax

Parameter	Description
<code>delay</code>	How much time (ms) is added to delay.

Default

Default packet delay is 1.000 ms

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command has been introduced.

Usage Guidelines

To configure bundle interface must be disabled. Values for delay must be multiple of 0.125 and between the range of 0.5 to 8.0. If defined line-type use CAS, packet-delay must be 2ms.

Example

This example shows how to define packet delay of 2.5 ms to the bundle 1 interface

```
DM4000(config)#interface bundle 1
DM4000(config-if-bundle-1/1)#shutdown
DM4000(config-if-bundle-1/1)#packet-delay 2.5
DM4000(config-if-bundle-1/1)#no shutdown
```

You may check the configured value by using the command **show interface bundle 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface
jitter-buffer	Defines bundle jitter-buffer size
line-type	Configure g704 line-type

bundle packet-loss-threshold

packet-loss-threshold [*loss percentage*]

no packet-loss-threshold

Description

Define the percentage of packet loss that trigger the alarm of bundle fail.

Inserting **no** as a prefix for this command will set packet-loss-threshold to its default value.

Syntax

Parameter	Description
packet-loss-threshold	Percentage of packets that can be lost until bundle become down.

Default

Default is 1%.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Configured percentage must be in steps of 0.1%. To configure bundle interface must be disabled.

Example

This example shows how to set a packet loss threshold of 15.3%

```
DM4000(config)#interface bundle 5
DM4000(config-if-bundle-1/5)#packet-loss-threshold 15.3
```

You can verify that the command was executed by entering the **show interface bundle 5** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface
<code>packet-delay</code>	Defines a value for packet-delay
<code>jitter-buffer</code>	Defines bundle jitter-buffer size

bundle psn-type

```
psn-type { udp | mef8 }
```

```
no psn-type
```

Description

Configure PSN header type.

Inserting **no** as a prefix for this command, it will reset psn-type to its default value.

Syntax

Parameter	Description
udp	Configure PSN to use IP and UDP headers.
mef8	Configure PSN to use MEF header.

Default

psn-type default value is udp.

Command Modes

Interface configuration.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

Bundle interface must be disabled before using psn-type command.

Example

This example shows how to set psn-type in the bundle interface 1.

```
DM4000(config)#interface bundle 1/1
DM4000(config-if-bundle-1/1)#psn-type mef8
DM4000(config-if-bundle-1/1)#
```

You can verify which test are enable by entering the **show interfaces bundle** user EXEC configuration command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface
show running-config	Shows the current operating configuration.

bundle qinq

qinq *vlan-id* **priority** *priority-level*

no **qinq**

Description

Use this command to define an vlan which the current bundle interface will use as external tag

Inserting **no** as a prefix for this command will remove the additional tag.

Syntax

Parameter	Description
vlan-id	Specifies VLAN ID used as QinQ external tag of the bundle interface. (Range: 1-4094)
priority-level	Specifies priority used in bundle interface. (Range: 0-7)

Default

By default QinQ vlan is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Used vlans must be already created.

Example

This example shows how to configure interface bundle 1 of unit 2 to use vlan 10 as internal vlan tag and vlan 20 as an external tag (QinQ).

```
DM4000(config-if-vlan-10)#interface bundle 2/1
DM4000(config-if-bundle-2/1)#vlan 10 priority 2
DM4000(config-if-bundle-2/1)#qinq 20 priority 2
```

You may check the configuration using the command *show interfaces bundle 2/1*

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface
<code>bundle vlan</code>	Defines which vlan current bundle interface will use.

bundle shutdown

shutdown

no shutdown

Description

Use the shutdown command to disable an interface.

Inserting **no** as a prefix for this command will enable the interface.

Syntax

No parameter accepted.

Default

Interface is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When enabling (*no shutdown*) a bundle interface, all coherence checks are done. If there is some inconsistent configuration an error message is displayed and the interface does not go up.

Example

This example shows how to enable interface bundle 10.

```
DM4000(config-if-g704-1/1)#interface bundle 10
DM4000(config-if-bundle-1/10)#no shutdown
```

You can verify that the bundle interface is up by entering the **show interfaces bundle 10** privileged EXEC command.

Related Commands

No related command.

bundle source-ip-address

source-ip-address *ip address*

no source-ip-address

Description

Set a source ip address for the current bundle interface

Inserting **no** as a prefix for this command will set source-ip-address to its default value.

Syntax

Parameter	Description
<i>ip address</i>	bundle source ip address

Default

Default is using interface PW source-ip-address.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Entered address must be a valid IP address.

Example

This example define the address 10.1.1.22 as the source address of interface bundle 1.

```
DM4000(config)#interface bundle 1
DM4000(config-if-bundle-1/1)#source-ip-address 10.1.1.22
```

The configuration may be checked using the command **show interfaces bundle 1** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle tdm-channel

```
tdm-channel { g704 } g704-id
```

```
no tdm-channel
```

Description

Use the command `tdm-channel` to map the current interface to an E1 interface.

Inserting **no** as a prefix for this command will remove the configured `tdm-channel`.

Syntax

Parameter	Description
<code>g704-id</code>	E1 interface id.

Default

By default all bundles are mapped to the first E1 interface.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

G704 interface must be enabled and bundle interface disabled, otherwise an error message is displayed.

Example

This example shows how to map bundle 5 to the second g704 interface.

```
DM4000(config-if-g704-1/2)#interface bundle 5
DM4000(config-if-bundle-1/5)#tdm-channel g704 2
DM4000(config-if-bundle-1/5)#no shutdown
```

You can verify that the command was executed by entering the **show interface bundle 5** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

bundle test

```
test { bert-error | bert-psn-side | bert-tdm-side | loop }
```

```
no test
```

Description

This command may be used to run different tests over the network. **bert-psn-side** , **bert-tdm-side** and **loop** may be saved on equipment configuration. The bert standart test used is 2^9-1 .

Inserting **no** as a prefix for this command will disable bundle interface tests.

Syntax

Parameter	Description
bert-error	Insert an error in a bert test.
bert-psn-side	Start bert packet switched network side test. (ethernet)
bert-tdm-side	Start bert tdm side test.
loop	Start a loop test on the interface.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Tests will start only if interface is enabled.

To insert a bert error is necessary that a bert test is running.

Example

This example shows how to start bert test at bundle 5 and insert an error.

```
DM4000 (config) #interface g704 1
DM4000 (config-if-g704-1/1) #no shutdown
DM4000 (config-if-g704-1/1) #interface bundle 5
DM4000 (config-if-bundle-1/5) #no shutdown
DM4000 (config-if-bundle-1/5) #test bert-tdm-side
DM4000 (config-if-bundle-1/5) #test bert-error
```

You can verify that the command was executed by entering the **show interface bundle 5** privileged EXEC command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface
show interfaces test bundle	the Section called <i>show interfaces test bundle</i> in Chapter 2

bundle timeslots

timeslots [*first-timeslot*] [*number-of-timeslots*]

no timeslots

Description

Define an initial timeslot and how many the bundle interface use of the mapped tdm-channel.

Inserting **no** as a prefix for this command will remove the configured timeslots.

Syntax

Parameter	Description
<i>First time slot</i>	0-31 (Max. Range) First time slot
<i>Number of time slots</i>	1-32 (Max. Range) Number of time slots

Default

By default the bundle interface uses all timeslots, initial timeslot 0 and 32 timeslots.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To configure bundle interface must be disabled. There must be a coherence between used timeslots and the line-type configured on g704 interface.

Example

This example show a bundle interface configured to use from timeslot 5 to timeslot 15.

```
DM4000(config)#interface bundle 1
DM4000(config-if-bundle-1/1)#shutdown
DM4000(config-if-bundle-1/1)#timeslots 5 10
DM4000(config-if-bundle-1/1)#no shutdown
```


You may check that the configuration was applied by the command **show interfaces bundle 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces bundle	Shows information about CESoP bundle interface
line-type	Configure g704 line-type
tdm-channel	Maps bundle in E1 interface

bundle vlan

vlan *vlan-id* **priority** *priority-level*

no vlan

Description

Use this command to define in which vlan current bundle interface will work.

Inserting **no** as a prefix for this command will set VLAN to its default value.

Syntax

Parameter	Description
vlan-id	Specifies VLAN ID used in bundle interface. (Range: 1-4094)
priority-level	Specifies priority used in bundle interface. (Range: 0-7)

Default

Default is using interface PW VLAN.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Selected vlan must .

Example

This example shows how to configure interface bundle 1 of unit 2 to use vlan 10.

```
DM4000(config-if-vlan-10)#interface bundle 2/1
DM4000(config-if-bundle-2/1)#vlan 10 priority 2
```

You may check the configuration using the command *show interfaces bundle 2/1*

Related Commands

Command	Description
<code>show interfaces bundle</code>	Shows information about CESoP bundle interface

Chapter 15. Interface Ethernet/Port-channel Commands

capabilities

```
capabilities { 10full | 10half | 100full | 100half | 1000full | flowcontrol [
transmit | receive ] }
```

```
no capabilities { 10full | 10half | 100full | 100half | 1000full | flowcontrol [
transmit | receive ] }
```

Description

Configure interface port capabilities for autonegotiation.

Inserting **no** as a prefix for this command will disable the specified capability.

Syntax

Parameter	Description
10full	Advertises 10Mbps full-duplex operation support.
10half	Advertises 10Mbps half-duplex operation support.
100full	Advertises 100Mbps full-duplex operation support.
100half	Advertises 100Mbps half-duplex operation support
1000full	Advertises 1000Mbps full-duplex operation support.
flowcontrol	Advertises flow control operation support.
transmit	(Optional) Advertises support of PAUSE frames for transmission.
receive	(Optional) Advertises support of PAUSE frames for reception.

Default

All supported speed and duplex capabilities enabled.

Flow control capabilities disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

When enabling flow control advertisement without specifying transmit or receive, flow control will be advertised for both of them.

Example

This example shows how to set interface capabilities for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#capabilities 100full
DmSwitch(config-if-eth-1/5)#no capabilities 10half
DmSwitch(config-if-eth-1/5)#no capabilities 10full
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was set by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
flowcontrol	Configures Flow Control for Ethernet interfaces.
negotiation	Controls autonegotiation status for an Ethernet interface.
speed-duplex	Configures speed and duplex operation.
show interfaces status	Shows interface configuration status.
show interfaces table configuration	Shows interface's configuration table.

description

description *string*

no description

Description

Use the description command to insert some descriptive text for Ethernet and Port-Channel interfaces.

Inserting **no** as a prefix for this command will remove the description.

Syntax

Parameter	Description
<i>string</i>	Some description for the interface. (Size: 128 characters)

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set a description for an Ethernet interface.

```
DmSwitch(config-if-eth-1/2)#description GatewayInterface
DmSwitch(config-if-eth-1/2)#
```

You can verify that the information was inserted by entering the **show interfaces status ethernet** user EXEC command.

Related Commands

Command	Description
<code>show interfaces status</code>	Shows interface configuration status.

dot1x captive-portal

dot1x captive-portal

no dot1x captive-portal

Description

Enables Captive Portal on the interface.

Inserting **no** as a prefix for this command will remove the Captive Portal on the interface.

Syntax

No parameter accepted.

Default

The 802.1X Captive Portal option is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

When enabled, this command redirects the user to an internal web page to provide authentication credentials.

The user will only be redirected to the internal captive-portal web page if its terminal does not have support to the protocol IEEE 802.1x.

When re-auth-enable is enabled, user loses network connectivity and must manually provide credentials to reestablish network connection periodically.

Example

This example shows how to enable Captive Portal.

```
DmSwitch(config)#interface ethernet 5
DmSwitch(config-if-eth-1/5)#dot1x captive-portal
DmSwitch(config-if-eth-1/5)#
```


You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x guest-vlan	Specifies an active VLAN as an 802.1X guest VLAN.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x guest-vlan

dot1x guest-vlan *id*

no dot1x guest-vlan

Description

Specifies an active VLAN as an 802.1X guest VLAN.

Inserting **no** as a prefix for this command will remove the guest VLAN on the interface.

Syntax

Parameter	Description
<i>id</i>	VLAN ID. (Range: 1-4094)

Default

The 802.1X guest VLAN option is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAPOL request/identity frame. The VLAN must be created to configure the 802.1X guest VLAN interface ethernet parameter. The **show vlan table** command shows whether the interface was put into the guest VLAN.

Example

This example shows how to configure VLAN 3 as an 802.1X guest VLAN.

```
DmSwitch(config)#interface vlan 3
DmSwitch(config-if-vlan-3)#interface ethernet 5
DmSwitch(config-if-eth-1/5)#dot1x guest-vlan 3
```

```
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x restricted-vlan	Specifies an active VLAN as an 802.1X restricted VLAN.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x mac-authentication

`dot1x mac-authentication`

`no dot1x mac-authentication`

Description

Use the `dot1x mac-authentication` command to enable the MAC authentication

Inserting **no** as a prefix for this command will disable the feature.

Syntax

No parameter accepted.

Default

Authentication is disable.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

When MAC authentication is enable, clients that have no support to IEEE 802.1x protocol are authenticated using its MAC addresses. The MAC addresses must be configured in the list of users in RADIUS server.

Example

This example shows how to enable dot1x MAC authentication for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x mac-authentication
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

freeradius MAC-user configuration example, /etc/freeradius/users

```
0004df010203 Cleartext-Password := "0004df010203"
```

Related Commands

Command	Description
<code>dot1x system-auth-control</code>	Configures global options for 802.1X.
<code>dot1x captive-portal</code>	Configures global options for 802.1X.
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x re-auth-max</code>	Sets the maximum EAP request/identity packet retransmissions.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x max-req

dot1x max-req *value*

no dot1x max-req

Description

Use the dot1x max-req command to set the maximum EAP request/identity packet retransmissions.

Inserting **no** as a prefix for this command will return the maximum EAP request/identity packet retransmissions to its default value.

Syntax

Parameter	Description
<i>value</i>	Max request count. (Range: 1-10)

Default

The default max-req value is 2.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
12.2	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to set the maximum EAP request/identity packet retransmissions for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x max-req 3
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x port-control	Sets the dot1x mode on a port interface.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
show dot1x	Shows 802.1X information.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
show running-config	Shows the current operating configuration.

dot1x max-users

dot1x max-users *number*

no dot1x max-users

Description

Use the dot1x max-users command to set the maximum users that can be learned via 802.1X per port. Inserting **no** as a prefix for this command will return the maximum 802.1X users to its default value.

Syntax

Parameter	Description
<i>number</i>	Max users. (Range: 1-256)

Default

The default max-users per port is 16.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Set max-users per port is only effective when host-mode on interface is multi-auth.

Example

This example shows how to set the maximum 802.1X users for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x host-mode multi-auth  
DmSwitch(config-if-eth-1/5)#
```

```
DmSwitch(config-if-eth-1/5)#dot1x max-users 100  
DmSwitch(config-if-eth-1/5)#
```


You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x max-users	Configures global options for 802.1X.
dot1x host-mode	Sets the dot1x host-mode on a port interface.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x port-control

```
dot1x port-control { auto | force-auth | force-unauth }
```

```
no dot1x port-control
```

Description

Use the dot1x port-control command to set the dot1x mode on a ethernet port.

Inserting **no** as a prefix for this command will return port-control mode to its default value.

Syntax

Parameter	Description
auto	Requires dot1x-aware client RADIUS server authorization.
force-auth	Configures the port to grant access to all clients.
force-unauth	Configures the port to deny access to all clients.

Default

The default mode is force-auth.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This interface configuration is only effective when enable the global configuration, by the command "dot1x system-auth-control"

Example

This example shows how to configure the port to grant access to all clients.

```
DmSwitch(config-if-eth-1/5)#dot1x port-control force-auth
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show dot1x interface ethernet [unit-number/] port-number** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x host-mode

```
dot1x host-mode { single | multi-auth }
```

```
no dot1x host-mode
```

Description

Use the dot1x host-mode command to set the dot1x host-mode on a ethernet port.

Inserting **no** as a prefix for this command will return host-mode to its default value.

Syntax

Parameter	Description
single	Configures the port to authenticate one client, grant access to all clients.
multi-auth	Configures the port to authenticate clients individually, grant or deny access to each client.

Default

The default mode is single.

Command Modes

Interface configuration.

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

The maximum number of individually authenticated users is limited by the parameter *max-users*.

Example

This example shows how to configure the port to authenticate each client individually.

```
DmSwitch(config-if-eth-1/5)#dot1x host-mode multi-auth
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show dot1x interface ethernet [unit-number/] port-number** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x max-users	Configures global options for 802.1X.
dot1x max-users	Sets the maximum users that can be learned via 802.1X per port.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x quiet-period

```
dot1x quiet-period { timeout }
```

```
no dot1x quiet-period
```

Description

Configure quiet period for a given ethernet port.

Inserting **no** as a prefix for this command will reset quiet period to default value.

Syntax

Parameter	Description
<i>timeout</i>	Timeout in seconds. (Range: 0-65535)

Default

The default value is 60.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

For a given interface, no authentication is allowed for some time after authentication failure to avoid denial of service attacks.

Example

This example shows how to set dot1x quiet period for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x quiet-period 600
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>dot1x system-auth-control</code>	Configures global options for 802.1X.
<code>dot1x captive-portal</code>	Configures global options for 802.1X.
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x re-auth-max</code>	Sets the maximum EAP request/identity packet retransmissions.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x re-auth-enable

dot1x re-auth-enable

no dot1x re-auth-enable

Description

Use the dot1x re-authentication command to enable/disable periodic re-authentication.

Inserting **no** as a prefix for this command will disable re-authentication.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

When enabled, this command periodically (with a time given by the **dot1x re-auth period**) forces a reauthentication of the suplicant.

If the new authentication succeeds, user is not disconnected and no data is lost. If authentication fails, user is disconnected. When user is authenticated by captive-portal, he loses network connectivity and must manually provide his credentials to reestablish network connection.

Example

This example shows how to enable periodic re-authentication for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x re-auth-enable
DmSwitch(config-if-eth-1/5)#
```


You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x port-control	Sets the dot1x mode on a port interface.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
dot1x	Enables or disables periodic re-authentication.
ddot1x_re-authentication	
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x re-authentication

`dot1x re-authentication`

`no dot1x re-authentication`

Description

Use the `dot1x re-authentication` command to enable/disable periodic re-authentication.

Inserting **no** as a prefix for this command will disable re-authentication.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
12.2	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to enable periodic re-authentication for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x re-authentication
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x port-control	Sets the dot1x mode on a port interface.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x re-auth-max

dot1x re-auth-max *value*

no dot1x re-auth-max

Description

Use the dot1x re-auth-max command to set the maximum EAP request/identity packet retransmissions.

Inserting **no** as a prefix for this command will return the maximum EAP request/identity packet retransmissions to its default value.

Syntax

Parameter	Description
<i>value</i>	Max request count. (Range: 1-10)

Default

The default re-auth-max value is 2.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command configure a certain number of reauthentication attempts to the suplicant. Used only if reauthentication is enabled.

Example

This example shows how to set the maximum EAP request/identity packet retransmissions for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x re-auth-max 3
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x port-control	Sets the dot1x mode on a port interface.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x server-timeout	Defines dot1x timeout value.
dot1x quiet-period	Defines dot1x quiet period timeout value.
show dot1x	Shows 802.1X information.
dot1x max-req	Sets the maximum EAP request/identity packet retransmissions.
show running-config	Shows the current operating configuration.

dot1x re-auth-period

```
dot1x re-auth-period { timeout }
```

```
no dot1x re-auth-period
```

Description

Use the dot1x re-auth-period command to define dot1x re-authentication period value for the ethernet port.

Inserting **no** as a prefix for this command will reset period to its default.

Syntax

Parameter	Description
<i>timeout</i>	Timeout in seconds. (Range: 1-65535)

Default

The default value is 3600.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command configures the interval between periodic reauthentication. Used only if reauthentication is enabled

Example

This example shows how to set dot1x re-authentication period for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x re-auth-timeout 600
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>dot1x system-auth-control</code>	Configures global options for 802.1X.
<code>dot1x captive-portal</code>	Configures global options for 802.1X.
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x quiet-period</code>	Defines dot1x quiet period timeout value.
<code>dot1x server-timeout</code>	Defines dot1x timeout value.
<code>dot1x re-auth-max</code>	Sets the maximum EAP request/identity packet retransmissions.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x restricted-vlan

dot1x restricted-vlan *id*

no dot1x restricted-vlan

Description

Specifies an active VLAN as an 802.1X restricted VLAN.

Inserting **no** as a prefix for this command will remove the restricted VLAN on the interface.

Syntax

Parameter	Description
<i>id</i>	VLAN ID. (Range: 1-4094)

Default

The 802.1X restricted VLAN option is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

When you configure a restricted VLAN, clients that are IEEE 802.1x-compliant and cannot access another VLAN because they fail the authentication process are put into the restricted VLAN. The VLAN must be created in order to configure the 802.1X restricted VLAN interface ethernet parameter. The **show vlan table** command shows whether the interface was put into the restricted VLAN.

Example

This example shows how to configure VLAN 3 as an 802.1X restricted VLAN.

```
DmSwitch(config)#interface vlan 3
DmSwitch(config-if-vlan-3)#interface ethernet 5
DmSwitch(config-if-eth-1/5)#dot1x restricted-vlan 3
```



```
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x guest-vlan	Specifies an active VLAN as an 802.1X guest VLAN.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dot1x server-timeout

```
dot1x server-timeout { timeout }
```

```
no dot1x server-timeout
```

Description

Use the dot1x server-timeout command to define dot1x timeout value for the Ethernet interface.

Inserting **no** as a prefix for this command will reset timeout to its default value.

Syntax

Parameter	Description
<i>timeout</i>	Timeout in seconds. (Range: 1-65535)

Default

The default value is 30.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Configure timeout for communication with RADIUS authentication server.

Example

This example shows how to set dot1x timeout period for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x server-timeout 600
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>dot1x system-auth-control</code>	Configures global options for 802.1X.
<code>dot1x captive-portal</code>	Configures global options for 802.1X.
<code>dot1x default</code>	Configures global options for 802.1X.
<code>dot1x quiet-period</code>	Defines dot1x quiet period timeout value.
<code>dot1x re-auth-period</code>	Defines dot1x re-authentication period value.
<code>dot1x re-auth-max</code>	Sets the maximum EAP request/identity packet retransmissions.
<code>dot1x port-control</code>	Sets the dot1x mode on a port interface.
<code>dot1x re-auth-enable</code>	Enables or disables periodic re-authentication.
<code>show dot1x</code>	Shows 802.1X information.
<code>show running-config</code>	Shows the current operating configuration.

dot1x timeout

```
dot1x timeout { quiet-period timeout | re-authperiod timeout | tx-period timeout }
```

```
no dot1x timeout { quiet-period | re-authperiod | tx-period }
```

Description

Use the dot1x timeout command to define dot1x timeout values for the Ethernet interface.

Inserting **no** as a prefix for this command will remove dot1x timeout for the specified configuration passed as parameter.

Syntax

Parameter	Description
quiet-period	Time after Max Request Count before gets new client.
re-authperiod	Time after connected client must be re-authenticated.
tx-period	Time switch waits before re-transmitting EAP packet.
<i>timeout</i>	Timeout in seconds. (Range: 1-65535)

Default

The default value for quiet-period is 60.

The default value for re-authperiod is 3600

The default value for tx-period is 30.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
12.2	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to set dot1x quiet-period, re-authperiod and tx-period for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dot1x timeout quiet-period 600
DmSwitch(config-if-eth-1/5)#dot1x timeout re-authperiod 3600
DmSwitch(config-if-eth-1/5)#dot1x timeout tx-period 60
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
dot1x system-auth-control	Configures global options for 802.1X.
dot1x captive-portal	Configures global options for 802.1X.
dot1x default	Configures global options for 802.1X.
dot1x re-auth-max	Sets the maximum EAP request/identity packet retransmissions.
dot1x port-control	Sets the dot1x mode on a port interface.
dot1x quiet-period	Defines dot1x quiet period timeout value.
dot1x re-auth-period	Defines dot1x re-authentication period value.
dot1x re-auth-enable	Enables or disables periodic re-authentication.
dot1x server-timeout	Defines dot1x timeout value.
show dot1x	Shows 802.1X information.
show running-config	Shows the current operating configuration.

dscp-mapping

dscp-mapping

no dscp-mapping

Description

Use the dscp-mapping command to enable or disable DiffServ Code Point.

Inserting **no** as a prefix for this command will disable autonegotiation.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable DiffServ Code Point for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#dscp-mapping
DmSwitch(config-if-eth-1/5)#
```

You can verify that the DiffServ Code Point was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

flowcontrol

```
flowcontrol [ transmit | receive ]
```

```
no flowcontrol [ transmit | receive ]
```

Description

Configures flow control on interfaces.

Inserting **no** as a prefix for this command will disable flow control.

Syntax

Parameter	Description
transmit	(Optional) Enables PAUSE frames transmission for flowcontrol.
receive	(Optional) Enables PAUSE frames reception for flowcontrol.

Default

Flow control is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

When enabling flowcontrol without specifying transmit or receive, Flow Control will be enabled for both of them.

Fast Ethernet ports do not support asymmetric Flow Control. That is only supported by Gigabit ports.

Example

This example shows how to enable Flow Control for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#flowcontrol
```



```
DmSwitch(config-if-eth-1/5) #
```

You can verify that the configuration was set by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
flowcontrol	Configures Flow Control for Ethernet interfaces.
negotiation	Controls autonegotiation status for an Ethernet interface.
speed-duplex	Configures speed and duplex operation.
show interfaces status	Shows interface configuration status.
show interfaces table configuration	Shows interface's configuration table.

garp timer

```
garp timer { join join-timer | leave leave-timer | leaveall leaveall-timer }
```

```
no garp timer { join | leave | leaveall }
```

Description

Use the garp timer command to set the values for the join, leave and leaveall timers.

Inserting **no** as a prefix for this command will reset the join, leave or leaveall timers to default value.

Syntax

Parameter	Description
join	Specifies the join timer.
<i>join-timer</i>	The value to be entered in centiseconds. (Range: 20-1000)
leave	Specifies the leave timer.
<i>leave-timer</i>	The value to be entered in centiseconds. (Range: 60-3000)
leaveall	Specifies the leaveall timer.
<i>leaveall-timer</i>	The value to be entered in centiseconds. (Range: 500-18000)

Default

Join timer: 20 centiseconds.

Leave timer: 60 centiseconds.

Leaveall timer: 1000 centiseconds.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to garp timers for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#garp timer join 30
DmSwitch(config-if-eth-1/5)#garp timer leave 600
DmSwitch(config-if-eth-1/5)#garp timer leaveall 5000
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was set by entering the **show garp timer** privileged EXEC command.

Related Commands

Command	Description
bridge-ext gvrp timer	Enables GVRP globally for the switch.
show garp timer	Shows GARP properties.
show gvrp timer	Shows GVRP configuration.
show running-config timer	Shows the current operating configuration.
switchport gvrp timer	Enables GVRP for a specific port.

ip arp-protection trust

```
ip arp-protection trust
```

```
no ip arp-protection trust
```

Description

Configures a port as trusted for ARP Protection purposes.

Inserting **no** as a prefix for this command will set port as untrusted.

Syntax

No parameter accepted.

Default

Default value for port is untrusted.

Command Modes

Interface configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This configuration takes effect when interface is member of a VLAN with **ip arp-protection action block** enabled.

Example

This example shows how to activate ARP Protection trust configuration at unit/port.

```
DmSwitch(config)#interface ethernet 1/5
DmSwitch(config-if-eth-1/5)#ip arp-protection trust
DmSwitch(config-if-eth-1/5)#
```

You can verify that the ARP Protection trust configuration at unit/port was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip arp-protection	Sets ARP protection for the selected VLAN.

ip dhcp snooping trust

```
ip dhcp snooping trust
```

```
no ip dhcp snooping trust
```

Description

Configures a port as trusted for DHCP snooping purposes.

Inserting **no** as a prefix for this command will set port as untrusted.

Syntax

No parameter accepted.

Default

Default value for port is untrusted.

Command Modes

Interface configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

To take effect on DHCP snooping trust or untrust configuration, DHCP snooping must be globally enabled.

Example

This example shows how to activate DHCP Snooping trust configuration at unit/port.

```
DmSwitch(config)#interface ethernet 1/5
DmSwitch(config-if-eth-1/5)#ip dhcp snooping trust
DmSwitch(config-if-eth-1/5)#
```

You can verify that the DHCP Snooping trust configuration at unit/port was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP Snooping globally.
ip dhcp snooping	Enables DHCP Snooping at VLAN.
ip dhcp snooping verify mac-address	Enables configuration to verify mac-address on a DHCP Snooping message.

ipfix

ipfix

Description

Enables IPFIX on the Interface.

Inserting **no** as a prefix for this command will disable IPFIX on the specified interface.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Example

This example shows how to enable IPFIX on an Ethernet Interface.

```
DmSwitch(config-if-eth-1/5)#ipfix
```

To verify the IPFIX configuration enter the **show ipfix** command.

Related Commands

Command	Description
ipfix host	Configures an IPFIX collector.
ipfix flow-trigger	Configures IPFIX flow monitoring parameters.
show ipfix	Shows IPFIX configuration.

l2protocol-tunnel

```
l2protocol-tunnel { cdp | control-protocols { option-1 } | dot1x | eaps | erps |  
extended | gvrp | lacp | lldp | marker | oam | pagp | pvst | stp | udld | vtp }
```

```
no l2protocol-tunnel { cdp | control-protocols { option-1 } | dot1x | eaps | erps  
| extended | gvrp | lacp | lldp | marker | oam | pagp | pvst | stp | udld | vtp }
```

Description

Use the l2protocol-tunnel command to configure Layer 2 protocols tunneling for the Ethernet interface.

Inserting **no** as a prefix for this command will disable l2protocol-tunnel for the specified protocol.

Syntax

Parameter	Description
cdp	Enable/disable CDP packets tunneling
control-protocols option-1	Enable/disable Control Protocols MEF Ethernet Private Line (EPL) Option 1 packets tunneling
dot1x	Enable/disable DOT1X (802.1X) packets tunneling
eaps	Enable/disable EAPS packets tunneling
erps	Enable/disable ERPS packets tunneling
extended	Enable/disable Extended packets tunneling
gvrp	Enable/disable GVRP packets tunneling
lacp	Enable/disable LACP packets tunneling
lldp	Enable/disable LLDP packets tunneling
marker	Enable/disable Marker packets tunneling
oam	Enable/disable OAM packets tunneling
pagp	Enable/disable PAGP packets tunneling
pvst	Enable/disable PVST packets tunneling
stp	Enable/disable STP packets tunneling
udld	Enable/disable UDLD packets tunneling
vtp	Enable/disable VTP packets tunneling

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
3.2	The pvst parameter was added.
4.3	The lACP , pagp and udld parameters were added.
7.0	The dot1x , gvrp , marker and oam parameters were added.
12.4	The lldp parameter was added.
13.4	The eaps and erps parameters were added.
14.0	The control-protocols option-1 parameter was added.
14.4	The extended parameter was added.

Usage Guidelines

L2 protocol tunneling is based on destination MAC address modification for protocol packets. Protocol packets received on a port that has tunneling enabled will have their destination address changed to another address. With that destination address the packets will be transparently forwarded (flooded) through the network until some other port with tunneling enabled is reached.

You must use this command on ports that will convert protocol packets into tunneled packets and/or convert tunneled packets into protocol packets. The intermediate ports on the tunneling path must not have this command enabled so that they will only forward tunneled packets without modifications.

Example

This example shows how to enable STP packets tunneling for the interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#l2protocol-tunnel stp
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show l2protocol-tunnel** privileged EXEC command.

Related Commands

Command	Description
l2protocol-tunnel (Global configuration)	Configures a Layer 2 protocols tunneling.
show l2protocol-tunnel	Shows Layer 2 Protocols Tunneling information.
show running-config	Shows the current operating configuration.

lacp

```
lacp [ actor { admin-key key } ]
```

```
no lacp [ actor { admin-key } ]
```

Description

This command is no longer available. Since version 13.4, LACP should be enabled directly in the port-channel. Ethernet ports should be added as it's done for port-channels without LACP. The LACP protocol can no longer create or destroy port-channels dynamically nor it will add or remove ports that weren't previously configured.

Command History

Release	Modification
3.1	This command was introduced.
13.4	This command was removed.

Related Commands

Command	Description
<code>debug</code>	Enables the printing of debug messages.
<code>lacp actor port-priority</code>	Configure LACP port priority.
<code>show interfaces status</code>	Shows interface configuration status.
<code>show lacp counters</code>	Shows the LACP traffic counters.
<code>show lacp group</code>	Shows the LACP information by port-channel.
<code>show lacp internal</code>	Shows the LACP internal information.
<code>show lacp neighbors</code>	Shows the LACP neighbors information.
<code>show lacp sysid</code>	Shows the system identifier used by LACP.

lacp actor port-priority

`lacp actor port-priority priority`

`no lacp actor port-priority priority`

Description

Change the port priority regarding LACP operation.

Inserting **no** as a prefix for this command change the port priority to its default value.

Syntax

Parameter	Description
<i>priority</i>	Port priority value. (Range: 0-65535)

Default

All ports have 32768 as default value for priority.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Currently, configure more than eight ports in a port-channel is not allowed, so this configuration has no practical use.

Example

This example shows how to change the LACP port priority to 20000 for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#lacp
DmSwitch(config-if-eth-1/5)#lacp actor port-priority 20000
DmSwitch(config-if-eth-1/5)#
```

You can verify that the priority was updated by entering the **show lacp internal** command.

Related Commands

Command	Description
debug	Enables the printing of debug messages.
show lacp group	Shows the LACP information by port-channel.
show lacp internal	Shows the LACP internal information.

link-flap

```
link-flap [ detection { flaps time-window } | unblock-time { time } |  
unblock-time-incremental ]
```

```
no link-flap [ detection | unblock-time | unblock-time-incremental ]
```

Description

Configures Link-Flap Detection.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
link-flap	Enables link-flap detection
detection	Configures the detection conditions
<i>flaps</i>	Selects the maximum number of link status flaps (Range 2-100)
<i>time-window</i>	Selects the interval time to count link status flaps (seconds)
unblock-time <i>time</i>	Selects the time interval to wait before unblock the interface (Range 0-86400 seconds)
unblock-time-incremental	Enable incremental mode for unblock timer. Each time a flap occurs during unblock countdown, unblock timer is set with progressively greater value. This value is defined by multiplying the unblock-time by an integer factor that increases each time a flap occurs during unblock countdown.

Default

The default values to detection are 10 flaps in 20 seconds to Fast Ethernet interfaces and 10 flaps in 40 seconds to Giga Ethernet interfaces. The default unblock time is 30 seconds to all Ethernet interfaces with incremental mode disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.
12.0	The option unblock-time-incremental was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure link-flap for interface Ethernet 5

```
DmSwitch(config-if-eth-1/5)#link-flap detection 3 15
DmSwitch(config-if-eth-1/5)#link-flap unblock-time 300
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was configured by entering the **show link-flap** privileged EXEC command.

Related Commands

Command	Description
show link-flap	Shows link-flap status and configuration
show running-config	Shows the current operating configuration.

lldp admin-status

```
lldp admin-status { disable | rx-only | tx-only | tx-and-rx }
```

Description

Configures the administratively desired status of the local LLDP agent.

Syntax

Parameter	Description
disable	Specifies that the transmit and receive mode are disabled.
rx-only	Specifies that only the receive mode is enabled.
tx-only	Specifies that only the transmit mode is enabled.
tx-and-rx	Specifies that the transmit and receive mode are enabled.

Default

The default is tx-and-rx.

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable only the LLDP receive mode for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#lldp admin-status rx-only
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp notification

`lldp notification`

`no lldp notification`

Description

Enables notification of LLDP events, such as add and removal of neighbors.

Inserting **no** as a prefix for this command, it disables notification of LLDP events.

Syntax

No parameter accepted.

Default

By default notification sending is disable.

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

In order to send traps to an SNMP host you must ensure that LLDP traps are enabled globally and for each interface.

Example

This example shows how to enable notifications for LLDP in interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#lldp notification
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp tlvs-tx-enable	Configures which optional TLVs are to be sent to neighbors.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, $(0.25 * \text{transmit-interval})$, to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is $\text{transmit-interval} * \text{transmit-hold}$.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp tlvs-tx-enable

```
lldp tlvs-tx-enable { all | management-address | org-spec-mac-phy  
| org-spec-power-MDI | port-description | system-capabilities |  
system-description | system-name }
```

```
no lldp tlvs-tx-enable { all | management-address | org-spec-mac-phy  
| org-spec-power-MDI | port-description | system-capabilities |  
system-description | system-name }
```

Description

Configures which optional TLVs are to be sent to neighbors.

Inserting **no** as a prefix for this command, it disable the specified TLV sending.

Syntax

Parameter	Description
all	Enables all TLVs sending.
management-address	Enables the Management Address TLV sending.
org-spec-mac-phy	Enables the Organizationally Specific MAC/PHY Config/Status TLV sending.
org-spec-power-MDI	Enables the Organizationally Specific Power via MDI TLV sending.
port-description	Enables the Port Description TLV sending.
system-capabilities	Enables the System Capabilities TLV sending.
system-description	Enables the System Description TLV sending.
system-name	Enables the System Name TLV sending.

Default

All optional TLVS sending are enabled.

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.
13.0	Options org-spec-mac-phy and org-spec-power-MDI were introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable the System Name TLV sending for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#no lldp tlvs-tx-enable system-name
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp admin-status	Configures the administratively desired status of the local LLDP agent.
lldp notification	Enables notification of LLDP events.
lldp notification-interval	Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.
lldp reinitialize-delay	Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.
lldp transmit-delay	Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, (0.25 * transmit-interval), to calculate the number of seconds.
lldp transmit-hold	Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is transmit-interval * transmit-hold.
lldp transmit-interval	Configures the periodic transmit interval for LLDP protocol data units (PDUs).
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp med enable

`lldp med enable`

`no lldp med enable`

Description

Enables LLDP Media Endpoint Devices extension.

Inserting **no** as a prefix for this command, it disables the transmission of LLDP-MED TLVs.

Syntax

No parameter accepted.

Default

The default is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable LLDP-MED for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#lldp med enable
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.

Command	Description
lldp med notification	Enables notification of MED events.
lldp med tlvs-tx-enable	Configures which optional TLVs LLDP-MED will be sent to neighbors.
lldp med fast-start-repeat-count	Configures the number of successive LLDP frame transmissions to device, such as a VoIP phone, is first detected.
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp med fast-start-repeat-count

```
lldp med fast-start-repeat-count { number }
```

```
no lldp med fast-start-repeat-count
```

Description

Configures the number of successive LLDP frame transmissions to device, such as a VoIP phone, is first detected.

Inserting **no** as a prefix for this command, it returns to default value.

Syntax

Parameter	Description
<i>number</i>	Specifies the number of repetitions.

Default

The default value is 4.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure fast-start-repeat-count parameter for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#lldp med fast-start-repeat-count 7
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
<code>lldp</code>	Enables the LLDP operation in the DmSwitch.
<code>lldp med enable</code>	Enables LLDP Media Endpoint Devices extension.
<code>lldp med notification</code>	Enables notification of MED events.
<code>lldp med tlvs-tx-enable</code>	Configures which optional TLVs LLDP-MED will be sent to neighbors.
<code>show lldp</code>	Shows LLDP configuration information.
<code>show lldp neighbor</code>	Shows LLDP neighbor information.
<code>clear lldp</code>	Clears LLDP data.

lldp med notification

`lldp med notification`

`no lldp med notification`

Description

Enables notification of MED (Media Endpoint Discovery) events, such as add and removal of MED capable devices.

Inserting **no** as a prefix for this command, it disables notifications MED events.

Syntax

No parameter accepted.

Default

By default notification sending is disable.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

In order to send traps to an SNMP host you must ensure that LLDP traps are enabled globally and for each interface.

Example

This example shows how to enable notifications for LLDP-MED in interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#lldp med notification
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp med enable	Enables LLDP Media Endpoint Devices extension.
lldp med tlvs-tx-enable	Configures which optional TLVs LLDP-MED will be sent to neighbors.
lldp med fast-start-repeat-count	Configures the number of successive LLDP frame transmissions to device, such as a VoIP phone, is first detected.
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

lldp med tlvs-tx-enable

```
lldp med tlvs-tx-enable { all | capabilities | network-policy | location-id |  
extended-power-mdi | inventory-management }
```

```
no lldp med tlvs-tx-enable { all | capabilities | network-policy |  
location-id | extended-power-mdi | inventory-management }
```

Description

Configures which optional TLVs LLDP-MED will be sent to neighbors.

Inserting **no** as a prefix for this command, it disable the specified TLV sending.

Syntax

Parameter	Description
all	Enables all TLVs sending.
capabilities	Enables the Capabilities TLV sending.
network-policy	Enables the Network Policy TLV sending.
location-id	Enables the Location ID TLV sending.
extended-power-mdi	Enables the Extended Power via MDI TLV sending.
inventory-management	Enables the Inventory TLV sending.

Default

All optional TLVS sending are enabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable the Network Policy TLV sending for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#no lldp med tlvs-tx-enable network-policy
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show lldp** privileged EXEC command.

Related Commands

Command	Description
lldp	Enables the LLDP operation in the DmSwitch.
lldp med enable	Enables LLDP Media Endpoint Devices extension.
lldp med notification	Enables notification of MED events.
lldp med fast-start-repeat-count	Configures the number of successive LLDP frame transmissions to device, such as a VoIP phone, is first detected.
show lldp	Shows LLDP configuration information.
show lldp neighbor	Shows LLDP neighbor information.
clear lldp	Clears LLDP data.

loopback-detection

```
loopback-detection [ unblock-time unblock-time ]
```

```
no loopback-detection [ unblock-time ]
```

Description

Configures Loopback Detection.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
unblock-time <i>unblock-time</i>	Selects the time interval to wait before unblock the interface (seconds)

Default

The default values to unblock time is 30 seconds.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure loopback-detection for interface Ethernet 5

```
DmSwitch(config-if-eth-1/5)#loopback-detection unblock-time 300
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was configured by entering the **show loopback-detection** privileged EXEC command.

Related Commands

Command	Description
<code>show loopback-detection</code>	Shows loopback-detection status and configuration
<code>show running-config</code>	Shows the current operating configuration.

loopback-internal

```
loopback-internal { phy }
```

```
no loopback-internal
```

Description

Configures Loopback Internal

Inserting **no** as a prefix for this command will disable loopback-internal

Syntax

Parameter	Description
phy	Enables phy loopback-internal

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure phy loopback-internal for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#loopback-internal phy
```

You can verify that the information was configured by entering the **show running-config interface ethernet 5** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

mac-address-table move-monitoring

mac-address-table move-monitoring

no mac-address-table move-monitoring

Description

Sets the MAC move addresses monitoring enable per interface.

Inserting **no** as a prefix for this command will disable feature.

Syntax

No parameter accepted.

Default

Enable

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If enable mac-adress-table move-monitoring global, log and sends out a notification trap announcing that a connected host has moved from one interface to another. Disable interface move-monitoring to suppress logs and traps

Example

This example shows how to enable move-monitoring global and disable move-monitoring in interface.

```
DM4000 (config) #mac-address-table move-monitoring
DM4000 (config-if-eth-1/1) #no mac-address-table move-monitoring
```

You can verify the duplication-monitoring was enable by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mac-address-table move-monitoring</code>	Configure global MAC address move monitoring.
<code>show logging ram</code>	Shows logging configuration.
<code>show running-config</code>	Shows the current operating configuration.

mac-learn

mac-learn

no mac-learn

Description

Enable MAC address learning per interface.

Inserting **no** as a prefix for this command will disable MAC learning.

Syntax

No parameter accepted.

Default

MAC learning is enabled for all interfaces.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command can enable or disable learning of MAC addresses per interface. Disable learning will clear MAC address table of the interface.

Example

This example shows how to enable the MAC address learning for an specific interface.

```
DmSwitch(config)#interface ethernet 10
DmSwitch(config-if-eth-1/10)#mac-learn
DmSwitch(config)#
```

You can verify that the information was inserted by entering the **show interfaces status ethernet** user EXEC command.

Related Commands

Command	Description
<code>show interfaces status</code>	Shows interface configuration status.
<code>show running-config</code>	Shows the current operating configuration.

mdix

```
mdix { auto | force-auto | normal | xover }
```

```
no mdix
```

Description

Use the `mdix` command to configure the Medium Dependent Interface Crossover mode.

Inserting **no** as a prefix for this command will disable MDIX.

Syntax

Parameter	Description
auto	Enables auto-MDIX when autonegotiation is enabled
force-auto	Enables auto-MDIX
normal	Disables auto-MDIX and force mode to normal
xover	Disables auto-MDIX and force mode to crossed-over

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable auto-MDIX and force mode to cross-over on interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#mdix xover
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was deleted by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
show interfaces status	Shows interface configuration status.

monitor source

```
monitor source { rx | tx | all }
```

```
no monitor source
```

Description

Sets the interface as a source of monitored traffic.

Inserting **no** as a prefix for this command will disable the interface as a monitor source.

Syntax

Parameter	Description
rx	Monitor only received traffic
tx	Monitor only transmitted traffic
all	Monitor all traffic

Default

By default, the interface is not a source of monitored traffic.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the interface Ethernet 5 as a monitoring source for the capture of its received traffic.

```
DmSwitch(config-if-eth-1/5)#monitor source rx
DmSwitch(config-if-eth-1/5)#
```


You can verify that the configuration was made by entering the **show monitor** privileged EXEC command.

Related Commands

Command	Description
monitor (Global configuration)	Configures the traffic monitoring.
show monitor	Shows traffic monitoring configuration.
show running-config	Shows the current operating configuration.

negotiation

negotiation

no negotiation

Description

Use the negotiation command to enable or disable autonegotiation.

Inserting **no** as a prefix for this command will disable autonegotiation.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable autonegotiation for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#no negotiation
DmSwitch(config-if-eth-1/5)#
```

You can verify that the autonegotiation was disabled by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
flowcontrol	Configures Flow Control for Ethernet interfaces.
negotiation	Controls autonegotiation status for an Ethernet interface.
speed-duplex	Configures speed and duplex operation.
show interfaces status	Shows interface configuration status.
show interfaces table configuration	Shows interface's configuration table.

network-policy

network-policy profile *profile-number*

no network policy { **all** | **profile** *profile-number* }

Description

Add Network Policy for Ethernet interface.

Syntax

Parameter	Description
profile <i>profile-number</i>	Add a specific profile for interface. Inserting no as a prefix, removes a specific profile.
all	Remove all profiles of interface.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add network policy profile 1 for the interface 1/10.

```
DmSwitch(config-if-eth-1/10)#network-policy profile 1
DmSwitch(config-if-eth-1/10)#
```

You can verify that the information was configured by entering the **show this** in the new prompt.

Related Commands

Command	Description
<code>voice vlan</code>	Configure Voice VLAN feature.
<code>voice-signaling vlan</code>	Configure Voice-Signaling VLAN feature.
<code>show network-policy</code>	Shows Network Policy settings.
<code>show running-config</code>	Shows the current operating configuration.

oam

```
oam { dying-gasp milliseconds | pdu-interval milliseconds | pdu-loss-limit limit-number |  
pdu-unblock-time seconds }
```

```
no oam{ dying-gasp | pdu-interval | pdu-loss-limit | pdu-unblock-time }
```

Description

Configures OAM status.

Inserting **no** as a prefix for this command will disable OAM.

Syntax

Parameter	Description
dying-gasp	Enable the dispatch of dying-gasp flag in case of shutdown of the equipment port.
pdu-interval <i>milliseconds</i>	Configure OAMPDU interval OAMPDU interval in milliseconds (Range: 100 - 1000)
pdu-loss-limit <i>limit-number</i>	Configure OAMPDU loss limit Number of OAMPDUs that can be lost (Range: 3 - 30)
pdu-unblock-time <i>seconds</i>	Configure OAMPDU unblock-time OAMPDU unblock time in seconds (Range: 0 - 86400)

Default

The OAM is disabled by default. The pdu-interval is 1000 ms by default. The pdu-loss-limit is 5 by default. The pdu-unblock-time is 0 by default.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure OAM for interface Ethernet 5

```
DmSwitch(config-if-eth-1/5) #oam
DmSwitch(config-if-eth-1/5) #
```

You can verify that the information was configured by entering the **show oam** privileged EXEC command.

Related Commands

Command	Description
show oam	Shows OAM information status and configuration
show running-config	Shows the current operating configuration.

openflow enable

openflow enable

no openflow enable

Description

Enables the use of ethernet interface by OpenFlow protocol.

The **no** command denies the usage of ethernet interface by OpenFlow protocol.

Syntax

No additional parameter is needed.

Default

Ethernet interface is not configured for OpenFlow usage by default.

Command Modes

Interface configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

Enabling OpenFlow in a ethernet interface let OpenFlow protocol use this interface.

Example

This example shows how to enable OpenFlow in a ethernet interface.

```
DmSwitch(config)#interface ethernet 1/1
DmSwitch(config-if-eth-1/1)#openflow enable
DmSwitch(config-if-eth-1/1)#show this
interface ethernet 1/1
  no loopback-detection
  openflow enable
  no mac-learn
  switchport native vlan 4000
  switchport block broadcast ethernet range 1/1 1/26
  switchport block multicast ethernet range 1/1 1/26
  switchport block unicast ethernet range 1/1 1/26
!
```



```
DmSwitch(config-if-eth-1/1) #
```

When enabling OpenFlow in a ethernet interface, some configurations are automatically included, as shown above.

Related Commands

Command	Description
<code>openflow</code>	Enables global OpenFlow protocol.
<code>openflow enable</code>	Enables VLAN usage by OpenFlow protocol.
<code>show openflow</code>	Shows global OpenFlow configuration.

poe

poe

poe mode dynamic priority { **high** | **low** } **power** { **limit** | **restrict** } *power-value*

poe mode static power { **limit** | **restrict** } *power-value*

no poe

Description

Configure port to supply electrical power to a powered device (PD).

Inserting **no** as a prefix for this command will disable the PoE capacity of the port. Using **poe** will enable the port capacity again.

Syntax

Parameter	Description
mode dynamic	Set dynamic power distribution.
mode static	Set static power distribution.
priority high	Set the port priority to high.
priority low	Set the port priority to low.
power limit <i>power-value</i>	Sets the maximum amount of power supplied to this port. If the power consumption by the powered device exceeds this value, power is turned off over that port.
power restrict <i>power-value</i>	Sets the maximum power rating permitted on this port. If the maximum power value of the class of the powered device connected to this port exceeds this value, power is denied to this port. Also, if the power consumption by the powered device exceeds this value, power is shut down over this port.

Power Parameters	Description
4000	Port supplies up to 4W.
7000	Port supplies up to 7W.
15400	Port supplies up to 15.4W.
34200	Port supplies up to 34.2W.

Default

At start, all ports are configured with PoE enabled, dynamic mode, low priority and power restrict up to 15.4W.

Command Modes

Privileged EXEC.

Interface configuration.

Command History

Release	Modification
10.6	This command was introduced.

Usage Guidelines

The power supply in a PoE port is independent of the data link. It is provided and limited by the unit according to the configured power.

Static and dynamic modes differ at the moment when the available power for a port is subtracted from the system's total available to PoE.

In static mode, the power to the port is reserved and subtracted from the total at configuration time. When using dynamic mode, the reserved power is defined at the connection time of the new device to the port.

IEEE defines that a PD can be associated with a class according to its maximum consumption. There are 5 classes, from 0 to 4. At the moment that a PD is plugged into a Power Sourcing Equipment (PSE) it announces its class (class 0 is assumed when there isn't announce).

Therefore, when using the limit parameter, if the PD announces a consumption greater than configured but actually is consuming less, the port will remain providing the configured power at most. If the consumption becomes greater than configured, the port enters in overcurrent state and the power will be turned off.

In power restricted mode, if the PD announced consumption is greater than the configured power, the power supply will not be turned on. If the consumption becomes greater than configured the port enters in overcurrent state and the power will be turned off.

The dynamic mode has a priority parameter to indicate which port should be on or off when the total power is not enough to all ports. This parameter can be set as high or low, but both of them have lower priority against the static mode ports.

The precedence of ports with the same priority is defined by the port number. Port 1 is powered before port 2 and so on.

Each unit manages its own power distribution, not interfering in any configuration of the others.

Example

This example shows how to set static PoE for interface Ethernet 1, limited by 7W.

```
DmSwitch(config-if-eth-1/1)#poe mode static power limit 7000
DmSwitch(config-if-eth-1/1)#
```

This example shows how to set dynamic PoE for interface Ethernet 1, with power restricted to 4W and low priority.

```
DmSwitch(config-if-eth-1/1)#poe mode dynamic priority low power restrict 4000
DmSwitch(config-if-eth-1/1)#
```

You can verify that the information was set by entering the **show poe** privileged EXEC command.

Related Commands

Command	Description
show poe	Shows the PoE current configuration.
rpu power-sharing	Enables RPU to increase PoE power.

queue max-bw

```
queue max-bw { unlim-all | { { unlimited | bandwidth1 } { unlimited | bandwidth2 }  
{ unlimited | bandwidth3 } { unlimited | bandwidth4 } { unlimited | bandwidth5 } {  
unlimited | bandwidth6 } { unlimited | bandwidth7 } { unlimited | bandwidth8 } } }
```

no queue max-bw

Description

Configure the maximum bandwidth allocation per queue.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
unlim-all	Selects unlimited bandwidth for all queues.
unlimited	Selects unlimited bandwidth for a queue.
<i>bandwidth1 ... bandwidth8</i>	Maximum bandwidth for each queue (1 ... 8) in kbit/s (8 kbit/s granularity)
all	Adds all ports

Default

The default is unlimited bandwidth for all queues of all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced. Before this was called qos max-bw .
5.0	This command was moved from Configure menu to Interface Ethernet menu. The description of the old command can be consulted in the DmSwitch Command Reference in case of using an older than 5.0 version by clicking here .
13.2	The granularity of bandwidth was changed from 64kbits/s to 8 kbits/s.

Usage Guidelines

Not available.

Example

This example shows how to configure maximum queue bandwidths to Ethernet interface 5.

```
DmSwitch(config)#queue max-bw 10048 unlimited 30016 unlimited 50048 60032 70016 8000 ethernet 5
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue max-bw** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue sched-mode wdr	Configures Ethernet interface queues in Weighted Deficit Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
show running-config	Shows the current operating configuration.

queue sched-mode sp

queue sched-mode sp

no queue sched-mode

Description

Configure Ethernet interface queues in the Strict Priority schedule mode.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

No parameter accepted.

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Queue	Weight
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced. Before this was called qos sched-mode sp .
5.0	This command was moved from Configure menu to Interface Ethernet menu. The description of the old command can be consulted in the DmSwitch Command Reference in case of using an older than 5.0 version by clicking here .

Usage Guidelines

Not available.

Example

This example shows how to configure sp schedule mode to Ethernet interfaces 9 to 16.

```
DmSwitch(config)#queue sched-mode sp unit 1 ethernet 9to16
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue sched-mode wdr	Configures Ethernet interface queues in Weighted Deficit Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

queue sched-mode wfq

```
queue sched-mode wfq { min-bw { bandwidth1 | sp } { bandwidth2 | sp } { bandwidth3 | sp }  
{ bandwidth4 | sp } { bandwidth5 | sp } { bandwidth6 | sp } { bandwidth7 | sp } { bandwidth8 | sp } }
```

```
no queue sched-mode
```

Description

Configure Ethernet interface queues in the Weighted Fair Queueing schedule mode.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
min-bw	Minimum bandwidth allocation per queue (for ports using WFQ mode only)
<i>bandwidth1 ... bandwidth8</i>	Minimum bandwidth for each queue (values from "0" to "Maximum Port Rate") in kbit/s (8 kbit/s granularity)
sp	Configures queue in strict priority

Default

The default queue schedule mode is wrt for all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced. Before this was called qos sched-mode wfq .
5.0	This command was moved from Configure menu to Interface Ethernet menu. The description of the old command can be consulted in the DmSwitch Command Reference in case of using an older than 5.0 version by clicking here .
13.2	The granularity of bandwidth was changed from 64kbits/s to 8 kbits/s.

Usage Guidelines

Strict Priority Queues will be served first. The remaining bandwidth, not used by sp queues, will be shared among the other queues. This queues receive bandwidth to fullfil the min-bw configuration, if possible. In the absence of sp queues, the min-bw will be used for each queue, and the excess traffic will also pass, if possible.

Example

This example shows how to configure wfq schedule mode to Ethernet interfaces 25 with different minimum bandwidth.

```
DmSwitch(config)#queue sched-mode wfq unit 1 ethernet 25 min-bw 1024 2048 sp sp sp sp 7040 sp
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue sched-mode wdrr	Configures Ethernet interface queues in Weighted Deficit Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

queue sched-mode wrr

```
queue sched-mode wrr [ queue-weights { weight1 | sp } { weight2 | sp } { weight3 | sp } {  
weight4 | sp } { weight5 | sp } { weight6 | sp } { weight7 | sp } { weight8 | sp } ]
```

```
no queue sched-mode
```

Description

Configure Ethernet interface queues in the Weighted Round Robin schedule mode.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
<i>queue-weights</i>	Enables the weight specification for each queue.
<i>weight1 ... weight8</i>	Weight for each queue (values between 1 and 15).
sp	Configures queue in strict priority.

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Queue	Weight
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Command Modes

Global configuration.

Command History

Release	Modification
---------	--------------

Release	Modification
4.0	This command was introduced. Before this was called qos sched-mode wrr .
5.0	This command was moved from Configure menu to Interface Ethernet menu. The description of the old command can be consulted in the DmSwitch Command Reference in case of using an older than 5.0 version by clicking here .

Usage Guidelines

Not available.

Example

This example shows how to configure wrr schedule mode to Ethernet interface 2 with different weights.

```
DmSwitch(config)#interface ethernet 1/2
DmSwitch(config-if-eth-1/2)#queue sched-mode wrr queue-weights 2 3 5 sp sp sp 8 15
DmSwitch(config-if-eth-1/2)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wdr	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

queue sched-mode wrr

```
queue sched-mode wrr [ queue-weights { weight1 } { weight2 } { weight3 } { weight4 } {  
weight5 } { weight6 } { weight7 } { weight8 } ]
```

```
no queue sched-mode
```

Description

Configure Ethernet interface queues in the Weighted Deficit Round Robin schedule mode.

Inserting **no** as a prefix for this command will return to the default values.

Syntax

Parameter	Description
<i>queue-weights</i>	Enables the weight specification for each queue.
<i>weight1 ... weight8</i>	Weight for each queue (values between 1 and 99).
sp	Configures queue in strict priority.

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
13.6.2	This command has been introduced in this release.

Usage Guidelines

A queue with weight 20 will be served twice as much as another with weight 10. A queue with weight sp will follow, for this queue, strict priority mode. This last queue will be served first, always. There is no 0 weight configuration, and 100 is the equivalent to sp mode.

Example

This example shows how to configure wrr schedule mode to Ethernet interface 1/2 with different weights.

```
DmSwitch(config)#interface ethernet 1/2
DmSwitch(config-if-eth-1/2)#queue sched-mode wdr queue-weights 10 20 20 sp 1 1 1 50
DmSwitch(config-if-eth-1/2)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

rate-limit

```
rate-limit { input | output } { rate rate-limit } { burst burst-size }
```

```
rate-limit input flowcontrol pause pause-limit resume resume-limit }
```

```
no rate-limit { input [ flowcontrol ] | output }
```

Description

Configures a maximum data rate for interfaces.

Inserting **no** as a prefix for this command will disable the data rate limit.

Syntax

Parameter	Description
input	Specifies the ingress rate-limit for a port.
output	Specifies the egress rate-limit for a port.
rate	Specifies the rate-limit.
<i>rate-limit</i>	Rate-limit in kilobits per second. (Range: 64-10000000. Must be multiple of 64.)
burst	Specifies the maximum burst size.
<i>burst-size</i>	Maximum burst size in kilobyte. (Range: 4-2048. Must be power of 2.)
flowcontrol	Specifies pause/resume frames sending.
pause	Specifies pause-frames sending threshold.
<i>pause-limit</i>	Pause-frames sending threshold in kilobits. Possible values: 4, 6, 8, 16, 24, 32, 40 or 48
resume	Specifies resume-frames sending threshold.
<i>resume-limit</i>	Resume-frames sending threshold in kilobits. (Range: 4-512. Must be power of 2.)

Default

By default, rate limit is disabled on interfaces.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Rate-limit flowcontrol can only be applied to input rate-limited interfaces. Rate-limit flowcontrol is functional only when flowcontrol (forced or negotiated) is enabled.

Example

This example shows how to configure rate-limits for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#rate-limit input rate 64000 burst 1024
DmSwitch(config-if-eth-1/5)#rate-limit output rate 64000 burst 1024
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was enabled by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

rmon collection history

```
rmon collection history { auto-index | index } [ buckets bucket-number ] [ interval seconds ] [ owner name ]
```

```
no rmon collection history index
```

Description

Configures a RMON history group of statistics.

Inserting **no** as a prefix for this command will remove the specified RMON history group of statistics.

Syntax

Parameter	Description
auto-index	Automatically identifies the RMON history group of statistics. (Range: 1-65535)
<i>index</i>	Identifies the RMON history group of statistics. (Range: 1-65535)
buckets <i>bucket-number</i>	Specifies the maximum number of buckets. (Range: 1-65535)
interval <i>seconds</i>	Specifies the number of seconds in each polling cycle
owner <i>ownername</i>	Specifies the owner of the RMON group of statistics

Default

Buckets : 8

Interval: 1800

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a RMON history group of statistics index 5 on interface Ethernet 5. In this configuration, the data is sampled every 30 seconds and are saved the maximum number of 8 samples.

```
DmSwitch(config-if-eth-1/5)#rmon collection history 5 buckets 8 interval 30 owner test
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show rmon history** privileged EXEC command.

Related Commands

Command	Description
rmon	Configures an RMON.
rmon alarm	Configures an RMON alarm.
rmon collection stats	Configures a RMON collection of statistics.
rmon event	Configures an RMON event.
show rmon alarm	Shows the RMON alarm table.
show rmon event	Shows the RMON event table.
show rmon history	Shows the RMON history table.
show running-config	Shows the current operating configuration.
show rmon statistics	Shows the RMON statistics table.

rmon collection stats

```
rmon collection stats { auto-index | index } [ owner name ]
```

```
no rmon collection stats index
```

Description

Configures a RMON collection of statistics.

Inserting **no** as a prefix for this command will remove the specified RMON statistics collection.

Syntax

Parameter	Description
auto-index	Automatically identifies the RMON history group of statistics. (Range: 1-65535)
<i>index</i>	Identifies the RMON group of statistics. (Range: 1-65535)
owner <i>ownername</i>	Specifies the owner of the RMON group of statistics.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a RMON collection of statistics index 5 on interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#rmon collection stats 5 owner test
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show rmon statistics** privileged EXEC command.

Related Commands

Command	Description
rmon	Configures an RMON.
rmon alarm	Configures an RMON alarm.
rmon collection history	Configures a RMON history group of statistics.
rmon event	Configures an RMON event.
show rmon alarm	Shows the RMON alarm table.
show rmon event	Shows the RMON event table.
show rmon history	Shows the RMON history table.
show running-config	Shows the current operating configuration.
show rmon statistics	Shows the RMON statistics table.

sflow counter-interval

sflow counter-interval {0-65535}

Description

Sets the counter sample interval on an Ethernet or Port-channel Interface.

Inserting **no** as a prefix for this command will set the default counter interval.

Syntax

Parameter	Description
<i>value</i>	Counter interval. (Range: 0-65535)

Default

Counter interval 0.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.
14.10	This command was extended to Port-channel interface.

Usage Guidelines

The maximum number of seconds between successive samples of the counters associated with this data source. A counter interval of 0 disables counter sampling.

Example

This example shows how to configure the SFLOW counter interval on an Ethernet Interface.

```
DmSwitch(config-if-eth-1/5)#sflow counter-interval 300
```

This example shows how to configure the SFLOW counter interval on an Port-channel Interface.

```
DmSwitch(config-if-port-ch-1)#sflow counter-interval 300
```

To verify the SFLOW configuration enter the **show sflow interfaces** command.

Related Commands

Command	Description
sflow	Enables SFLOW on an Ethernet or Port-channel Interface.
sflow max-header-size	Sets the number of bytes copied from packet.
sflow receiver	Sets a receiver to send the SFLOW packages.
sflow sample-rate	Sets as sample rate on an Ethernet or Port-channel Interface.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

sflow max-header-size

sflow max-header-size {0-128}

Description

Sets the maximum number of bytes copied from sampled packet to SFLOW packet.

Inserting **no** as a prefix for this command will set to default max header size.

Syntax

Parameter	Description
<i>value</i>	Max header size. (Range: 0-128)

Default

Max header size 128.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.
14.10	This command was extended to Port-channel interface.

Usage Guidelines

The maximum number of bytes that should be copied from a sampled packet.

Example

This example shows how to configure the SFLOW max header size on an Ethernet Interface.

```
DmSwitch(config-if-eth-1/5)#sflow max-header-size 100
```

This example shows how to configure the SFLOW max header size on an Port-channel Interface.

```
DmSwitch(config-if-port-ch-1)#sflow max-header-size 100
```

To verify the SFLOW configuration enter the **show sflow interfaces** command.

Related Commands

Command	Description
sflow	Enables SFLOW on an Ethernet or Port-channel Interface.
sflow counter-interval	Sets the counter sample interval on an Ethernet or Port-channel Interface.
sflow receiver	Sets a receiver to send the SFLOW packages.
sflow sample-rate	Sets as sample rate on an Ethernet or Port-channel Interface.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

sflow receiver

sflow receiver {1-3}

Description

Sets a receiver to send SFLOW packets.

Inserting **no** as a prefix for this command will set to default receiver.

Syntax

Parameter	Description
<i>value</i>	Receiver index. (Range: 1-3)

Default

Receiver 1.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.
14.10	This command was extended to Port-channel interface.

Usage Guidelines

The SFLOW receiver for this flow sampler.

Example

This example shows how to set a receiver for an Ethernet Interface.

```
DmSwitch(config-if-eth-1/5)#sflow receiver 3
```

This example shows how to set a receiver for an Port-channel Interface.

```
DmSwitch(config-if-port-ch-1)#sflow receiver 3
```

To verify the SFLOW configuration enter the **show sflow interfaces** command.

Related Commands

Command	Description
sflow	Enables SFLOW on an Ethernet or Port-channel Interface.
sflow counter-interval	Sets the counter sample interval on an Ethernet or Port-channel Interface.
sflow max-header-size	Sets the number of bytes copied from packet.
sflow sample-rate	Sets as sample rate on an Ethernet or Port-channel Interface.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

sflow sample-rate

```
sflow sample-rate {2000-65535}
```

Description

Sets a sample rate (rate is 1/sample_rate packet/s.) on an Ethernet or Port-channel Interface.

Inserting **no** as a prefix for this command will set the default sample rate value.

Syntax

Parameter	Description
<i>value</i>	Sample rate. (Range: 2000-65335)

Default

Sample rate 4096.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.
14.10	This command was extended to Port-channel interface.

Usage Guidelines

The statistical sampling rate for packet sampling from this source. Set to N to sample 1/Nth of the packets in the monitored interface.

Example

This example shows how to configure the SFLOW sample rate on an Ethernet Interface.

```
DmSwitch(config-if-eth-1/5)#sflow sample-rate 8000
```

This example shows how to configure the SFLOW sample rate on an Port-channel Interface.

```
DmSwitch(config-if-port-ch-1)#sflow sample-rate 8000
```

To verify the SFLOW configuration enter the **show sflow interfaces** command.

Related Commands

Command	Description
sflow	Enables SFLOW on an Ethernet or Port-channel Interface.
sflow counter-interval	Sets the counter sample interval on an Ethernet or Port-channel Interface.
sflow max-header-size	Sets the number of bytes copied from packet.
sflow receiver	Sets a receiver to send the SFLOW packages.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

sflow

sflow

Description

Enables SFLOW on an Ethernet or Port-channel interface.

Inserting **no** as a prefix for this command will disable SFLOW on the specified interface.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.
14.10	This command was extended to Port-channel interface.

Usage Guidelines

If not enabled none traffic will be sampled on an Ethernet interface. There is a limit of 24Gb to be distributed on Ethernet interfaces with sflow enabled, for example, 2 * 10Gb interfaces + 4 * 1Gb interfaces, or 1 * 10Gb interface + 14 * 1Gb interfaces. Tries to enable more than 24Gb will result on an error message.

Example

This example shows how to enable SFLOW on an Ethernet Interface.

```
DmSwitch(config-if-eth-1/5)#sflow
```

This example shows how to enable SFLOW on an Port-channel Interface.

```
DmSwitch(config-if-port-ch-1)#sflow
```

To verify the SFLOW configuration enter the **show sflow interfaces** command.

Related Commands

Command	Description
sflow counter-interval	Sets the counter sample interval on an Ethernet or Port-channel Interface.
sflow max-header-size	Sets the number of bytes copied from packet.
sflow receiver	Sets a receiver to send the SFLOW packages.
sflow sample-rate	Sets as sample rate on an Ethernet or Port-channel Interface.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

shutdown

shutdown

no shutdown

Description

Use the shutdown command to disable an interface.

Inserting **no** as a prefix for this command will re-enable the interface.

Syntax

No parameter accepted.

Default

Interface is enabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to shutdown an Ethernet interface.

```
DmSwitch(config)#interface ethernet 10
DmSwitch(config-if-eth-1/10)#shutdown
DmSwitch(config-if-eth-1/10)#
```

You can verify that the Ethernet interface is down by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces status</code>	Shows interface configuration status.
<code>show interfaces table configuration</code>	Shows interface's configuration table.

slow-protocols

```
slow-protocols { destination-address { alternative | standard } }
```

```
no slow-protocols destination-address
```

Description

Configures Slow Protocols destination address.

Inserting **no** as a prefix for this command will return to the default value.

Syntax

Parameter	Description
alternative	Selects a alternative destination address
standard	Selects the IEEE standard destination address

Default

The default values to the Slow Protocols destination address is the standard.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the alternative destination address to slow-protocols in interface Ethernet 5

```
DmSwitch(config-if-eth-1/5)#slow-protocols destination-address alternative
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was configured by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
show interfaces status	Shows interface configuration status.
show running-config	Shows the current operating configuration.

spanning-tree

```
spanning-tree { instance instance-parameters | edge-port | link-type  
link-type-parameters | restricted-role | restricted-tcn }
```

```
no spanning-tree { instance instance-parameters | edge-port | link-type |  
restricted-role | restricted-tcn }
```

Description

Adds an Ethernet interface in a Spanning-Tree.

Inserting **no** as a prefix for this command will remove the Ethernet interface from a Spanning-Tree.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
instance-parameters	Click here to see the <i>instance</i> parameters description.
edge-port	Specifies spanning-tree edge port. Click here to see the edge-port parameter description.
link-type link-type-parameters	Specifies spanning-tree link type. Click here to see the link-type parameter and parameters description.
restricted-role	Disallows Root Role on interface. Click here to see the restricted-role parameter description.
restricted-tcn	Disallows Topology Change Notification on interface. Click here to see the restricted-tcn command description.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

Not available.

Example

This example shows how to add the selected interface Ethernet 5 to spanning-tree instance 1.

```
DmSwitch(config-if-eth-1/5)#spanning-tree 1
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show spanning-tree instance ethernet ethernet-instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpduguard	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree bpdupfilter

spanning-tree bpdupfilter

no spanning-tree bpdupfilter

Description

Enables Bridge Protocol Data Unit (BPDU) filter on the interface.

Inserting **no** as a prefix for this command disable the BPDU filter on the interface.

Syntax

No parameter accepted.

Default

The BPDU filter is disabled on all interfaces by default.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.
13.0	BPDU filter on interface is no longer disabled when a BPDUs is received.

Usage Guidelines

Configuring BPDU filter on a interface prevents it from sending or receiving any BPDUs. It works independently from edge configuration and no frames are sent at link up.

WARNING: Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

When configured on an interface, BPDU filter has higher priority than BPDU guard. Configuring BPDU guard on a BPDU filtered interface has no effect.

Example

To configure BPDU filter for an interface:

```
DmSwitch#configure
DmSwitch(config)#interface ethernet 1
DmSwitch(config-if-eth-1/1)#spanning-tree bpdufilter
```

To verify that BPDU filter was enabled:

```
DmSwitch#show spanning-tree interface ethernet 1
Eth 1/ 1 information
-----
Edge port:          admin: disabled, oper: disabled
Link type:          admin: auto, oper: point-to-point
BPDU Filter:        enabled  <==
BPDU Guard:         disabled
Restricted role:     disabled
Restricted TCN:      disabled

DmSwitch#
```

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree bpdufilter	Enables the Bridge Protocol Data Unit (BPDU) filter.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree bpduguard (Interface configuration)	Enables the Bridge Protocol Data Unit (BPDU) guard on the interface.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree bpduguard

spanning-tree bpduguard

no spanning-tree bpduguard

Description

Enables Bridge Protocol Data Unit (BPDU) guard on the interface.

Inserting **no** as a prefix for this command disable the BPDU guard on the interface.

Syntax

No parameter accepted.

Default

The BPDU guard is disabled on all interfaces by default.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The BPDU guard is used to prevent BPDU attacks from spanning-tree ports.

If an port receives a BPDU when BPDU guard is enabled, that port is administratively disabled. It works as BPDU guard global configuration, except that it's independent from edge configuration.

When configured on an interface, BPDU filter has higher priority than BPDU guard. Configuring BPDU guard on a BPDU filtered interface has no effect.

Example

To configure BPDU guard for an interface:

```
DmSwitch#configure
DmSwitch(config)#interface ethernet 1
DmSwitch(config-if-eth-1/1)#spanning-tree bpduguard
```

To verify that BPDU guard was enabled:

```
DmSwitch#show spanning-tree interface ethernet 1
Eth 1/ 1 information
-----
Edge port:          admin: disabled, oper: disabled
Link type:          admin: auto, oper: point-to-point
BPDU Filter:        disabled
BPDU Guard:         enabled  <==
Restricted role:     disabled
Restricted TCN:      disabled

DmSwitch#
```

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree bpdufilter	Enables the Bridge Protocol Data Unit (BPDU) filter.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree bpdufilter (Interface configuration)	Enables the Bridge Protocol Data Unit (BPDU) filter on the interface.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree edge-port

spanning-tree edge-port

no spanning-tree edge-port

Description

Use the spanning-tree edge-port to define the Ethernet interface as a spanning-tree edge port.

Inserting **no** as a prefix for this command will undefine the Ethernet interface as a spanning-tree edge port.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Edge ports are directly moved to the forwarding state in the spanning-tree. However, after a BPDU is received on these ports, their state will be controlled by the STP execution.

Enable the edge-port parameter on interfaces directly connected to end stations.

Example

This example shows how to define an Ethernet interface as a spanning-tree edge port.

```
DmSwitch(config-if-eth-1/5)#spanning-tree edge-port
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show spanning-tree instance ethernet ethernet-instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpduguard	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree *instance*

spanning-tree *instance* [**cost** *path-cost* | **port-priority** *priority*]

no spanning-tree *instance* [**cost** | **port-priority**]

Description

Configures an Ethernet interface in a Spanning-Tree instance.

Inserting **no** as a prefix for this command will remove the Ethernet interface from a Spanning-Tree instance, or will remove the cost and port-priority configurations of the interface in the Spanning-Tree instance.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
cost	(Optional) Specifies spanning-tree cost.
<i>path-cost</i>	Value of spanning-tree path cost. (Range: 1-200000000)
port-priority	(Optional) Specifies spanning-tree port priority.
<i>priority</i>	Values of spanning tree port priority in steps of 16. (Range: 0-240)

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.

Usage Guidelines

Not available.

Example

This example shows how to set spanning-tree cost and port-priority for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#spanning-tree 1
DmSwitch(config-if-eth-1/5)#

DmSwitch(config-if-eth-1/5)#spanning-tree 1 cost 1000000
DmSwitch(config-if-eth-1/5)#spanning-tree 1 port-priority 128
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show spanning-tree instanceinstance ethernet ethernet-instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree link-type

```
spanning-tree link-type { auto | point-to-point | shared }
```

```
no spanning-tree link-type
```

Description

Use the spanning-tree link-type command to specify the type of link used with spanning-tree.

Inserting **no** as a prefix for this command will return the link-type configuration to its default value.

Syntax

Parameter	Description
auto	Specifies spanning tree link-type as auto. The link type will be derived from the current duplex mode for this interface. If full-duplex is used, the link type will be point-to-point. If half-duplex is used, the link type will be shared.
point-to-point	Specifies spanning tree link-type as point-to-point
shared	Specifies spanning tree link-type as shared

Default

Link type is configured as auto.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to define the spanning-tree link-type in interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#spanning-tree link-type point-to-point
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show spanning-tree instance ethernet ethernet-instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance bpdu-tag	Configure the default STP BPDU tag mode in the DmSwitch.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree instance vlan-group	Adds VLAN groups to a spanning-tree instance.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree restricted-role

spanning-tree restricted-role

no spanning-tree restricted-role

Description

Forbids the interface to become the root port on spanning-tree.

Inserting **no** as a prefix for this command will make it possible for the interface to become the root port.

Syntax

No parameter accepted.

Default

By default, restricted-role is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If restricted-role is enabled for an interface that would be chosen as the root port, the interface will become an alternate port instead.

Use this command to prevent bridges that are not under your control from becoming the root bridge or being in the path to the root bridge. Incorrectly using this command may cause lack of spanning-tree connectivity.

Example

This example shows how to enable restricted-role on interface ethernet 1/5

```
DmSwitch(config-if-eth-1/5)#spanning-tree restricted-role
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show spanning-tree instance ethernet ethernet-instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree edge-port	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree restricted-tcn	Forbids the interface to propagate topology changes to other interfaces.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.

spanning-tree restricted-tcn

spanning-tree restricted-tcn

no spanning-tree restricted-tcn

Description

Forbids the interface to propagate topology changes to other interfaces.

Inserting **no** as a prefix for this command will make it possible for the interface to propagate topology changes.

Syntax

No parameter accepted.

Default

By default, restricted-tcn is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If restricted-tcn is enabled for an interface it will not propagate topology changes due to received messages or port state changes.

Use this command to prevent bridges that are not under your control from causing address flushing in the network core. Incorrectly using this command may cause temporary loss of connectivity after topology changes.

Example

This example shows how to enable restricted-tcn on interface ethernet 1/5

```
DmSwitch(config-if-eth-1/5)#spanning-tree restricted-tcn
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show spanning-tree instance ethernet ethernet-instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree <i>instance</i>	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree edge-port	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree restricted-role	Forbids the interface to become the root port on spanning-tree.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.

speed-duplex

```
speed-duplex { 10full | 10half | 100full | 100half | 1000full }
```

```
no speed-duplex
```

Description

Configures forced speed and duplex modes.

Inserting **no** as a prefix for this command will reset speed and duplex modes to the default values.

Syntax

Parameter	Description
10full	Force 10Mbps full-duplex operation.
10half	Force 10Mbps half-duplex operation.
100full	Force 100Mbps full-duplex operation.
100half	Force 100Mbps half-duplex operation.
1000full	Force 1Gbit/s full-duplex operation.

Default

100half for electrical Fast Ethernet ports.

100full for optical Fast Ethernet ports.

100half for Gigabit Ethernet ports.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The forced mode configuration is only used when autonegotiation is disabled.

Example

This example shows how to configure speed and duplex operation for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#speed-duplex 10full
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
flowcontrol	Configures Flow Control for Ethernet interfaces.
negotiation	Controls autonegotiation status for an Ethernet interface.
speed-duplex	Configures speed and duplex operation.
show interfaces status	Shows interface configuration status.
show interfaces table configuration	Shows interface's configuration table.

switchport acceptable-frame-types

```
switchport acceptable-frame-types { all | tagged | untagged }
```

```
no switchport acceptable-frame-types
```

Description

Use the switchport acceptable-frame-types command to configure the type of frames to be accepted by the interface.

Inserting **no** as a prefix for this command will return the configuration for acceptable-frame-types to its default value.

Syntax

Parameter	Description
all	Accepts tagged and untagged frames.
tagged	Accepts tagged frames only.
untagged	Accepts untagged frames only.[1]

Default

All frame types are accepted.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
3.2	The untagged parameter was added.
7.0	The untagged parameter was available only for DM4000.

Usage Guidelines

Not available.

Example

This example shows how to set interface Ethernet 5 for accepting only tagged frames.

```
DmSwitch(config-if-eth-1/5)#switchport acceptable-frame-types tagged
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.
switchport ingress-filtering	Enables ingress filtering

Notes

[1] - Option available only to DM4000 Switches.

switchport backup-link

```
switchport backup-link interface { ethernet [ unit-number/ ] port-number |  
port-channel channel-group-number } [ action { block | shutdown } ]
```

```
switchport backup-link preempt { delay seconds | mode { forced | off } }
```

```
no switchport backup-link
```

```
no switchport backup-link preempt
```

Description

Configure an alternative link for this interface. In action block, if an interface is down/blocked, the other one is unblocked. In action shutdown, if an interface is down/blocked, the other one is shutdown. Only one interface is unblocked/up at a given time. Preemption is only available in action block. In action block, if preemption is forced and both interfaces are error free, this interface will be unblocked after a configurable delay and the alternative interface will be blocked. In shutdown action, when both interface is down/block, both interfaces will be no shutdown.

Inserting **no** as a prefix for this command, it will disable backup-link.

Syntax

Parameter	Description
action	Configure action for down or block interfaces.
block	Block backup interface.
shutdown	Shutdown backup interface.
preemption mode	Configure preemption mode.
forced	Turn on preemption.
off	Turn off preemption.
preemption delay <i>seconds</i>	Configure <i>seconds</i> as the delay for forced preemption from backup interface to main interface. Forced preemption mode must be configured. (Range: 1-300 seconds)

Default

If action not defined, default action is block.

If set preemption mode force and preemption delay not defined, default delay is 35 seconds.

Command Modes

Interface configuration.

Command History

Release	Modification
9.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure ethernet 3 as the alternative interface for ethernet 2. Ethernet 2 is the main interface. The preemption mode is configured as forced; if both interfaces are error free, ethernet 2 is preferred: it will be unblocked and ethernet 3 will be blocked after 45 seconds.

```
DmSwitch(config-if-eth-1/2)#switchport backup-link interface ethernet 3
DmSwitch(config-if-eth-1/2)#switchport backup-link preemption mode forced
DmSwitch(config-if-eth-1/2)#switchport backup-link preemption delay 45
```

Related Commands

Command	Description
show backup-link	Shows backup-link status information.
show interfaces switchport	Shows switchport information.
show interfaces status	Shows interface configuration status.

switchport block broadcast ethernet

```
switchport block broadcast ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

```
no switchport block broadcast ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

By default, broadcast packets are flooded out of all ports. You can block a port from flooding such packets to other ports.

Inserting **no** as a prefix for this command will unblock broadcast flooding.

Syntax

Parameter	Description
[unit-number/] port-number	Blocks broadcast flooding to a specific unit and port
range [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Blocks broadcast flooding to a range of units and ports

Default

Broadcast flooding block is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command is used to block broadcast flooding. .

Example

This example shows how to block broadcast flooding for a specific port.

```
DmSwitch(config-if-eth-1/5)#switchport block broadcast ethernet 3
```

You can verify that the configuration was made by entering the **show interface switchport ethernet 5** privileged EXEC command.

Related Commands

Command	Description
switchport storm-control	Configures packet storm control.
show interface switchport	Shows switchport information.
show running-config	Shows the current operating configuration.

switchport block multicast ethernet

```
switchport block multicast ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

```
no switchport block multicast ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

By default, packets with unknown destination MAC address are flooded out of all ports. You can block a port from flooding such packets to other ports.

Inserting **no** as a prefix for this command will unblock unknown multicast flooding.

Syntax

Parameter	Description
[unit-number/] port-number	Blocks unknown multicast flood to a specific unit and port.
range [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Blocks unknown multicast flood to a range of units and ports.

Default

Unknown multicast flooding block is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command is used to block unknown multicast flooding. .

Example

This example shows how to block unknown flooding from a specific port to another.

```
DmSwitch(config-if-eth-1/5)#switchport block multicast ethernet 3
```

You can verify that the configuration was made by entering the **show interface switchport ethernet 5** privileged EXEC command.

Related Commands

Command	Description
switchport storm-control	Configures packet storm control.
show interface switchport	Shows switchport information.
show running-config	Shows the current operating configuration.

switchport block unicast ethernet

```
switchport block unicast ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

```
no switchport block unicast ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

By default, packets with unknown destination MAC address are flooded out of all ports. You can block a port from flooding such packets to other ports.

Inserting **no** as a prefix for this command will unblock unknown unicast flooding.

Syntax

Parameter	Description
[unit-number/] port-number	Blocks unknown unicast flood to a specific unit and port
range [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Blocks unknown unicast flood to a range of units and ports

Default

Unknown unicast flooding block is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command is used to block unknown unicast flooding. .

Example

This example shows how to block unknown unicast flooding from a specific port to another.

```
DmSwitch(config-if-eth-1/5)#switchport block unicast ethernet 3
```

You can verify that the configuration was made by entering the **show interface switchport ethernet 5** privileged EXEC command.

Related Commands

Command	Description
switchport storm-control	Configures packet storm control.
show interface switchport	Shows switchport information.
show running-config	Shows the current operating configuration.

switchport bpdu-protect

```
switchport bpdu-protect { block-time seconds | enable | limit BPDU limit per second | mode { block-all | block-bpdu | log } }
```

```
no switchport bpdu-protect { block-time | enable | limit | mode }
```

Description

Use the switchport bpdu-protect to protect configuration for an interface.

Syntax

Parameter	Description
block-time <i>seconds</i>	Specifies the blocking time. (Range: 10-3600)
enable	Enables BPDU protection.
limit <i>BPDU limit per second</i>	Configures the maximum number of BPDU's per second. (Range: 5-1000)
mode	Configures notification and action mode
block-all	Blocks BPDUs and data when limit is reached.
block-bpdu	Blocks BPDUs when limit is reached.
log	Log when limit is reached.

Default

BPDU-protect: Disable

Limit: 30 BPDUs per second

Block-time: 10 seconds

Mode: Block all

Command Modes

Interface configuration.

Command History

Release	Modification
9.6	This command was introduced.

Usage Guidelines

This command can be used to prevent problems in protocols when there is flood of BPDUs in this interface. When occur a flood of BPDUs block interface, unblock after time configured in command bpdu-block-time reached. Block again if flood not stop and limit reached.

Example

This example shows how to enable bpdu-limit for interface Ethernet 5.

```
DmSwitch(config)#interface ethernet 1
DmSwitch(config-if-eth-1/1)#switchport bpdprotect enable
DmSwitch(config-if-eth-1/1)#
```

You can verify that the configuration was made by entering the **show interfaces switchport ethernet 1** privileged EXEC command.

Related Commands

Command	Description
cpu protocols bpdprotect	Control BPDU packets per second.
show running-config	Shows the current operating configuration.
show interfaces switchport	Shows switchport information.
show interfaces status	Shows interface configuration status.

switchport egress-block ethernet

```
switchport egress-block ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

```
no switchport egress-block ethernet { [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

Blocks traffic from a specified interface to a set of interfaces. The traffic source interface is the interface being currently configured. The destination interfaces are specified on the command parameters.

Inserting **no** as a prefix for this command will remove the egress-block configuration.

Syntax

Parameter	Description
[unit-number/] port-number	Blocks traffic to a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Blocks traffic to a range of units and ports.

Default

Egress-block is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set interface Ethernet 5 for blocking egress to Ethernet 6.

```
DmSwitch(config-if-eth-1/5)#switchport egress-block ethernet 6
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
cpu egress-block	Configures the switch to block CPU traffic from a specified Ethernet interface to another for a set of VLAN IDs.

switchport gvrp

switchport gvrp

no switchport gvrp

Description

Enables GVRP for a specific port.

Inserting **no** as a prefix for this command will disable the GVRP.

Syntax

No parameter accepted.

Default

GVRP is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command is used to enable specific ports to automatically learn VLANs from connected devices where GVRP is also enabled. You must also globally enable the GVRP operation.

Example

This example shows how to enable the GVRP for a specific port.

```
DmSwitch(config-if-eth-1/1)#switchport gvrp
DmSwitch(config-if-eth-1/1)#
```

You can verify that the GVRP was enabled by entering the **show gvrp** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
bridge-ext gvrp	Enables GVRP globally for the switch.
garp timer	Set values for GARP timers.
show garp timer	Shows GARP properties.
show gvrp	Shows GVRP configuration.
show running-config	Shows the current operating configuration.

switchport ingress-filtering

`switchport ingress-filtering`

`no switchport ingress-filtering`

Description

Use the switchport ingress-filtering command to enable ingress filtering by VLAN.

Inserting **no** as a prefix for this command will disable ingress-filtering.

Syntax

No parameters accepted.

Default

Ingress filtering is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Use this command to discard received packets from VLANs which do not have this interface as a member.

Example

This example shows how to enable ingress-filtering for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport ingress-filtering
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show interfaces switchport</code>	Shows switchport information.
<code>switchport acceptable-frame-types</code>	Configures the type of frames accepted by the switch.

switchport multicast-flood

```
switchport multicast-flood
```

```
no switchport multicast-flood
```

Description

By default, packets with unknown destination MAC address are flooded out of all ports. You can block a port from flooding such packets to other ports.

Inserting **no** as a prefix for this command will unblock unknown multicast flooding.

Syntax

No parameter accepted.

Default

Unknown multicast flooding block is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command is used to block unknown multicast flooding. .

Example

This example shows how to block unknown multicast flooding for a specific port.

```
DmSwitch(config-if-eth-1/5)#no switchport multicast-flood
```

You can verify that the configuration was made by entering the **show interface switchport ethernet 5** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>switchport storm-control</code>	Configures packet storm control.
<code>show interface switchport</code>	Shows switchport information.
<code>show running-config</code>	Shows the current operating configuration.

switchport mtu

switchport mtu *value*

no switchport mtu

Description

Use the switchport mtu command to configure maximum transmission unit for the specified interface.

Inserting **no** as a prefix for this command will return the maximum transmission unit to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the maximum transmission unit in bytes. (Range: 64-9198)

Default

The default MTU is 9198 bytes.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the maximum transmission unit for interface Ethernet 5 to 1024 bytes.

```
DmSwitch(config-if-eth-1/5)#switchport mtu 1024
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces switchport</code>	Shows switchport information.

switchport native vlan

switchport native vlan *vlan-id*

no switchport native vlan

Description

Use the switchport native vlan command to configure PVID, the default VLAN ID for untagged frames.

Inserting **no** as a prefix for this command will remove the configuration that specifies which is the native VLAN for the interface.

Syntax

Parameter	Description
<i>vlan-id</i>	Specifies the Port VLAN ID. (Range: 1-4094)

Default

PVID is 1, the default VLAN ID.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The specified VLAN should exist, otherwise the command will return an error.

Example

This example shows how to create a VLAN with ID 3 and set interface Ethernet 5 as native from VLAN 3.

```
DmSwitch(config)#interface vlan 3
DmSwitch(config-if-vlan-3)#interface ethernet 5
DmSwitch(config-if-eth-1/5)#switchport native vlan 3
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.
show running-config	Shows the current operating configuration.

switchport port-security maximum ^[3]

```
switchport port-security maximum { num-of-macs }
```

```
no switchport port-security maximum
```

Description

Use the switchport port-security maximum to configure the maximum number of MAC addresses per ethernet or port-channel interface.

Inserting **no** as a prefix for this command will disable port-security.

Syntax

Parameter	Description
<i>num-of-macs</i>	Specifies the maximum number of MAC addresses for this interface.

Default

MAC address limit is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable port-security for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport port-security maximum 10
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
<code>switchport port-security violation</code>	Configures port-security violation.
<code>show interfaces switchport</code>	Shows switchport information.

switchport port-security mac-address ^[3]

```
switchport port-security mac-address sticky [ mac-address ]
```

```
no switchport port-security mac-address sticky [ mac-address | all ]
```

Description

Use the switchport port-security mac-address command to configure the sticky learning on interface.

Enters the command without parameters to enable sticky learning.

Enters the command with a MAC address parameters to add the MAC as sticky.

Inserting **no** as a prefix for this command will disable port-security sticky learning or remove sticky MAC entries.

Syntax

Parameter	Description
<i>mac-address</i>	Installs a sticky MAC address at interface.
all	In no command, removes all sticky MAC address from interface.

Default

MAC address sticky learning is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Port-security must be enabled on interface before configuring sticky learning.

The command **no switchport port-security mac-address sticky** transforms all sticky MAC

entries in dynamic entries.

However, the command **no switchport port-security mac-address sticky** [*mac-address* | **all**] removes MAC addresses from hardware directly.

Example

This example shows how to enable port-security sticky learning for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport port-security mac-address sticky
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show port-security** privileged EXEC command.

Related Commands

Command	Description
switchport port-security violation	Configures port-security violation.
show interfaces switchport	Shows switchport information.

switchport port-security violation ^[3]

switchport port-security violation { *protect* | *restrict* | *shutdown* }

no switchport port-security violation

Description

Use the switchport port-security violation to configure the action when maximum number of MAC addresses per port exceeded (only for ethernet interface).

Inserting **no** as a prefix for this command will set to default port-security violation.

Syntax

Parameter	Description
<i>protect</i>	Drop packets with an unknown source MAC address after limit configured in port-security maximum has exceeded.
<i>restrict</i>	Drop, log and send trap.
<i>shutdown</i>	Drop, log, send trap and shutdown port.

Default

Protect.

Command Modes

Interface configuration.

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure port-security vioalction for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport port-security maximum 10
```

```
DmSwitch(config-if-eth-1/5)#switchport port-security violation shutdown
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
switchport port-security maximum	Configures port-security maximum.
show interfaces switchport	Shows switchport information.

switchport priority default

switchport priority default *value*

no switchport priority default

Description

Use the switchport priority default command to configure 802.1p priorities for the specified interface.

Inserting **no** as a prefix for this command will disable the default priority.

Syntax

Parameter	Description
<i>value</i>	Specifies the priority value for untagged frames. (Range: 0-7)

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the default priority for untagged frames to 3.

```
DmSwitch(config-if-eth-1/5)#switchport priority default 3
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces switchport</code>	Shows switchport information.

switchport protocol

```
switchport protocol { vlan index frame-type { 802.3 | ethernet2 | llc }  
protocol-type { arp | ip | ipv6 | ipx | ether-type-field } }
```

```
no switchport protocol { vlan frame-type { 802.3 | ethernet2 | llc }  
protocol-type { arp | ip | ipv6 | ipx | ether-type-field } }
```

Description

Use the switchport protocol command to configure VID through the specification of the protocol.

Inserting **no** as a prefix for this command will unconfigure the VID.

Syntax

Parameter	Description
vlan	Configures VLAN ID.
<i>index</i>	Specifies protocol VLAN ID. (Range: 1-4094)
frame-type	Data link layer frame-type.
802.3	Ethernet 802.3 or SNAP.
ethernet2	Ethernet II.
llc	Logical Link Control.
protocol-type	Network protocol type.
arp	Address Resolution Protocol.
ip	Internet Protocol.
ipv6	Internet Protocol, version 6.
ipx	Internetwork Packet Exchange.
<i>ether-type-field</i>	Custom value for EtherType field.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure VID for interface Ethernet 5 through the specification of the protocol.

```
DmSwitch(config-if-eth-1/5)#switchport protocol vlan 1 frame-type 802.3 protocol-type  
arp priority 1  
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.

switchport qinq

```
switchport qinq { external | internal }
```

```
no switchport qinq
```

Description

Use the switchport qinq command to configure Double Tagging mode for the specified interface.

Inserting **no** as a prefix for this command will remove the Double Tagging mode configuration for the specified interface.

Syntax

Parameter	Description
external	Configures Double Tagging external mode. A VLAN tag is always inserted on received packets.
internal	Configures Double Tagging internal mode. A VLAN tag is only inserted if the packet does not have a TPID which matches the TPID configured on this interface.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Use this command to configure tagging behavior for interfaces on service provider switches.

The external mode is recommended for client ports so that a provider tag is always inserted.

The internal mode is recommended for uplink ports so that duplicated tags are not inserted on these interfaces.

Example

This example shows how to set Double Tagging external mode for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport qinq external
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.

switchport storm-control

```
switchport storm-control { broadcast | multicast | unicast } [ pps [ pps-maxvalue ]  
| [ percent percent-maxvalue ] ]
```

```
switchport storm-control { ( broadcast | multicast ) action [ limit | notify |  
shutdown after seconds ] | mode [ percent | pps ] }
```

```
no switchport storm-control { ( broadcast | multicast ) [ action | mode ] }
```

Description

Use the switchport storm-control to configure packet storm control for the specified interface.

Inserting **no** as a prefix for this command will remove a broadcast, multicast or unicast storm-control configuration and revert to default.

Storm control can operate in *either* "percent" mode as percentage of total bandwidth or in mode "PPS" for an absolute number of packets per second. The level can be an integer value between 1 and 100, where 100 effectively disables storm-control. For percent the absolute value in bit per second is changed automatically if the link speed changes. If for instance an 1Gbps link is configured to limit broadcast at 50% and the peer changes form 1Gbps to 100Mbps the limit changes automatically form 500Mbps to 50Mbps. The only valid action for **mode percent** is "limit" thus before changing the mode the action for broadcast and mulitcast has to be changed to "limit".

An action is triggered after software recognizes an increase in number of (broadcast or multicast) ingress packets at given interface. Option "limit" is default behavior, limiting at hardware ingress. "Notify" generates a log entry and an SNMP trap. "Shutdown" will shutdown this port, disrupting any traffic passing it. Being "shutdown" an aggressive action, it is triggered only after configured a timer. This timer ranges from 10 to 600 seconds.

Syntax

Parameter	Description
broadcast	Configures broadcast storm-control.
multicast	Configures multicast storm-control.
unicast	Configures unknown unicast storm-control.
pps	(Optional) Sets maximum packets per second.
<i>pps-maxvalue</i>	Specifies the maximum packets per second (Range: 0-262143)
percent	(Optional) Sets limit as percentage of port speed
<i>percent-maxvalue</i>	Maximum percentage (Range: 1-100) where 100 effectively disables storm-control
action	Configures an action to be taken after ingress packet rate at given interface exceeded configured maxvalue. Rate is measured and normalized in a time function.
<i>action limit</i>	Limit at hardware ingress.
<i>action notify</i>	Limit at hardware ingress, notify using log and SNMP trap infrastructure.

Parameter	Description
<i>action shutdown</i>	Limit at hardware ingress, notify using log and SNMP trap infrastructure, shutdown port if port goes under storm for more than configured time. Shutdown must be removed manually by administrator.
mode	Configures the operation mode. The values configured for each mode become effective when the mode is selected.
<i>mode pps</i>	Packets per second mode is activated. The traffic is limited to <i>broadcast-value</i> , <i>multicast-value</i> and <i>unicast-value</i> .
<i>mode percent</i>	Percent mode is activated. The traffic is limited to <i>broadcast-percentage</i> , <i>multicast-percentage</i> and <i>unicast-percentage</i> .

Default

For broadcast, multicast and unicast the default mode is pps with a limit 10000 packets/second and actions notify and limit for 1Gbps ethernet ports, and 100000 packets/second and actions notify and limit for 10Gbps ethernet ports. The default limit is 10% if the mode is changed to percent.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.
11.2	Notify and shutdown port actions for threshold control were made available.
13.4	Percent mode introduced.

Usage Guidelines

Not available.

Example

This example shows how to set broadcast storm-control to 1024 packets per second for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport storm-control broadcast pps 1024
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was done by entering the **show interfaces switchport** privileged EXEC command.

This example shows how to set multicast storm-control to 15 percent for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport storm-control multicast percent 15
```

```
DmSwitch(config-if-eth-1/5)#switchport storm-control multicast action limit
DmSwitch(config-if-eth-1/5)#switchport storm-control broadcast action limit
DmSwitch(config-if-eth-1/5)#switchport storm-control mode percent
```

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.
storm-control	Configures storm control high level actions.

switchport tpid

switchport tpid *ether-type-field*

no switchport tpid

Description

Use the switchport tpid command to configure Tag Protocol ID for an interface. The TPID is the first two bytes in the VLAN tag which also corresponds to the Ethertype field on untagged packets.

Inserting **no** as a prefix for this command will remove a Tag Protocol ID configuration.

Syntax

Parameter	Description
<i>ether-type-field</i>	Tag Protocol ID. (Range: 0x0000-0xFFFF)

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

You can use this command in double tagging (qinq) network setups in order to have distinct tag types for clients and service provider or in order to interoperate with switches that use different values of TPID.

Example

This example shows how to set the tag protocol ID to 0x9100 on interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#switchport tpid 0x9100
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was made by entering the **show interfaces switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Shows switchport information.

vlan-translate

switchport vlan-translate { *egress-table* | *ingress-table* }

Description

Enable VLAN-translate on a given interface.

Syntax

Parameter	Description
<i>egress-table</i>	Enable VLAN-translate egress-table configuration on this interface
<i>ingress-table</i>	Enable VLAN-translate ingress-table configuration on this interface

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable vlan-translate egress-table configuration on a interface.

```
DmSwitch(config)#interface ethernet 3/5
DmSwitch(config-if-eth-3/5)#switchport vlan-translate egress-table
DmSwitch(config-if-eth-3/5)#
```

You can verify that the VLAN translate is enable with command **show running-config**

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
vlan-translate	Adds a new VLAN tag or replaces an associated VLAN tag with another tag. Can be used to change the priority of a VLAN on certain interfaces.

trap-enable

```
trap-enable [ link-flap-detected | link-flap-no-more-detected  
| link-up-down | loopback-detected | loopback-no-more-detected |  
transceiver-presence | unidir-link-detected | unidir-link-recovered ]
```

```
no trap-enable [ link-flap-detected | link-flap-no-more-detected  
| link-up-down | loopback-detected | loopback-no-more-detected |  
transceiver-presence | unidir-link-detected | unidir-link-recovered ]
```

Description

Enable traps by each port.

Inserting **no** as a prefix for this command will disable the specified trap.

Syntax

Parameter	Description
link-flap-detected	Issue link flap detected traps.
link-flap-no-more-detected	Issue link flap no more detected traps.
link-up-down	Issue link-up or link-down traps.
loopback-detected	Issue loopback detected traps.
loopback-no-more-detected	Issue loopback no more detected traps.
transceiver-presence	Issue transceiver-presence traps.
unidir-link-detected	Issue unidirectional link detected traps.
unidir-link-recovered	Issue unidirectional link recovered traps.

Default

All supported traps enabled.

Command Modes

Interface configuration.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Pressing *enter* it will issue all traps.

Example

This example shows how to disable an trap for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#no trap-enable loopback-detected
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was set by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

wred averaging-time

wred averaging-time *time*

no wred averaging-time

Description

Configure the queue size averaging time.

Inserting **no** as a prefix for this command will return to the default value.

Syntax

Parameter	Description
<i>time</i>	Specifies the first queue size averaging time in microseconds

Default

The default value is 4 microseconds.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure wred averaging time for interface Ethernet 5

```
DmSwitch(config-if-eth-1/5)#wred averaging-time 20
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>wred cng-drop-start-point</code>	Configures the start point to drop CNG marked packets for Ethernet interface
<code>wred cng-slope</code>	Configures the slope of drop probability function for CNG marked packets for Ethernet interface
<code>wred drop-start-point</code>	Configures the start point to drop for Ethernet interface
<code>wred slope</code>	Configures the slope of drop probability function for Ethernet interface

wred cng-drop-start-point

```
wred cng-drop-start-point { 1st_queue_start_point ... 8th_queue_start_point }
```

```
no wred cng-drop-start-point
```

Description

Configures the queue size where WRED can start the drop on CNG marked packets

Inserting **no** as a prefix for this command will return to the default value.

Syntax

Parameter	Description
<i>1st_queue_start_point ... 8th_queue_start_point</i>	% of max queue size for each queue (1 ... 8).

Default

The default value for each queue is 100%.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure different start points for each queue for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#wred cng-drop-start-point 10 20 30 40 50 60 70 80
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>wred averaging-time</code>	Configures the queue size averaging time for Ethernet interface
<code>wred cng-slope</code>	Configures the slope of drop probability function for CNG marked packets for Ethernet interface
<code>wred drop-start-point</code>	Configures the start point to drop for Ethernet interface
<code>wred slope</code>	Configures the slope of drop probability function for Ethernet interface

wred cng-slope

```
wred cng-slope { 1st_queue_slope ... 8th_queue_slope }
```

```
no wred cng-slope
```

Description

Configures the slope of drop probability function for CNG marked packets.

Inserting **no** as a prefix for this command will return to the default value.

Syntax

Parameter	Description
<i>1st_queue_slope ... 8th_queue_slope</i>	Specifies the queue slope for each queue (1 ... 8) of drop probability function for CNG marked packets in degrees.

Default

The default value for each queue is 15 degrees.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure different slopes for each queue for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#wred cng-slope 15 25 35 45 55 65 75 85
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was deleted by entering the **COMMAND** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>wred averaging-time</code>	Configures the queue size averaging time for Ethernet interface
<code>wred cng-drop-start-point</code>	Configures the start point to drop CNG marked packets for Ethernet interface
<code>wred drop-start-point</code>	Configures the start point to drop for Ethernet interface
<code>wred slope</code>	Configures the slope of drop probability function for Ethernet interface

wred drop-start-point

```
wred drop-start-point { 1st_queue_start_point ... 8th_queue_start_point }
```

```
no wred drop-start-point
```

Description

Configures the queue size where WRED can start the drop

Inserting **no** as a prefix for this command will return to the default value.

Syntax

Parameter	Description
<i>1st_queue_start_point ... 8th_queue_start_point</i>	% of max queue size for each queue (1 ... 8).

Default

The default value for each queue is 75%.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure different start points for each queue for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#wred drop-start-point 10 20 30 40 50 60 70 80
DmSwitch(config-if-eth-1/5)#
```

You can verify that the configuration was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
wred averaging-time	Configures the queue size averaging time for Ethernet interface
wred cng-drop-start-point	Configures the start point to drop CNG marked packets for Ethernet interface
wred cng-slope	Configures the slope of drop probability function for CNG marked packets for Ethernet interface
wred slope	Configures the slope of drop probability function for Ethernet interface

wred slope

```
wred slope { 1st_queue_slope ... 8th_queue_slope }
```

```
no wred slope
```

Description

Configures the slope of drop probability function.

Inserting **no** as a prefix for this command will return to the default value.

Syntax

Parameter	Description
<i>1st_queue_slope ... 8th_queue_slope</i>	Specifies the queue slope for each queue (1 ... 8) of drop probability function in degrees.

Default

The default value for each queue is 15 degrees.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure different slopes for each queue for interface Ethernet 5.

```
DmSwitch(config-if-eth-1/5)#wred slope 15 25 35 45 55 65 75 85
DmSwitch(config-if-eth-1/5)#
```

You can verify that the information was deleted by entering the **COMMAND** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
wred averaging-time	Configures the queue size averaging time for Ethernet interface
wred cng-drop-start-point	Configures the start point to drop CNG marked packets for Ethernet interface
wred cng-slope	Configures the slope of drop probability function for CNG marked packets for Ethernet interface
wred drop-start-point	Configures the start point to drop for Ethernet interface

Chapter 16. Interface IP Tunnel Commands

description

description *description*

no description

Description

Describes the IP tunnel.

Inserting **no** as a prefix for this command will remove the IP tunnel description.

Syntax

Parameter	Description
<i>description</i>	Describes the IP tunnel.

Default

No default is defined.

Command Modes

IP tunnel configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a IP tunnel description.

```
DmSwitch(config-if-ip-tunnel-1)#description test
```

```
DmSwitch(config-if-ip-tunnel-1)#
```

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ipv6 address

```
ipv6 address { ipv6address/prefix-length | ipv6prefix/prefix-length eui-64 }
```

```
no ipv6 address { [ ipv6address/prefix-length ] | [ ipv6prefix/prefix-length eui-64 ] }
```

Description

Sets an IPv6 address for the selected IP tunnel.

Inserting **no** as a prefix for this command will delete the IPv6 address from the selected IP tunnel.

Using the *ipv6prefix/prefix-length***eui-64** form causes the switch to use interface physical address to compose the IPv6 address in EUI-64 format.

Syntax

Parameter	Description
<i>ipv6address/prefix-length</i>	Specifies the IPv6 address and prefix-length to the selected IP tunnel.
<i>ipv6prefix/prefix-length</i> eui-64	Specifies the IPv6 prefix and prefix-length to be used to compose the IPv6 address in EUI-64 format.

Default

No default is defined.

Command Modes

IP tunnel configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a static IPv6 address for IP tunnel 1.

```
DmSwitch(config-if-ip-tunnel-1)#ipv6 address 2001:DB8::1/64
DmSwitch(config-if-ip-tunnel-1)#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

tunnel destination ip-address

```
tunnel destination ip-address { ip_address }
```

```
no tunnel destination ip-address { ip_address }
```

Description

Sets the IP Tunnel destination IPv4 address.

Inserting **no** as a prefix for this command will delete the destination IPv4 address from the selected IP tunnel.

Syntax

Parameter	Description
<i>ip_address</i>	Destination IPv4 address of IP tunnel.

Default

No default is defined.

Command Modes

IP tunnel configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The destination IP address must be the same address configured in the interface specified as tunnel source interface of the remote tunnel endpoint.

Example

This example shows how to specify a destination IPv4 address for IP tunnel via VLAN interface 1.

```
DmSwitch(config-if-ip-tunnel-1)#tunnel destination ip-address 100.100.150.1
DmSwitch(config-if-ip-tunnel-1)#
```


Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

tunnel source interface

```
tunnel source interface { vlan | loopback } id
```

```
no tunnel source interface { vlan | loopback } id
```

Description

Sets the interface which acts as IPv4 source for IP Tunnel.

Inserting **no** as a prefix for this command will remove tunnel source interface configuration.

Syntax

Parameter	Description
vlan	Source IPv4 address of IP tunnel is the primary address of a VLAN interface.
loopback	Source IPv4 address of IP tunnel is the address of a Loopback interface.
<i>id</i>	Specifies the VLAN or Loopback identifier whose IP address acts as source for the IP tunnel.

Default

No default is defined.

Command Modes

IP tunnel configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

The interface IP address specified as tunnel source must be the same address configured as tunnel destination in remote tunnel endpoint.

Example

This example shows how to specify a static IPv4 address for IP tunnel via VLAN interface.

```
DmSwitch(config-if-ip-tunnel-1)#tunnel source interface vlan 140
DmSwitch(config-if-ip-tunnel-1)#
```

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

tunnel type

tunnel type

Description

Sets the IPv6 over IPv4 tunneling type. This version supports only *ipv6ip* type

Syntax

Parameter	Description
type	Specifies IPv6 over IPv4 tunneling type.
<i>ipv6ip</i>	Specifies manual IPv6 over IPv4 tunneling type.

Default

ipv6ip type.

Command modes

IP tunnel configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the tunneling type (Only *ipv6ip* supported).

```
DmSwitch(config-if-ip-tunnel-1)#tunnel type ipv6ip
DmSwitch(config-if-ip-tunnel-1)#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

Chapter 17. Interface Local Tunnel Commands

[5][7]

ltn-endpoint ^[1] ^[3] ^[5]

```
ltn-endpoint {1|2}
```

```
no ltn-endpoint {1|2}
```

Description

Activates the selected local tunnel endpoint interface.

Inserting **no** as a prefix for this command will deactivate the selected local tunnel endpoint interface. Meaning that the endpoint will be administratively disabled, keeping the link down.

Syntax

Parameter	Description
{1 2}	Specific local tunnel endpoint to be activated/deactivated. The endpoint must be specified in accordance with the endpoints available in the switch. (Range: 1-2)

Default

No default is defined.

Command Modes

Loopback interface configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to deactivate the selected local tunnel endpoint interface.

```
DmSwitch(config-local-tunnel)#no ltn-endpoint 1
DmSwitch(config-local-tunnel)#
```

You can verify that the local tunnel endpoint interface was activated/deactivated by entering the **show interfaces local-tunnel** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show interfaces local-tunnel	Shows the local-tunnel interfaces.

Chapter 18. Interface G704 Commands

g704 line-type

```
line-type { unframed | pcm31 | pcm31-crc | pcm30-cas | pcm30-cas-crc
}
```

```
no line-type
```

Description

Use the command to define which kind of line type the interface use.

Inserting **no** as a prefix for this command will set line-type as unframed.

Syntax

Parameter	Description
unframed	Line type unframed 32 time slots.
pcm31	Line type framed 31 time slots.
pcm31-crc	Line type framed 31 time slots with CRC.
pcm30-cas	Line type framed 30 time slots with CAS.
pcm30-cas-crc	Line type framed 30 time slots with CAS and CRC.

Default

By default g704 interfaces work as unframed.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If there's any enabled bundle at current g704 interface its not possible to change line-type from pcm31 to pcm30 (and vice-versa), also from unframed to any other. To configure interface must be disabled.

Example

This example shows how to configure interface g704 6 to work as pcm31 with CRC.

```
DM4000 (config)#interface g704 6
DM4000 (config-if-g704-1/6)#line-type pcm31-crc
```

You can verify that the command was executed by entering the **show interface g704 6** privileged EXEC command.

Related Commands

Command	Description
show interfaces g704 timeslots	the Section called <i>show interfaces g704</i> in Chapter 2 Configures inicial timeslot and how many are used.

g704 shutdown

shutdown

no shutdown

Description

Use the shutdown command to disable an interface.

Inserting **no** as a prefix for this command will enable the interface.

Syntax

No parameter accepted.

Default

Interface is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To disable g704 interface (*no shutdown*), no bundle can be mapped to the interface.

Example

This example shows how to enable a g704 interface.

```
DM4000(config)#interface g704 10
DM4000(config-if-g704-1/10)#no shutdown
```

You can verify that the g704 interface is up by entering the **show interfaces g704 10** privileged EXEC command.

Related Commands

No related command.

g704 sync-source

```
sync-source { adaptive bundle bundle-id | system }
```

```
no sync-source
```

Description

Use the command to define the g704 interface transmission synchronization source.

Inserting **no** as a prefix for this command will set sync-source as system.

Syntax

Parameter	Description
adaptive bundle	Uses the clock recovered from an specific bundle.
system	Uses the configured global clock hierarchy system.

Default

By default g704 interfaces work using system clock.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Bundle selected as adaptive clock source must be mapped to the same g704 which is being configured. To configure, the interface must be disabled.

Example

This example shows how to configure interface g704 6 to regenerate clock from bundle 1.

```
DM4000(config)#interface g704 1/6
DM4000(config-if-g704-1/6)#sync-source adaptive bundle 1
```

You can verify that the command was executed by entering the **show interface g704 1/6** privileged EXEC command.

Related Commands

Command	Description
show interfaces g704	the Section called <i>show interfaces g704</i> in Chapter 2

g704 test

```
test { lal | ldl }
```

```
no test
```

Description

Use the command to start local digital loop or local analog loop tests on current g704 interface.

Inserting **no** as a prefix for this command will stop test on current interface.

Syntax

No parameter accepted.

Default

It is disabled by default.

Command Modes

Interface configuration.

Command History

Release	Modification
11.2	This command was introduced.
15.2.16	Added LAL loop option.

Usage Guidelines

Not available.

Example

This example shows how to start ldl test on interface g704 8.

```
DM4000(config)#interface g704 8
DM4000(config-if-g704-1/8)#test ldl
```

You can verify that the command was executed by entering the **show interface g704 8** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces g704</code>	the Section called <i>show interfaces g704</i> in Chapter 2

Chapter 19. Interface E1C Commands

e1c line-type

```
line-type { unframed | pcm31 | pcm31-crc | pcm30-cas | pcm30-cas-crc
}
```

```
no line-type
```

Description

Use the command to define which kind of line type the interface use.

Inserting **no** as a prefix for this command will set line-type as unframed.

Syntax

Parameter	Description
unframed	Line type unframed 32 time slots.
pcm31	Line type framed 31 time slots.
pcm31-crc	Line type framed 31 time slots with CRC.
pcm30-cas	Line type framed 30 time slots with CAS.
pcm30-cas-crc	Line type framed 30 time slots with CAS and CRC.

Default

By default e1c interfaces work as unframed.

Command Modes

Interface configuration.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

If there's any enabled bundle at current e1c interface its not possible to change line-type from pcm31 to pcm30 (and vice-versa), also from unframed to any other. To configure interface must be disabled.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to configure interface e1c 6 to work as pcm31 with CRC.

```
DM4000(config)#interface e1c 6
DM4000(config-if-e1c-1/6)#line-type pcm31-crc
```

You can verify that the information was configured by entering the **show interface e1c 6** privileged EXEC command.

Related Commands

Command	Description
show interfaces e1c timeslots	the Section called <i>show interfaces e1c</i> in Chapter 2
show sdh-map	Configures inicial timeslot and how many are used.
	Show the mappings of SDH interfaces.

e1c shutdown

shutdown

no shutdown

Description

Use the shutdown command to disable an e1c interface.

Inserting **no** as a prefix for this command will enable the interface.

Syntax

No parameter accepted.

Default

Interface is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

To disable e1c interface (*no shutdown*), no bundle can be mapped to the interface.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to enable an e1c interface.

```
DM4000(config)#interface e1c 10
DM4000(config-if-e1c-1/10)#no shutdown
```

You can verify that the e1c interface is up by entering the **show interfaces e1c 10** privileged EXEC command.

Related Commands

No related command.

e1c sync-source

```
sync-source { adaptive bundle bundle-id | system }
```

```
no sync-source
```

Description

Use the command to define the e1c interface transmission synchronization source.

Inserting **no** as a prefix for this command will set sync-source as system.

Syntax

Parameter	Description
adaptive bundle	Uses the clock recovered from an specific bundle.
system	Uses the configured global clock hierarchy system.

Default

By default e1c interfaces work using system clock.

Command Modes

Interface configuration.

Command History

Release	Modification
14.0	This command was introduced.

Usage Guidelines

Bundle selected as adaptive clock source must be mapped to the same e1c which is being configured. To configure, the interface must be disabled.

Example

This example shows how to configure interface e1c 6 to regenerate clock from bundle 1.

```
DM4000(config)#interface e1c 1/6
DM4000(config-if-e1c-1/6)#sync-source adaptive bundle 1
```

You can verify that the command was executed by entering the **show interface e1c 1/6** privileged EXEC command.

Related Commands

Command	Description
show interfaces e1c	the Section called <i>show interfaces e1c</i> in Chapter 2

Chapter 20. Interface Loopback Commands

ip address

ip address { *ip-address/mask* }

no ip address

Description

Sets an IP address for the selected loopback.

Inserting **no** as a prefix for this command will delete the IP address from the selected loopback.

Syntax

Parameter	Description
<i>ip-address/mask</i>	Specifies the IP address and network mask to the selected loopback.

Default

No IP address is defined to selected loopback.

Command Modes

Interface loopback configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a static IP address to the loopback 0.

```
DmSwitch#config
```

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-loop-0)#ip address 100.100.100.1/32
DmSwitch(config-if-loop-0)#end
DmSwitch#
```

You can verify that the IP address was specified by entering the **show running-config** user EXEC command.

Related Commands

Command	Description
mpls enable	Enables MPLS on the specified loopback interface.
show running-config	Shows the current operating configuration.

ipv6 enable

ipv6 enable

no ipv6 enable

Description

Enable IPv6 support for the selected loopback interface.

Inserting **no** as a prefix for this command will disable IPv6 support for the selected loopback interface.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Interface loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable IPv6 in the loopback 0.

```
DmSwitch#config
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-loop-0)#ipv6 enable
DmSwitch(config-if-loop-0)#end
```

You can verify that the IPv6 feature was enabled in the selected loopback interface by entering the **show running-config** user EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ipv6 address

ipv6 address { *ipv6-address/prefix-length* }

ipv6 address { *ipv6-prefix/prefix-length* | **eui-64** }

no ipv6 address

Description

Sets an IPv6 address for the selected loopback.

Inserting **no** as a prefix for this command will delete the IPv6 address from the selected loopback.

Syntax

Parameter	Description
<i>ipv6-address/prefix-length</i>	Specifies the IPv6 address and prefix length to the selected loopback.
<i>ipv6-prefix/prefix-length</i>	Specifies the IPv6 address prefix and prefix length to the selected loopback.
eui-64	Complete the IPv6 address prefix with a suffix in EUI-64 format.

Default

No IP address is defined to selected loopback.

Command Modes

Interface loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

IPv6 feature must be enabled in the specific loopback interface to be able to set and IPv6 address.

Example

This example shows how to specify a static IPv6 address to the loopback 0.

```
DmSwitch#config
```

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-loop-0)#ipv6 address 2001:DB8::1234/64
DmSwitch(config-if-loop-0)#end
DmSwitch#
```

This example shows how to specify an IPv6 address in EUI-64 format to the loopback 0.

```
DmSwitch#config
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-loop-0)#ipv6 address 2001:DB8::/64 eui-64
DmSwitch(config-if-loop-0)#end
DmSwitch#
```

You can verify that the IPv6 address was specified by entering the **show ip** privileged EXEC command.

Related Commands

Command	Description
mpls enable	Enables MPLS on the specified loopback interface.
show running-config	Shows the current operating configuration.
show ip	Shows the IP configuration.

ipv6 ripng

ipv6 ripng

no ipv6 ripng

Description

Enables RIPng routing on this loopback interface. Since it is a loopback interface, the RIPng routing on this interface will be always on passive mode.

The **no** command disables RIPng routing on this interface.

Syntax

No parameter accepted.

Default

RIPng routing process is not associated with the interface.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Interface loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The RIPng process will act only over the specified interface.

Example

This example shows how to specify the RIPng routing process to the specified loopback interface.

```
DmSwitch(config-if-loop-0)#ipv6 ripng
DmSwitch(config-if-loop-0)#
```

You can verify that the RIPng process was associated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ipv6 rip</code>	Shows the OSPFv3 process parameters.
<code>show running-config</code>	Shows the current operating configuration.

isis authentication direction recv-only

```
isis authentication direction recv-only [ level-1 | level-2 ]
```

```
no isis authentication direction recv-only [ level-1 | level-2 ]
```

Description

Use this command to configure that authentication is performed only on IS-IS packets being received in an interface.

Inserting **no** as a prefix for this command will disable the recv-only authentication direction for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the recv-only authentication direction for IS-IS level-1.
level-2	(Optional) Specifies the recv-only authentication direction for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the isis authentication recv-only direction for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the configuration of recv-only authentication direction in a loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis authentication direction recv-only
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in a loopback interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for a loopback interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for a loopback interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for a loopback interface.
show isis	Shows the IS-IS routing table entries.

isis authentication direction send-only

```
isis authentication direction send-only [ level-1 | level-2 ]
```

```
no isis authentication direction send-only [ level-1 | level-2 ]
```

Description

Use this command to configure that authentication is performed only on IS-IS packets being sent in an interface.

Inserting **no** as a prefix for this command will disable the send-only authentication direction for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the send-only authentication direction for IS-IS level-1.
level-2	(Optional) Specifies the send-only authentication direction for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the isis authentication send-only direction for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the configuration of send-only authentication direction in a loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis authentication direction send-only
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction recv-only	Configure the IS-IS recv-only authentication direction in a loopback interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for a loopback interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for a loopback interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for a loopback interface.
show isis	Shows the IS-IS routing table entries.

isis authentication key-chain

```
isis authentication key-chain key-chain name [ level-1 | level-2 ]
```

```
no isis authentication key-chain key-chain name [ level-1 | level-2 ]
```

Description

Configures authentication for IS-IS packets and specifies the set of keys that can be used on an interface.

Inserting **no** as a prefix for this command will disable the authentication key-chain for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
key-chain name	Specifies the key-chain name.
level-1	(Optional) Specifies the authentication key-chain for IS-IS level-1.
level-2	(Optional) Specifies the authentication key-chain for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Configures first the key-chain in the configuration mode and after enables it for the IS-IS router.

Example

The following example enables the key-chain for level-2 in a loopback interface.

```
DmSwitch(config)#key chain isis_level_2
DmSwitch(config-keychain)#key 1
DmSwitch(config-keychain-key)#key-string datacom
```

```
DmSwitch(config-keychain-key) #exit
DmSwitch(config-keychain) #exit
DmSwitch(config) #interface loopback 0
DmSwitch(config-if-lo-0) #isis authentication key-chain isis_level_2 level-2
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction rcv-only	Configure the IS-IS rcv-only authentication direction in a loopback interface.
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in a loopback interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for a loopback interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for a loopback interface.
show isis	Shows the IS-IS routing table entries.

isis authentication mode clear-text

```
isis authentication mode clear-text [ level-1 | level-2 ]
```

```
no isis authentication mode clear-text [ level-1 | level-2 ]
```

Description

The **isis authentication mode** command specifies the type of authentication used for an interface. The parameter **clear-text** enables the clear-text authentication.

Inserting **no** as a prefix for this command will disable the clear-text authentication mode for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the clear-text authentication mode for IS-IS level-1.
level-2	(Optional) Specifies the clear-text authentication mode for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the clear-text authentication mode for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the clear-text authentication mode configuration in a loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis authentication mode clear-text level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction rcv-only	Configure the IS-IS rcv-only authentication direction in a loopback interface.
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in a loopback interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for a loopback interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for a loopback interface.
show isis	Shows the IS-IS routing table entries.

isis authentication mode hmac-md5

```
isis authentication mode hmac-md5 [ level-1 | level-2 ]
```

```
no isis authentication mode hmac-md5 [ level-1 | level-2 ]
```

Description

The **isis authentication mode** command specifies the type of authentication used for an interface. The parameter **hmac-md5** enables the Message Digest 5 (MD5) authentication.

Inserting **no** as a prefix for this command will disable the hmac-md5 authentication mode for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the hmac-md5 authentication mode for IS-IS level-1.
level-2	(Optional) Specifies the hmac-md5 authentication mode for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the hmac-md5 authentication mode for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the hmac-md5 authentication mode configuration in a loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis authentication mode hmac-md5 level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction rcv-only	Configure the IS-IS rcv-only authentication direction in a loopback interface.
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in a loopback interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for a loopback interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for a loopback interface.
show isis	Shows the IS-IS routing table entries.

isis circuit-type

```
isis circuit-type { level-1 | level-2 | level-1-2 }
```

```
no isis circuit-type
```

Description

This command configures the circuit-type of the IS-IS routing process on an interface.

Inserting **no** as a prefix for this command will reset the configured circuit-type to the default configuration.

Syntax

Parameter	Description
level-1	Configures this interface as level-1 only.
level-2	Configures this interface as level-2 only.
level-1-2	Configures this interface as both level-1 and level-2.

Default

The default configuration is level-1-2.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command allows the configuration of an interface's circuit type level for the IS-IS routing process independently of the IS type configured in the router, given that the desired circuit type level is possible within that router. For example, a level-1-2 router allows the configuration of circuit types level-1 only, level-2 only or level-1-2 in the interfaces that belong to its routing process. However, a level-1 router will only allow configuration of circuit type level-1 on its interfaces.

Example

The following example shows the circuit type configuration:

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis circuit-type level-1
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
is-type	Configure the IS-IS Level type
show isis	Shows the IS-IS routing table entries.

isis hello-interval

```
isis hello-interval hello_interval_value [ level-1 | level-2 ]
```

```
no isis hello-interval [ level-1 | level-2 ]
```

Description

Maximum period, in milliseconds, between IS-IS Hello (IIH) PDUs on multiaccess networks for LANs. The range of valid values for this field is 30 - 360000.

Inserting **no** as a prefix for this command will set this value to the default one.

Syntax

Parameter	Description
hello_interval_value	Specifies the hello interval value.
level-1	(Optional) Specifies the hello interval value for IS-IS level-1.
level-2	(Optional) Specifies the hello interval value for IS-IS level-2.

Default

The default hello interval value is 3000.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the hello interval for an interface. If neither the level-1 nor level-2 is configured, the command is applied to both levels. However, if this router is the DIS(Designated IS), the actual interval used will be 1/3 of the configured hello interval. This happens due to the need of fast failure detection for the DIS.

Example

The following example shows the hello interval configuration in an loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis hello interval 30
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
graceful-restart	Configure graceful restart parameters
show isis	Shows the IS-IS routing table entries.

isis metric

```
isis metric metric_value [ level-1 | level-2 ]
```

```
no isis metric [ metric_value [ level-1 | level-2 ] ]
```

Description

Use this command to configure the metric value of a circuit used for IS-IS. The range of valid values for this field is 1 - 63.

Inserting **no** as a prefix for this command will set this value to the default one for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
metric_value	Specifies the metric value.
level-1	(Optional) Specifies the metric for IS-IS level-1.
level-2	(Optional) Specifies the metric for IS-IS level-2.

Default

The default metric value is 10.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the metric for an interface. If neither the level-1 nor level-2 is configured, the command is applied to both levels.

Example

The following example shows the metric configuration in a loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis metric 12
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis metric-wide	Configure the IS-IS wide metric for a loopback
metric-style	Configure the IS-IS metric style
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

isis metric-wide

```
isis metric-wide metric_value [ level-1 | level-2 ]
```

```
no isis metric-wide [ level-1 | level-2 ]
```

Description

Use this command to configure the wide metric value of a circuit used for IS-IS. The range of valid values for this field is 1 - 16777215.

Inserting **no** as a prefix for this command will set this value to the default one for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
metric_value	Specifies the wide metric value.
level-1	(Optional) Specifies the wide metric for IS-IS level-1.
level-2	(Optional) Specifies the wide metric for IS-IS level-2.

Default

The default wide metric value is 10.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the wide metric for an interface. It is necessary to configure the metric style for "wide" in the router isis configuration. If neither the level-1 nor level-2 is configured, the command is applied to both levels.

Example

The following example shows the wide metric configuration in a loopback interface.

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis metric-wide 12
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis metric	Configure the IS-IS metric in a loopback
metric-style	Configure the IS-IS metric style
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

isis passive-interface

isis passive-interface *area-name*

no isis passive-interface *area-name*

Description

This command configures an interface as a passive IS-IS interface.

Inserting **no** as a prefix for this command will remove this interface from the IS-IS routing process.

Syntax

Parameter	Description
area-name	Area name of IS-IS router to which this interface should be associated.

Default

There is no default configuration for this command.

Command Modes

Loopback configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command allows an interface to be inserted into the IS-IS routing process without actually sending or receiving any IS-IS packets. This means that its IP address will be redistribute into IS-IS and, consequently, to other neighbors, removing the need to redistribute all connected routes.

Example

The following example shows the passive interface configuration:

```
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-lo-0)#isis passive-interface isisl
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>router isis</code>	Enables and accesses the IS-IS configuration.
<code>show ip route</code>	Shows the IP routing table.
<code>show isis</code>	Shows the IS-IS routing table entries.

mpls enable ^[1] ^[3] ^[6]

mpls enable

no mpls enable

Description

Set the IP address of the specified loopback interface as LSR Id for MPLS protocols.

Inserting **no** as a prefix for this command will remove the configuration from the selected loopback.

Syntax

No parameter accepted.

Default

LSR identifier is not defined.

Command Modes

Loopback configuration.

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The LSR-ID for MPLS protocols is obtained from a local IP address assigned to a loopback interface that has MPLS enabled. A loopback interfaces' IP address, whose both administrative and operational status never change, is considered a stable address in the system.

Although the user can activate up to 8 loopback interfaces and assign an IP address to each one, it's allowed to enable MPLS only in one of them because all MPLS protocols (e.g. LDP, RSVP) should use the same LSR-ID.

Changing the current LSR-ID affects those protocols and their running sessions. Both LDP and RSVP have to tear down running connections in order to advertise their new router identity. At the same time, all peers must accept to establish a connection with the new local router identity.

Example

This example shows how to enable loopback IP to be LSR Identifier.

```
DmSwitch#config
DmSwitch(config)#interface loopback 0
DmSwitch(config-if-loop-0)#mpls enable
DmSwitch(config-if-loop-0)#end
DmSwitch#
```

You can verify the loopback configuration by entering the **show interfaces loopback** user EXEC command. This can also be verified through the **show mpls ldp parameters** user EXEC command. The IP address of the loopback interface is listed in the "Local addresses" section of the command output.

Related Commands

Command	Description
interface vlan	Enables the VLAN configuration mode.
ldp enable	Enable LDP capability in selected VLAN.
loopback ip address	Sets an IP address for the selected loopback.
show running-config	Shows the current operating configuration.
show interfaces loopback	Shows the interfaces loopback.
show mpls ldp parameters	Shows current LDP parameters.

shutdown

shutdown

no shutdown

Description

Deactivates the selected loopback interface.

Inserting **no** as a prefix for this command will reactivate the selected loopback interface.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Loopback interface configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to deactivate the selected loopback interface.

```
DmSwitch(config-if-lo-1)#shutdown
DmSwitch(config-if-lo-1)#
```

You can verify that the loopback interface was deactivated by entering the **show interfaces loopback** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show interfaces loopback</code>	Shows the interfaces loopback.

Chapter 21. Interface Port-channel Commands

load-balance

```
load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac |  
enhanced }
```

```
no load-balance
```

Description

Configures load distribution method among the ports.

Inserting **no** as a prefix for this command will reset the load balancing to its default value.

Syntax

Parameter	Description
dst-ip	Destination IP address.
dst-mac	Destination MAC address.
src-dst-ip	Source and destination IP addresses.
src-dst-mac	Source and destination MAC addresses.
src-ip	Source IP address.
src-mac	Source MAC address.
enhanced	MPLS labels, IP addresses (source and destination), MAC addresses (source and destination) and TCP/UDP ports (source and destination). NOTE: for MPLS packets, only the labels and the external MAC addresses are considered.

Default

Load-balance: source and destination MAC addresses.

Command Modes

Interface configuration.

Command History

Release	Modification
4.0	This command was introduced.

Release	Modification
13.6	Enhanced balance configuration was added.

Usage Guidelines

This will configure the port selection criteria for egress traffic of Port-Channels. For chassis systems, it may be necessary to configure also the load balance of the internal chassis connections (please refer to the related commands).

Example

This example shows how to change the load distribution method.

```
DmSwitch(config-if-port-ch-1)#load-balance src-ip
DmSwitch(config-if-port-ch-1)#
```

You can verify that the configuration was made by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
show interfaces status	Shows interface configuration status.
show running-config	Shows the current operating configuration.
chassis load-balance	Configures load balance for internal chassis connections.

set-member ethernet

```
set-member ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-  
port-number [ last-unit-number/ ] last-port-number }
```

```
no set-member ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ]  
first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

Adds Ethernet ports to selected port-channel.

Inserting **no** as a prefix for this command will remove ports from selected port-channel.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Adds a range of units and ports.

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add the Ethernet port 1 to selected port-channel.

```
DmSwitch(config-if-port-ch-1)#set-member ethernet 1
DmSwitch(config-if-port-ch-1)#
```

You can verify that the configuration was made by entering the **show interfaces status** privileged EXEC command.

Related Commands

Command	Description
show interfaces status	Shows interface configuration status.
show running-config	Shows the current operating configuration.

lACP

lACP

no lACP

Description

Enables use of LACP in port-channel.

Inserting **no** as a prefix for this command will disable LACP for port-channel.

Syntax

No parameter accepted.

Default

LACP is disabled by default on port-channels.

Command Modes

Interface configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Once LACP is enabled in the port-channel, LACPDUs will be sent and received through each member port. Based on the information exchanged, only ports that are considered OK to be aggregated will be enabled on the port-channel. Otherwise, the member interface will remain inactive.

Example

This example shows how to create a new port-channel, add interfaces Ethernet 5 and 6 and enable LACP on it.

```
DmSwitch(config)#interface port-channel 3
DmSwitch(config-if-port-ch-3)#set-member ethernet range 5 6
DmSwitch(config-if-port-ch-3)#lACP
DmSwitch(config-if-port-ch-3)#
```

You can verify that LACP was enabled for the corresponding ports using **show interfaces status** and **show lACP** privileged EXEC command.

Related Commands

Command	Description
<code>debug</code>	Enables the printing of debug messages.
<code>show interfaces status</code>	Shows interface configuration status.
<code>show lacp counters</code>	Shows the LACP traffic counters.
<code>show lacp port-channel</code>	Shows the LACP information by port-channel.
<code>show lacp internal</code>	Shows the LACP internal information.
<code>show lacp neighbors</code>	Shows the LACP neighbors information.
<code>show lacp sysid</code>	Shows the system identifier used by LACP.

Chapter 22. Interface PTP Commands

ptp announce-rate

```
announce-rate { 1pps | 0.5pps | 0.25pps | 0.125pps }
```

```
no announce-rate
```

Description

This command defines the rate which announce packets are sent.

Inserting **no** as a prefix for this command will set announce-rate to its default value.

Syntax

Parameter	Description
1pps	1 packet per second.
0.5pps	1 packets every 2 seconds.
0.25pps	1 packets every 4 seconds.
0.125pps	1 packets every 8 seconds.

Default

The default value is 1 packet per second.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This examples shows how to configure interface ptp 1 to send announce packet every two seconds

```
DM4000(config)#interface ptp 1
DM4000(config-if-ptp-1/1)#announce-rate 0.5pps
```

You may check the configured value by using the command **show interface ptp 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces ptp	Shows ptp interface configuration.

ptp delay-req-rate

```
delay-req-rate { 64pps | 32pps | 16pps | 8pps | 4pps | 2pps | 1pps |  
0.5pps | 0.25pps | 0.125pps }
```

```
no delay-req-rate
```

Description

This command defines the rate which delay request packets are sent.

Inserting **no** as a prefix for this command will set delay-req-rate to its default value.

Syntax

Parameter	Description
64pps	64 packets per second.
32pps	32 packets per second.
16pps	16 packets per second.
8pps	8 packets per second.
4pps	4 packets per second.
2pps	2 packets per second.
1pps	1 packet per second.
0.5pps	1 packets every 2 seconds.
0.25pps	1 packets every 4 seconds.
0.125pps	1 packets every 8 seconds.

Default

The default value is 1 packet per second.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This examples shows how to configure interface ptp 1 to send one packet of delay request per second.

```
DM4000 (config)#interface ptp 1
DM4000 (config-if-ptp-1/1)#delay-req-rate 1pps
```

You may check the configured value by using the command **show interface ptp 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces ptp	Shows ptp interface configuration.

ptp destination-ip-address

destination-ip-address [*ip-address*]

no destination-ip-address

Description

Use this command to define a destination ip address for current interface.

Inserting **no** as a prefix for this command will remove the configured destination-ip-address.

Syntax

Parameter	Description
ip-address	destination ip address

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

To configure ptp interface must be disabled.

Example

This example shows how to set a destination address for interface ptp 2.

```
DM4000(config)#interface ptp 2
DM4000(config-if-ptp-1/2)#destination-ip-address 10.0.0.254
```

You can verify that the command was executed by entering the **show interface ptp 1** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces ptp</code>	Shows ptp interface configuration.
<code>ip-next-hop</code>	Defines the ip address of the next network hop.

ptp ip-next-hop

ip-next-hop [*ip-address*]

no ip-next-hop

Description

Define an address of next hop of the network. If none is defined, it use configured destination ip address.

Inserting **no** as a prefix for this command will remove the configured ip-next-hop.

Syntax

Parameter	Description
ip-address	ip address of next hop.

Default

Destination IP address is used if ip-next-hop is not configured.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

To configure ptp interface must be disabled.

Example

This example shows how to define a next hop address.

```
DM4000(config)#interface ptp 10
DM4000(config-if-ptp-1/10)#ip-next-hop 10.10.10.10
```

You can verify that the command was executed by entering the **show interface ptp 10** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces ptp</code>	Shows ptp interface configuration.
<code>destination-ip-address</code>	Defines destination ip address.

ptp name

name [*text*]

no name

Description

This command is used to define a label for the interface.

Inserting **no** as a prefix for this command will remove the configured name.

Syntax

Parameter	Description
text	"text" interface ptp name

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

The interface ptp name cannot be longer than 127 characters. To configure ptp interface must be disabled.

Example

This example shows how to set a interface ptp name for an interface.

```
DM4000(config)#interface ptp 1
DM4000(config-if-ptp-1/1)#name abc001
```

You can verify that the command was executed by entering the **show interface ptp 1** user EXEC command.

Related Commands

Command	Description
<code>show interfaces ptp</code>	Shows ptp interface configuration.

ptp role

```
role { master | slave }
```

Description

This command defines the role which interface ptp will operate.

Syntax

Parameter	Description
master	Interface will act as ordinary master.
slave	Interface will act as ordinary slave.

Default

The default value is role master.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

The interface should be disabled to change this parameter.

Example

This example shows how to configure interface ptp 1 as a slave clock.

```
DM4000(config)#interface ptp 1
DM4000(config-if-ptp-1/1)#role slave
```

You may check the configured value by using the command **show interface ptp 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces ptp	Shows ptp interface configuration.

ptp shutdown

shutdown

no shutdown

Description

Use the shutdown command to disable an interface.

Inserting **no** as a prefix for this command will enable the interface.

Syntax

No parameter accepted.

Default

Interface is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

When enabling (*no shutdown*) a ptp interface, all coherence checks are done. If there is some inconsistent configuration an error message is displayed and the interface does not go up.

Example

This example shows how to enable interface ptp 10.

```
DM4000(config)#interface ptp 10
DM4000(config-if-ptp-1/10)#no shutdown
```

You can verify that the ptp interface is up by entering the **show interfaces ptp 10** privileged EXEC command.

Related Commands

No related command.

ptp source-ip-address

source-ip-address *ip address*

no source-ip-address

Description

Set a source ip address for the current ptp interface

Inserting **no** as a prefix for this command will remove the configured source-ip-address.

Syntax

Parameter	Description
<i>ip address</i>	ptp source ip address

Default

No default is defined.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Entered address must be a valid IP address.

Example

This example define the address 10.1.1.22 as the source address of interface ptp 1.

```
DM4000(config)#interface ptp 1
DM4000(config-if-ptp-1/1)#source-ip-address 10.1.1.22
```

The configuration may be checked using the command **show interfaces ptp 1** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces ptp</code>	Shows ptp interface configuration.

ptp sync-rate

```
sync-rate { 64pps | 32pps | 16pps | 8pps | 4pps | 2pps | 1pps |  
0.5pps | 0.25pps | 0.125pps }
```

sync-rate

Description

This command defines the rate which sync packets are sent.

Inserting **no** as a prefix for this command will set sync-rate to its default value.

Syntax

Parameter	Description
64pps	64 packets per second.
32pps	32 packets per second.
16pps	16 packets per second.
8pps	8 packets per second.
4pps	4 packets per second.
2pps	2 packets per second.
1pps	1 packet per second.
0.5pps	1 packets every 2 seconds.
0.25pps	1 packets every 4 seconds.
0.125pps	1 packets every 8 seconds.

Default

The default value is 64 packets per second.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This examples shows how to configure interface ptp 1 to send synchronization packet every two seconds

```
DM4000 (config)#interface ptp 1
DM4000 (config-if-ptp-1/1)#sync-rate 0.5pps
```

You may check the configured value by using the command **show interface ptp 1** privileged EXEC command.

Related Commands

Command	Description
show interfaces ptp	Shows ptp interface configuration.

ptp transport-mode

```
transport-mode { ipv4 { unicast [ negotiation ] } }
```

```
no transport-mode ipv4 unicast [ negotiation ]
```

Description

Configure transport mode of ptp interface.

Syntax

Parameter	Description
<code>ipv4</code>	Interface will send PTP messages on ipv4 protocol.
<code>unicast</code>	Interface will send PTP messages by unicast.
<code>negotiation</code>	Interface will send PTP messages by unicast with negotiation.

Default

The default value is "transport-mode ipv4 unicast" (unicast without negotiation)

Command Modes

Interface configuration.

Command History

Release	Modification
14.10	This command was introduced.

Usage Guidelines

The interface should be disabled to change this parameter.

Example

This example shows how to configure interface ptp 1 transport-mode as unicast negotiation.

```
DM4000(config)#interface ptp 1
DM4000(config-if-ptp-1/1)#transport-mode ipv4 unicast negotiation
```

You may check the configured value by using the command **show interface ptp 1** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces ptp</code>	Shows ptp interface configuration.

ptp vlan

vlan *vlan-id* **priority** *priority-level*

no vlan

Description

Use this command to define in which vlan precision time protocol interface will work.

Inserting **no** as a prefix for this command will remove the configured VLAN.

Syntax

Parameter	Description
vlan-id	Specifies VLAN ID used in interface PTP. (Range: 1-4094)
priority-level	Specifies priority used in interface PTP. (Range: 0-7)

Default

By default, every ptp interface is configured with vlan 1 and priority 0.

Command Modes

Interface configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Selected vlan must .

Example

This example shows how to configure interface ptp 1 of unit 2 to use vlan 10.

```
DM4000(config-if-vlan-10)#interface ptp 2/1
DM4000(config-if-ptp-2/1)#vlan 10 priority 2
```

You may check the configuration using the command *show interfaces ptp 2/1*

Related Commands

Command	Description
<code>show interfaces ptp</code>	Shows ptp interface configuration.

Chapter 23. Interface SDH Commands

sdh path-trace

```
path-trace { evaluation | type { string | byte } | rx { string | byte } value | tx { string | byte } value }
```

```
no path-trace { evaluation | type | rx { string | byte } | tx { string | byte } }
```

Description

Configure path trace of selected SDH interface. It will determine how j0 is going to be interpreted and transmitted.

Syntax

Parameter	Description
type { string byte }	Select if string or byte is used at path-trace (j0).
rx { string byte } <i>value</i>	Configure the expected value of path-trace which is received.
tx { string byte } <i>value</i>	Configure value of path-trace to be sent.
evaluation	Set RS-TIM alarm evaluation.

Default

By default the evaluation of path-trace is desactivated and type is string.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

The byte configuration is set by its decimal value, not hexa. The sdh interface must be enabled to evaluation of path trace work.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

```
DM4000(config)#interface sdh 2/4
DM4000(config-if-sdh-2/4)#path-trace rx byte 124
DM4000(config-if-sdh-2/4)#path-trace tx byte 242
DM4000(config-if-sdh-2/4)#path-trace type byte
DM4000(config-if-sdh-2/4)#path-trace evaluation
```

You can verify that the command was executed by entering the **show interface sdh 2/4** privileged EXEC command.

Related Commands

Command	Description
vc4 path-trace	Configure vc4 path-trace.
vc12 path-trace	Configure vc12 path-trace.

sdh shutdown

shutdown

no shutdown

Description

Use the shutdown command to disable an SDH interface.

Inserting **no** as a prefix for this command will enable the SDH interface.

Syntax

No parameter accepted.

Default

Interface SDH is disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to enable interface sdh 1.

```
DM4000(config)#interface sdh 1
DM4000(config-if-sdh-1/1)#no shutdown
```

You can verify that the sdh interface is up by entering the **show interfaces sdh 1** privileged EXEC command.

Related Commands

No related command.

sdh test

```
test { loop { back | front } | laser-force { on | off }
```

```
no test [ loop { back | front } | lase-force ]
```

Description

Use this command to set a variety of tests on the SDH interface.

Syntax

Parameter	Description
loop { back front }	Insert an loop on the front or at the backend of a given interface of the equipment.
laser-force { on off }	Force interface laser to keep it turned on or off.
no test	Disable any activated test.
no test lase-force	Disable laser-force test.
no test loop	Disable loop tests.

Default

All tests are disabled by default.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

How to set loop on the front-end of sdh interface 1 of unit 2 and force the laser on at interface 2.

```
DM4000(config)#interface sdh 2/1
DM4000(config-if-sdh-2/1)#test loop front
DM4000(config-if-sdh-2/1)#interface sdh 2/2
```

```
DM4000(config-if-sdh-2/2)#test laser-force on
```

You can verify that the command was executed by entering the **show running-config** privileged EXEC command.

Related Commands

No related command.

sdh vc4

vc4 [*vc4-id*]

Description

Use this command to start configuring vc4 settings.

Syntax

Parameter	Description
<i>vc4-id</i>	Get inside configuration prompt of the vc4 of index <i>vc4-id</i>

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to get to the vc4 prompt of the second stm interface of a given unit.

```
DM4000 (config-if-sdh-2/3) #vc4 1
DM4000 (config-if-sdh-2/3-vc4-1) #
```

You can verify that the command was executed by the prompt modification, which is now on an sdh-X-vc4-Y.

Related Commands

Command	Description
h4-multiframe	Configure the multiframe identifier.
path-trace	Configure vc4 path-trace.

Command	Description
<code>path-label</code>	Configure vc4 path-label.

Chapter 24. Interface SDH VC4 Commands

sdh vc4 h4-multiframe

```
h4-multiframe { reduced-sequence [ 0 | 1 ] | full-sequence | c0c1-sequence }
```

```
no h4-multiframe
```

Description

Use this command to configure the byte which indicates the framelabel for a multiframe in the next VC4 payload.

Syntax

Parameter	Description
reduced-sequence [0 1]	Set H4-Multiframe to reduced-sequence and its value.
full-sequence	Set H4-Multiframe to full-sequence.
c0c1-sequence	Set H4-Multiframe to c0c1-sequence.

Default

By default its configured as *reduced-sequence 0* .

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to set h4-multiframe to operate using c0c1-sequence.

```
DM4000 (config-if-sdh-1/1) #vc4 1
```

```
DM4000(config-if-sdh-1/1-vc4-1)#h4-multiframe c0c1-sequence
DM4000(config-if-sdh-1/1-vc4-1)#
```

You can verify that the command was executed by entering the *show running-config* command **COMMAND** privileged EXEC command.

Related Commands

No related command.

sdh vc4 path-label

path-label { *equipped-non-specific* | *tug-structure* | *mapping-under-development* }

no path-label

Description

Use to configure byte C2 of the vc4 - it's used to describe the contents and payload structure.

Syntax

Parameter	Description
<i>equipped-non-especific</i>	Set path-label byte(C2) value (0x01).
<i>tug-structure</i>	Set path-label byte(C2) value (0x02).
<i>mapping-under-development</i>	Set path-label byte(C2) value (0x05).

Default

The default value is *equipped-non-specific* .

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to configure a path-label with tug-structure value.

```
DM4000(config)#interface sdh 2/2
DM4000(config-if-sdh-2/2)#vc4 1
DM4000(config-if-sdh-2/2-vc4-1)#path-label tug-structure
DM4000(config-if-sdh-2/2-vc4-1)#
```

You can verify that the command was executed by entering the **show interface sdh 2/4** privileged EXEC command.

Related Commands

Command	Description
vc4	Select vc4
vc12 path-label	Configure vc12 path-label.

sdh vc4 path-trace

```
path-trace { evaluation | string-size { 16 | 64 } | rx { mode string | mode hex }  
value | tx { mode string | mode hex } value }
```

```
no path-trace { evaluation | string-size | rx | tx }
```

Description

Configure path trace of selected vc4 interface and if it's evaluated or not by the equipment.

Syntax

Parameter	Description
evaluation	Set RS-TIM alarm evaluation of j1 byte.
string-size { 16 64 }	Define the size (in bytes) of the path-trace.
tx { mode string mode hex } value	Configure the data that will be sent on the path-trace byte (J1).
rx { mode string mode hex } value	Configure the data that is expected to be received on the path-trace byte (J1), if it does not match HP-TIM alarm is raised.

Default

By default the evaluation of path-trace is desactivated and the string-size is 64 bytes long.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

The byte configuration is set by its decimal value, not hexa. The sdh interface must be enabled to evaluation of path trace work.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

```
DM4000(config)#interface sdh 2/4
DM4000(config-if-sdh-2/4)#vc4 1
DM4000(config-if-sdh-2/4-vc4-1)#path-trace rx byte 124
DM4000(config-if-sdh-2/4-vc4-1)#path-trace tx byte 242
DM4000(config-if-sdh-2/4-vc4-1)#path-trace type byte
DM4000(config-if-sdh-2/4-vc4-1)#path-trace evaluation
```

You can verify that the command was executed by entering the **show interface sdh 2/4** privileged EXEC command.

Related Commands

Command	Description
vc4	Select vc4
stm path-trace	Configure stm path-trace.
vc12 path-trace	Configure vc12 path-trace.

sdh vc4 tug-structure

```
tug-structure [ 100 { tu12 | tu3 } | 200 { tu12 | tu3 } | 300 { tu12 | tu3 } ]
```

```
no tug-structure [ 100 | 200 | 300 ]
```

Description

Use this command to configure the structure of vc4.

Syntax

Parameter	Description
100 [tu12 tu3]	Configure if vc4 work as 21*vc12 (tu12) or 1*vc3 (tu3). This command configure all virtual carriers with k=1.
200 [tu12 tu3]	Configure if vc4 work as 21*vc12 (tu12) or 1*vc3 (tu3). This command configure all virtual carriers with k=2.
300 [tu12 tu3]	Configure if vc4 work as 21*vc12 (tu12) or 1*vc3 (tu3). This command configure all virtual carriers with k=3.

Default

By default vc4 operate as tu12 structured.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

If a given structure is mapped (to another sdh interface or to e1c interface), then it cannot change its structure.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to set vc4 of the first sdh interface to operate structured with tu3.

```
DM4000(config)#interface sdh 1
DM4000(config-if-sdh-1/1)#vc4 1
DM4000(config-if-sdh-1/1-vc4-1)#tug-structure 100 tu3
DM4000(config-if-sdh-1/1-vc4-1)#tug-structure 200 tu3
DM4000(config-if-sdh-1/1-vc4-1)#tug-structure 300 tu3
```

You can verify that the command was executed by entering the *show running-config* command **COMMAND** privileged EXEC command.

Related Commands

Command	Description
vc4_structure	Configure vc4 mode of operation.

sdh vc4 vc4-structure

vc4-structure { bearer|trail }

no vc4-structure

Description

Use this command to configure the mode of operation of vc4.

Syntax

Parameter	Description
bearer	Configure vc4 as bearer.
trail	Configure vc4 as trail.

Default

By default vc4 operate as bearer.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to set vc4 as trail

```
DM4000(config)#interface sdh 1
DM4000(config-if-sdh-1/1)#vc4 1
DM4000(config-if-sdh-1/1-vc4-1)#vc4-structure trail
```

You can verify that the command was executed by entering the *show running-config* command **COMMAND** privileged EXEC command.

Related Commands

Command	Description
<code>tug_structure</code>	Configure vc4 tug structure.

sdh vc4 vc12

vc12 *klm*

Description

Use the command to enter on the prompt of vc12 configurations.

Syntax

Parameter	Description
<i>klm</i>	Defines which vc12 is going to be configured. It stands for 3 different values putted together. Which ranges may go from: K (1~3), L (1~7) and M(1~3).

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to select vc12 number 321.

```
DM4000(config)#interface sdh 4
DM4000(config-if-sdh-1/4)#vc4 1
DM4000(config-if-sdh-1/4-vc4-1)#vc12 321
DM4000(config-if-sdh-1/4-vc4-1-vc12-321)#
```

You can verify that the command was executed by noting the change of the prompt.

Related Commands

No related command.

Chapter 25. Interface SDH VC4 VC12 Commands

sdh vc12 path-label

```
path-label { equipped-non-especific | asynchronous }
```

```
no path-label
```

Description

Use to configure the signal label of byte V5 on the selected vc12.

Syntax

Parameter	Description
equipped-non-especific	Set path-label byte(V5) value.
asynchronous	Set path-label byte(V5) value.

Default

The default value is *asynchronous* .

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

The current vc12 must be mapped to be configured.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

This example shows how to configure a path-label with equipped-non-especific value.

```
DM4000(config)#sdh-map unit 4 new elc 1 to sdh 1 vc4 1 vc12 373
DM4000(config)#interface sdh 4/1
DM4000(config-if-sdh-4/1)#vc4 1
DM4000(config-if-sdh-4/1-vc4-1)#vc12 373
DM4000(config-if-sdh-4/1-vc4-1-vc12-373)#path-label equipped-non-especific
```

You can verify that the command was executed by entering the **show interface sdh 2/4** privileged EXEC command.

Related Commands

Command	Description
vc12	Select vc12
vc4 path-label	Configure vc4 path-label.
sdh-map	Configure mapping of SDH interfaces and E1C.

sdh vc12 path-trace

```
path-trace { evaluation | rx { string } text | tx { string } text }
```

```
no path-trace { evaluation | rx | tx }
```

Description

Configure path trace of selected vc12 interface and if it's evaluated or not by the equipment.

Syntax

Parameter	Description
evaluation	Set LP-TIM alarm evaluation of j2 byte.
tx string <i>text</i>	Configure the data that will be sent on the path-trace byte (J2).
rx string <i>text</i>	Configure the data that is expected to be received on the path-trace byte (J2), if it does not match LP-TIM alarm is raised.

Default

By default the evaluation of path-trace is deactivated.

Command Modes

Privileged EXEC.

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

Path-trace string is limited on 15 characters.

This command is only available on ETH16GX+4STM1 and ETH16GX+4STM1+2x10GX boards.

Example

```
DM4000(config)#interface sdh 2
DM4000(config-if-sdh-1/2)#vc4 1
```

```
DM4000 (config-if-sdh-1/2-vc4-1) #vc12 121
DM4000 (config-if-sdh-1/2-vc4-1-vc12-121) #path-trace rx string j2_rx
DM4000 (config-if-sdh-1/2-vc4-1-vc12-121) #path-trace tx string j2_tx
DM4000 (config-if-sdh-1/2-vc4-1-vc12-121) #path-trace evaluation
```

You can verify that the command was executed by entering the **show interface sdh 1/2** privileged EXEC command.

Related Commands

Command	Description
vc12	Select vc12
sdh path-trace	Configure stm path-trace.
vc4 path-trace	Configure vc4 path-trace.

Chapter 26. Interface Private VLAN Commands

community-vlan

community-vlan *index*

no community-vlan *index*

Description

Enables the Community VLAN configuration mode. The Community VLAN is created and enabled if it does not exist.

Inserting **no** as a prefix for this command will remove the specified Community VLAN.

Syntax

Parameter	Description
<i>index</i>	Enables for a specific Community VLAN index. (Range: 1-4094)

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

A community VLAN can only belong to one private VLAN and cannot be already created as a regular VLAN.

Example

This example shows how to enable a Community VLAN with index 100 associated with a private VLAN 10.

```
DmSwitch(config-if-pvlan-10)#community-vlan 100
DmSwitch(config-if-pvlan-10-community-100)#
```

You can verify that the Community VLAN was accepted as it is shown in the new prompt.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

isolated-vlan

isolated-vlan *index*

no isolated-vlan *index*

Description

Enables the isolated VLAN configuration mode. The isolated VLAN is created and enabled if it does not exist.

Inserting **no** as a prefix for this command will remove the specified isolated VLAN.

Syntax

Parameter	Description
<i>index</i>	Enables for a specific isolated VLAN index. (Range: 1-4094)

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

An isolated VLAN can only belong to one private VLAN and cannot be already created as a regular VLAN.

Example

This example shows how to enable a isolated VLAN with index 900 associated with a private VLAN 10.

```
DmSwitch(config-if-pvlan-10)#isolated-vlan 900
DmSwitch(config-if-pvlan-10-isolated-900)#
```

You can verify that the isolated VLAN was accepted as it is shown in the new prompt.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

mac-address-table learn

`mac-address-table learn`

`no mac-address-table learn`

Description

Enables MAC address learning on the selected Private VLAN.

Inserting **no** as a prefix for this command will disable VLAN MAC address learning.

Syntax

No parameter accepted.

Default

VLAN MAC address learning is enabled for all Private VLANs.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command can enable or disable learning of MAC addresses in the selected Private VLAN.

Example

This example shows how to enable the VLAN MAC address learning for a specific Private VLAN interface.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#mac-address-table learn
DmSwitch(config-if-pvlan-1000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>clear mac-address-table</code>	Erases entries stored in the MAC address table.

Command	Description
<code>mac-address-table maximum</code>	Sets the Private VLAN MAC address table maximum number of entries.
<code>show mac-address-table</code>	Shows the MAC address table.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

mac-address-table maximum

mac-address-table maximum *num-of-macs*

no mac-address-table maximum

Description

Use the mac-address-table maximum to configure the maximum limit of MAC address per Private VLAN for each unit.

The **no** command form removes the configured limit.

Syntax

Parameter	Description
<i>maximum</i>	Configures the maximum number of MAC addresses.

Default

No limit is configured.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This value also applies to the MACs learned in the secondary VLANs associated to this primary VLAN.

Example

This example shows how to set the limit of MAC address table entries on the selected Private VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#mac-address-table maximum 10
DmSwitch(config-if-pvlan-1000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>clear mac-address-table</code>	Erases entries stored in the MAC address table.
<code>mac-address-table learn</code>	Enables MAC address learning on the selected Private VLAN.
<code>show mac-address-table</code>	Shows the MAC address table.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

name

name *name*

no name

Description

Specifies the Private VLAN name.

Inserting **no** as a prefix for this command will remove the Private VLAN name.

Syntax

Parameter	Description
<i>name</i>	Specifies a Private VLAN name.

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a Private VLAN name.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#name VlanTest
DmSwitch(config-if-pvlan-1000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

set-member interswitch

```
set-member interswitch tagged { ethernet { all | [ unit-number/ ] port-number | range  
{ [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member interswitch tagged { port-channel channel-group-number }
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ]  
first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ]
```

Description

Adds interswitch members to selected Private VLAN.

Entering with **no** command, it removes interswitch members from selected Private VLAN.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Adds a range of specific units and ports.
port-channel channel-group-number	Adds a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

For interswitch ports, only tagged members are allowed.

Example

This example shows how to add an ethernet port range with interswitch members to a Private VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#set-member interswitch tagged ethernet range 1/25 1/28
DmSwitch(config-if-pvlan-1000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

set-member promiscuous

```
set-member promiscuous {tagged|untagged} { ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member promiscuous {tagged|untagged} { port-channel channel-group-number }
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ]
```

Description

Adds promiscuous members to selected Private VLAN.

Entering with **no** command, it removes promiscuous members from selected Private VLAN.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Adds a range of specific units and ports.
port-channel channel-group-number	Adds a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available

Example

This example shows how to add an ethernet port range with promiscuous tagged members to a Private VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#set-member promiscuous tagged ethernet range 1/25 1/28
DmSwitch(config-if-pvlan-1000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

shutdown

shutdown

no shutdown

Description

Deactivates the selected Private VLAN.

Inserting **no** as a prefix for this command will reactivate the selected Private VLAN.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command does not affect the secondary VLANs associated with this primary. The only effect is that no data will pass between primary and secondary ports.

Example

This example shows how to deactivate the selected Private VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#shutdown
DmSwitch(config-if-pvlan-1000)#
```

To verify the Private VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

Chapter 27. Community VLAN Commands

mac-address-table learn

mac-address-table learn

no mac-address-table learn

Description

Enables MAC address learning on the selected Community VLAN.

Inserting **no** as a prefix for this command will disable VLAN MAC address learning.

Syntax

No parameter accepted.

Default

VLAN MAC address learning is enabled for all Community VLANs.

Command Modes

Community VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command can enable or disable learning of MAC addresses in the selected Community VLAN.

Example

This example shows how to enable the VLAN MAC address learning for a specific Community VLAN interface.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#community-vlan 2000
DmSwitch(config-if-pvlan-1000-community-2000)#mac-address-table learn
DmSwitch(config-if-pvlan-1000-community-2000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
clear mac-address-table	Erases entries stored in the MAC address table.
community-vlan	Enables the community VLAN configuration mode.
show mac-address-table	Shows the MAC address table.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

name

name *name*

no name

Description

Specifies the Community VLAN name.

Inserting **no** as a prefix for this command will remove the Community VLAN name.

Syntax

Parameter	Description
<i>name</i>	Specifies a Community VLAN name.

Default

No default is defined.

Command Modes

Community VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a Community VLAN name.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#community-vlan 2000
DmSwitch(config-if-pvlan-1000-community-2000)#name VlanTest
DmSwitch(config-if-pvlan-1000-community-2000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>community-vlan</code>	Enables the community VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

set-member

```
set-member {tagged|untagged} { ethernet { all | [ unit-number/ ] port-number | range  
{ [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member {tagged|untagged} { port-channel channel-group-number }
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ]  
first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ]
```

Description

Adds members to selected Community VLAN.

Entering with **no** command, it removes members from selected Community VLAN.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Adds a range of specific units and ports.
port-channel channel-group-number	Adds a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available

Example

This example shows how to add an ethernet port range with tagged members to a Community VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#community-vlan 2000
DmSwitch(config-if-pvlan-1000-community-2000)#set-member tagged ethernet range 1/25 1/28
DmSwitch(config-if-pvlan-1000-community-2000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

shutdown

shutdown

no shutdown

Description

Deactivates the selected Community VLAN.

Inserting **no** as a prefix for this command will reactivate the selected Community VLAN.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Community VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available

Example

This example shows how to deactivate the selected Community VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#community-vlan 2000
DmSwitch(config-if-pvlan-1000-community-2000)#shutdown
DmSwitch(config-if-pvlan-1000-community-2000)#
```

To verify the Community VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>community-vlan</code>	Enables the community VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

Chapter 28. Isolated VLAN Commands

mac-address-table learn

mac-address-table learn

no mac-address-table learn

Description

Enables MAC address learning on the selected Isolated VLAN.

Inserting **no** as a prefix for this command will disable VLAN MAC address learning.

Syntax

No parameter accepted.

Default

VLAN MAC address learning is enabled for all Isolated VLANs.

Command Modes

Isolated VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

This command can enable or disable learning of MAC addresses in the selected Isolated VLAN.

Example

This example shows how to enable the VLAN MAC address learning for a specific Isolated VLAN interface.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#isolated-vlan 2000
DmSwitch(config-if-pvlan-1000-isolated-2000)#mac-address-table learn
DmSwitch(config-if-pvlan-1000-isolated-2000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
clear mac-address-table	Erases entries stored in the MAC address table.
isolated-vlan	Enables the isolated VLAN configuration mode.
show mac-address-table	Shows the MAC address table.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

name

name *name*

no name

Description

Specifies the Isolated VLAN name.

Inserting **no** as a prefix for this command will remove the Isolated VLAN name.

Syntax

Parameter	Description
<i>name</i>	Specifies the Isolated VLAN name.

Default

No default is defined.

Command Modes

Isolated VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify an Isolated VLAN name.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#isolated-vlan 2000
DmSwitch(config-if-pvlan-1000-isolated-2000)#name VlanTest
DmSwitch(config-if-pvlan-1000-isolated-2000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>isolated-vlan</code>	Enables the isolated VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

set-member

```
set-member {tagged|untagged} { ethernet { all | [ unit-number/ ] port-number | range  
{ [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member {tagged|untagged} { port-channel channel-group-number }
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ]  
first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ]
```

Description

Adds members to selected Isolated VLAN.

Entering with **no** command, it removes members from selected Isolated VLAN.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Adds a range of specific units and ports.
port-channel channel-group-number	Adds a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Private VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available

Example

This example shows how to add an ethernet port range with tagged members to an Isolated VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#isolated-vlan 2000
DmSwitch(config-if-pvlan-1000-isolated-2000)#set-member tagged ethernet range 1/25 1/28
DmSwitch(config-if-pvlan-1000-isolated-2000)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

shutdown

shutdown

no shutdown

Description

Deactivates the selected Isolated VLAN.

Inserting **no** as a prefix for this command will reactivate the selected Isolated VLAN.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Isolated VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available

Example

This example shows how to deactivate the selected Isolated VLAN.

```
DmSwitch(config)#interface private-vlan 1000
DmSwitch(config-if-pvlan-1000)#isolated-vlan 2000
DmSwitch(config-if-pvlan-1000-isolated-2000)#shutdown
DmSwitch(config-if-pvlan-1000-isolated-2000)#
```

To verify the Isolated VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>isolated-vlan</code>	Enables the isolated VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

Chapter 29. Interface VLAN Commands

bfd interval

bfd interval *interval* **minrx** *minrx* **multiplier** *multiplier*

no bfd interval

Description

Configures BFD interval parameters on a VLAN.

The **no** command resets the parameters to their default values.

Syntax

Parameter	Description
<i>interval</i>	Specifies the minimum desired interval to transmit BFD packets (in milliseconds). The ranges for the equipments DM4001, DM4004 and DM4008 are from 300 through 1000 and for DM4100 is 1000.
<i>minrx</i>	Specifies the minimum required interval to transmit BFD packets (in milliseconds). The ranges for the equipments DM4001, DM4004 and DM4008 are from 300 through 1000 and for DM4100 is 1000.
<i>multiplier</i>	Specifies the number of BFD packets from a peer that can be missed before reporting a failure. Range: 3-100

Default for equipments:

. DM4001, DM4004 and DM4008: Interval: 500 milliseconds. Minrx: 500 milliseconds. Multiplier: 3.

. DM4100: Interval and Minrx: 1000 milliseconds. Multiplier: 3.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

Defines the minimum transmit and receive intervals of BFD packets, as well as the number of packets from a peer that can be missed before reporting a failure. Note that the actual transmit interval and failure detection time for a given BFD session is calculated based on the interval parameters of both peers that are part of the session. This configuration causes OSPF sessions using BFD on this VLAN to be reset. Similarly, static routes using BFD and whose output interfaces are on this VLAN, will flap momentarily.

Example

This example shows how to configure the BFD interval parameters on a VLAN.

```
DmSwitch(config-if-vlan-1)#bfd interval 400 minrx 400 multiplier 3
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip bfd neighbors	Show the state of all BFD IPv4 sessions.

gratuitous-arp-handling

gratuitous-arp-handling

no gratuitous-arp-handling

Description

Enables Gratuitous ARP (Request/Reply) handling on selected VLAN.

Inserting **no** as a prefix for this command will disable Gratuitous ARP handling on selected VLAN.

Syntax

No parameter accepted.

Default

Enabled.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command defines if the received Gratuitous ARP frame, whose IP is not already present in the ARP table, will create a new entry in the ARP table or not. If enabled, both Gratuitous ARP of type Reply and Request will be processed. If the IP address of Gratuitous ARP is already installed in the ARP table, this will be updated regardless if gratuitous-arp-handling is set or not.

Example

This example shows how to deactivate Gratuitous ARP handling on the selected VLAN.

```
DmSwitch(config-if-vlan-2)#no gratuitous-arp-handling
DmSwitch(config-if-vlan-2)#
```

You can verify that the Gratuitous ARP handling is enabled/disabled by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

ip address

```
ip address { ip-address/mask [ secondary ] | dhcp [ release ] }
```

```
no ip address [ ip-address/mask secondary | dhcp ]
```

Description

Sets an IP address for the selected VLAN.

Inserting **no** as a prefix for this command will delete the IP address from the selected VLAN.

Can't enable DHCP Client service in VLAN while any of the static network configurations - ip address, default-gateway, dns-server and domain-name - or DHCP Client for IPv6 are enabled.

Syntax

Parameter	Description
<i>ip-address/mask</i>	Specifies the IP address and network mask to the selected VLAN.
dhcp	Gets an IP address from DHCP server to the selected VLAN (provided only for the default VLAN).
release	(Optional) Releases the IP address leased from DHCP server to the selected VLAN.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.4	Option renew was removed.

Usage Guidelines

The DHCP Client service will get a network configuration lease, that includes IP/mask, DNS servers, default gateway and domain name.

Example

This example shows how to specify a static IP address to the VLAN 1.

```
DmSwitch(config-if-vlan-1)#ip address 10.10.10.15/24
DmSwitch(config-if-vlan-1)#
```

You can verify that the IP address was specified by entering the **show ip** privileged EXEC command.

Related Commands

Command	Description
ip default-gateway	Configures the default gateway for DmSwitch.
ip dns-server	Configures the DNS servers used by DmSwitch
ip domain-name	Configures the domain name for DmSwitch.
show ip	Shows the IP configuration.
show running-config	Shows the current operating configuration.

ip arp-protection

```
ip arp-protection action { block | override }
```

```
no ip arp-protection action { block | override }
```

Description

Sets ARP protection for the selected VLAN by overriding forged ARP packets with the trusted MAC addresses or Blocking it.

This command protects all ARP static entries or locally assigned addresses.

Inserting **no** as a prefix for this command will remove the ARP protection from the selected VLAN.

Syntax

Parameter	Description
block	Block ARP packets with untrusted addresses for ports in VLAN.
override	Override ARP packets with trusted addresses for ports in VLAN.

Default

Command is disabled by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.0	This command was introduced.
13.4	Added new parameter block .

Usage Guidelines

Not available.

Example

This example shows how to add ARP protection override to VLAN 100.

```
DmSwitch(config-if-vlan-100)#ip arp-protection action override
DmSwitch(config-if-vlan-100)#
```

You can verify that an ARP antidote is sent by the switch when a forged ARP packet is detected.

Related Commands

Command	Description
arp static	Adds a static entry to the ARP table.
show running-config	Shows the current operating configuration.
ip arp-protection eth	Configures port as trusted for ARP Protection.

ip dhcp relay

`ip dhcp relay`

`no ip dhcp relay`

Description

Enables DHCP relay on the selected vlan.

Inserting **no** as a prefix for this command will disable DHCP relay on vlan.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate DHCP relay on VLAN 2.

```
DmSwitch(config-int-vlan-2)#ip dhcp relay
DmSwitch(config-int-vlan-2)#
```

You can verify that the DHCP relay was enabled by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>ip dhcp relay</code>	Enables DHCP relay globally.
<code>ip dhcp relay information option</code>	Enables DHCP Agent Information Option (option 82).
<code>ip dhcp relay information trusted</code>	Mark a Vlan as a trusted interface.
<code>ip helper-address</code>	Add an address to the list of DHCP servers global.
<code>ip helper-address</code>	Add an address to the VLAN list of DHCP servers in VLAN.
<code>show ip dhcp relay</code>	Shows the DHCP relay settings.

ip dhcp relay information trusted

```
ip dhcp relay information trusted
```

```
no ip dhcp relay information trusted
```

Description

Mark a Vlan as a trusted interface. If a packet is received with the option 82 field set, and a giaddr field not set, the packet is discarded, unless the incoming packet came from a trusted interface.

Inserting **no** as a prefix for this command will mark the selected vlan as untrusted.

Default

All untrusted.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to mark Vlan 2 as a trusted interface.

```
DmSwitch(config-if-vlan-2)#ip dhcp relay information trusted
DmSwitch(config-if-vlan-2)#
```

You can verify that the Vlan is marked as trusted by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
ip dhcp relay	Enables DHCP relay globally.
ip dhcp relay	Enables DHCP relay on the selected Vlan.

Command	Description
ip dhcp relay information option	Enables DHCP Agent Information Option (option 82).
ip helper-address	Add an address to the list of DHCP servers global.
ip helper-address	Add an address to the VLAN list of DHCP servers in VLAN.
show ip dhcp relay	Shows the DHCP relay settings.

ipv6 dhcp relay

`ipv6 dhcp relay`

`no ipv6 dhcp relay`

Description

It enables the DHCPv6 relay agent on a VLAN.

Inserting **no** as a prefix for this command will disable DHCPv6 relay agent.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

The global DHCPv6 relay must be enabled to the VLAN relay agent works appropriately.

Example

This example shows how to activate DHCPv6 relay agent at VLAN 100.

```
DmSwitch(config)#interface vlan 100
DmSwitch(config-if-vlan-100)#
DmSwitch(config-if-vlan-100)#ipv6 dhcp relay
DmSwitch(config-if-vlan-100)#
```

You can verify that the DHCPv6 relay agent was enabled by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
ipv6 dhcp relay	It enables the global DHCPv6 relay.
ipv6 helper-address	It adds unicast or multicast IPv6 address into the list of DHCPv6 servers global.
ipv6 dhcp relay	It enables the DHCPv6 relay agent on a VLAN.
show ipv6 dhcp relay	It shows the details about DHCPv6 relay configurations.

ip helper-address

ip helper-address *ip-address*

no ip helper-address *ip-address*

Description

Add an address to the VLAN list of DHCP servers.

Inserting **no** as a prefix for this command will erase the address from the list.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the IP address to the list of DHCP servers

Default

Disabled.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add the address 192.168.0.254 to the DHCP relay servers list to the VLAN 1.

```
DmSwitch(config-if-vlan-1)#ip helper-address 192.168.0.254
DmSwitch(config-if-vlan-1)#
```

You can verify that the address was added to the list by entering the **show ip dhcp relay** privileged EXEC command.

Related Commands

Command	Description
<code>ip dhcp relay</code>	Enables DHCP relay globally.
<code>ip dhcp relay</code>	Enables DHCP relay on the selected Vlan.
<code>ip dhcp relay information option</code>	Enables DHCP Agent Information Option (option 82).
<code>ip dhcp relay information trusted</code>	Mark a Vlan as a trusted interface.
<code>ip helper-address</code>	Add an address to the list of DHCP servers global.
<code>show ip dhcp relay</code>	Shows the DHCP relay settings.

ipv6 enable

ipv6 enable

no ipv6 enable

Description

Enable IPv6 support for the selected VLAN and assign a Link-Local address.

Inserting **no** as a prefix for this command will disable IPv6 support for the selected VLAN.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable IPv6 in VLAN 1.

```
DmSwitch(config-if-vlan-1)#ipv6 enable
DmSwitch(config-if-vlan-1)#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

ipv6 address

```
ipv6 address { ipv6address/prefix-length | ipv6prefix/prefix-length eui-64 | dhcp [ release ] }
```

```
no ipv6 address { ipv6address/prefix-length | ipv6prefix/prefix-length | dhcp }
```

Description

Sets an IPv6 address for the selected VLAN.

Inserting **no** as a prefix for this command will delete the IPv6 address from the selected VLAN.

Using the *ipv6prefix/prefix-length***eui-64** form causes the switch to use interface physical address to compose the IPv6 address in EUI-64 format.

Can't enable DHCP Client service in VLAN while any of the static network configurations - ip address, dns-server and domain-name - or DHCP Client for IPv4 are enabled.

Syntax

Parameter	Description
<i>ipv6address/prefix-length</i>	Specifies the IPv6 address and prefix-length to the selected VLAN.
<i>ipv6prefix/prefix-length</i> eui-64	Specifies the IPv6 prefix and prefix-length to be used to compose the IPv6 address in EUI-64 format.
dhcp	Gets an IP address from DHCP server to the selected VLAN (provided only for the default VLAN).
release	(Optional) Releases the IP address leased from DHCP server to the selected VLAN.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.
13.4	IPv6 DHCP Client was introduced.

Usage Guidelines

The DHCP Client service will get a network configuration lease, that includes IP/mask, DNS servers and domain name. In order to enable the DHCP Client, is needed that the IPv6 is enabled (**ipv6 enable**) for the given interface.

Example

This example shows how to specify a static IPv6 address to the VLAN 1.

```
DmSwitch(config-if-vlan-1)#ipv6 address 2001:DB8::1/64
DmSwitch(config-if-vlan-1)#
```

You can verify that the IPv6 address was specified by entering the **show ipv6 interface** privileged EXEC command.

Related Commands

Command	Description
ip dns-server	Configures the DNS servers used by DmSwitch
ip domain-name	Configures the domain name for DmSwitch.
show running-config	Shows the current operating configuration.
show ipv6 interface	Shows IPv6 interface information.

ip dhcp snooping

`ip dhcp snooping`

`no ip dhcp snooping`

Description

Enables DHCP snooping on a VLAN.

Inserting **no** as a prefix for this command will disable DHCP Snooping at VLAN.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

DHCP snooping must be globally enabled to take effect on enabling DHCP snooping on a VLAN.

Example

This example shows how to activate DHCP Snooping at VLAN.

```
DmSwitch(config)#interface vlan 1000
DmSwitch(config-if-vlan-1000)#ip dhcp snooping
DmSwitch(config)#
```

You can verify that the DHCP Snooping at VLAN was enabled by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>ip dhcp snooping</code>	Enables DHCP Snooping globally.
<code>ip dhcp snooping verify mac-address</code>	Enables configuration to verify mac-address on a DHCP Snooping message.
<code>ip dhcp snooping trust</code>	Configures port as trusted for DHCP Snooping.

ip directed-broadcast

```
ip directed-broadcast [ source-address ip address ]
```

```
no ip directed-broadcast
```

Description

Configures IP Directed Broadcast forwarding for the selected VLAN.

Inserting **no** as a prefix for this command will disable the IP Directed Broadcast forwarding for the selected VLAN.

Syntax

Parameter	Description
<i>source-address</i>	(Optional) Allow IP Directed Broadcast forwarding only for packets originated from a specific IP address. Packets not originated from <i>source-address</i> IP address will be discarded.

Default

IP Directed Broadcast is disabled by default

Command Modes

VLAN configuration.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

IP Directed Broadcast command applies for all IP addresses configured in VLAN. This feature can be enabled for at most 384 IP addresses configured in the equipment. The feature is not available for DM4100 equipments.

Example

This example shows how to enable IP Directed Broadcast forwarding for VLAN 2.

```
DmSwitch(config-if-vlan-2)#ip directed-broadcast
DmSwitch(config-if-vlan-2)#
```

This example shows how to enable IP Directed Broadcast forwarding with source address parameter for VLAN 2

```
DmSwitch(config-if-vlan-2)#ip directed-broadcast source-address 192.168.0.1
DmSwitch(config-if-vlan-2)#
```

This example shows how to disable IP Directed Broadcast for VLAN 2.

```
DmSwitch(config-if-vlan-2)#no directed-broadcast
DmSwitch(config-if-vlan-2)#
```

You can verify that IP Directed Broadcast is configured on a VLAN interface by entering the **show vlan id** privileged EXEC command.

Related Commands

Command	Description
show vlan	Shows the Virtual LAN settings.
show running-config	Shows the current operating configuration.

ip local-proxy-arp

```
ip local-proxy-arp
```

```
no ip local-proxy-arp
```

Description

Sets Local Proxy ARP for selected VLAN.

Inserting **no** as a prefix for this command will disable Local Proxy ARP for the selected VLAN.

Syntax

No parameter accepted.

Default

Command is disabled by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable Local Proxy ARP on the selected VLAN.

```
DmSwitch(config-if-vlan-2)#ip local-proxy-arp
DmSwitch(config-if-vlan-2)#
```

You can verify that the Local Proxy ARP was enabled by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

Command	Description
<code>ip proxy-arp</code>	Enables proxy ARP on selected VLAN.

ip ospf authentication

```
ip ospf authentication [ message-digest | null ]
```

```
no ip ospf authentication
```

Description

Configures authentication on a VLAN.

The **no** command disables authentication on the VLAN.

Syntax

Parameter	Description
message-digest	(Optional) Uses message-digest authentication.
null	(Optional) Does not use authentication.

Default

No authentication is enabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure authentication in OSPF packets on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf authentication
```



```
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf authentication	Configures authentication on a VLAN.
ip ospf message-digest-key	Configures message digest key on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf authentication-key

ip ospf authentication-key *key*

no ip ospf authentication-key

Description

Configures authentication key on a VLAN.

The **no** command removes the authentication key configured on the VLAN.

Syntax

Parameter	Description
<i>key</i>	Specifies the authentication key (OSPF password).

Default

No authentication key is configured.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Defines a password to be used by neighboring OSPF routers on a network segment that is using OSPF simple password authentication.

Example

This example shows how to configure the authentication key on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf authentication-key key_test
```

```
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf authentication	Configures authentication on a VLAN.
ip ospf message-digest-key	Configures message digest key on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf bfd

```
ip ospf bfd
```

```
no ip ospf bfd
```

Description

Configures BFD support for OSPF on a VLAN.

The **no** command resets the parameters to their default values.

Syntax

No parameter accepted.

Default

BFD support for OSPF is disabled by default.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

This command enables or disables BFD support for OSPF adjacencies that are established on this VLAN.

Example

This example shows how to configure BFD support for OSPF on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf bfd
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>bfd interval</code>	Configure BFD interval parameters on a VLAN.
<code>show ip bfd neighbors</code>	Show the state of all BFD IPv4 sessions.

ip ospf cost

`ip ospf cost value`

`no ip ospf cost`

Description

Configures the cost of sending a packet on an OSPF interface.

The **no** command resets the cost to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the cost value. (Range: 1-65535)

Default

Cost: 10.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the cost on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf cost 5
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf dead-interval

```
ip ospf dead-interval value
```

```
no ip ospf dead-interval
```

Description

Configures dead router detection time on a VLAN.

The **no** command resets the dead interval to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the dead interval (in seconds). (Range: 1-65535)

Default

Dead interval: 40 seconds.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Defines the number of seconds that a device's hello packets must not have been seen before its neighbors declare the OSPF router down.

Example

This example shows how to configure the dead router detection time on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf dead-interval 20
```



```
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf hello-interval	Configures the hello packet interval on a VLAN.
ip ospf retransmit-interval	Configures the link state retransmit interval on a VLAN.
ip ospf transmit-delay	Configures the link state transmit delay on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf hello-interval

```
ip ospf hello-interval value
```

```
no ip ospf hello-interval
```

Description

Configures the hello packet interval on a VLAN.

The **no** command resets the hello interval to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the hello interval value. (Range: 1-65535)

Default

Hello interval: 10 seconds.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Defines the time between the hello packets that the DmSwitch sends on an OSPF interface.

Example

This example shows how to configure the hello packet interval on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf hello-interval 20
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf dead-interval	Configures dead router detection time on a VLAN.
ip ospf retransmit-interval	Configures the link state retransmit interval on a VLAN.
ip ospf transmit-delay	Configures the link state transmit delay on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf message-digest-key

```
ip ospf message-digest-key key-id md5 key-text
```

```
no ip ospf message-digest-key key-id
```

Description

Configures message digest key on a VLAN.

The **no** command removes the specified message digest key configured on the VLAN.

Syntax

Parameter	Description
<i>key-id</i>	Specifies the key ID. (Range: 1-255)
md5	Uses the MD5 algorithm.
<i>key-text</i>	Specifies the key string (OSPF password).

Default

No message digest key is configured.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a message digest key on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf message-digest-key 1 md5 test_key
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf authentication	Configures authentication on a VLAN.
ip ospf authentication-key	Configures authentication key on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf mtu-ignore

```
ip ospf mtu-ignore
```

```
no ip ospf mtu-ignore
```

Description

Disables MTU checking on this interface.

The **no** command disables the mtu-ignore option.

Syntax

No parameter accepted.

Default

MTU checking is enabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

MTU check should be disabled in case there are OSPF neighbors that have to use different MTU sizes.

Example

This example shows how to disable the MTU checking on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf mtu-ignore
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip ospf</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.

ip ospf network

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint |  
point-to-point }
```

```
no ip ospf network
```

Description

Configures the OSPF network type.

The **no** command resets the network to its default type.

Syntax

Parameter	Description
broadcast	Specifies OSPF broadcast multi-access networks.
non-broadcast	Specifies OSPF NBMA networks.
point-to-multipoint	Specifies OSPF point-to-multipoint networks.
point-to-point	Specifies OSPF point-to-point networks.

Default

Network: broadcast.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes.

Example

This example shows how to configure the OSPF network type for a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf network point-to-multipoint
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf priority

```
ip ospf priority value
```

```
no ip ospf priority
```

Description

Configures the priority for a network.

The **no** command resets the priority to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the priority value. (Range: 0-255)

Default

Priority: 1.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Defines the priority to help determine the OSPF designated router for a network.

Example

This example shows how to configure the priority on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf priority 10
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf retransmit-interval

```
ip ospf retransmit-interval value
```

```
no ip ospf retransmit-interval
```

Description

Configures the link state retransmit interval on a VLAN.

The **no** command resets the retransmit interval to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the retransmit interval (in seconds). (Range: 3-65535)

Default

Retransmit interval: 5 seconds.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Defines the number of seconds between LSA (link state advertisement) retransmissions for adjacencies belonging to an OSPF interface.

Example

This example shows how to configure the link state retransmit interval on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf retransmit-interval 8
```

```
DmSwitch(config-if-vlan-1) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf dead-interval	Configures dead router detection time on a VLAN.
ip ospf hello-interval	Configures the hello packet interval on a VLAN.
ip ospf transmit-delay	Configures the link state transmit delay on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ip ospf transmit-delay

```
ip ospf transmit-delay value
```

```
no ip ospf transmit-delay
```

Description

Configures the link state transmit delay on a VLAN.

The **no** command resets the transmit delay to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the transmit delay (in seconds). (Range: 1-65535)

Default

Transmit delay: 1 second.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Defines the estimated number of seconds it takes to transmit a link state update packet on an OSPF interface.

Example

This example shows how to configure the link state transmit delay on a VLAN.

```
DmSwitch(config-if-vlan-1)#ip ospf transmit-delay 2
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip ospf dead-interval	Configures dead router detection time on a VLAN.
ip ospf hello-interval	Configures the hello packet interval on a VLAN.
ip ospf retransmit-interval	Configures the link state retransmit interval on a VLAN.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ipv6 nd ra

```
ipv6 nd ra { max-interval seconds | min-interval seconds |  
prefix-adv-autonomous | prefix-adv-onlink }
```

```
no ipv6 nd ra { max-interval | min-interval | prefix-adv-autonomous |  
prefix-adv-onlink }
```

Description

This command configures Router Advertisement parameters for IPv6 on a VLAN interface.

The **no** command for the parameters **prefix-adv-autonomous** and **prefix-adv-onlink** turns off the flag(s) in the prefix information. The **no** command for parameters **max-interval** and **min-interval** will set the Router Advertisement interval (maximum or minimum) to its default value.

Syntax

Parameter	Description
max-interval <i>seconds</i>	The maximum time allowed between sending unsolicited multicast Router Advertisements from the interface. Range: 4-1800.
min-interval <i>seconds</i>	The minimum time allowed between sending unsolicited multicast Router Advertisements from the interface. Range: 3-1350.
prefix-adv-autonomous	Indicates that this prefix can be used for autonomous address configuration as specified in RFC 4862.
prefix-adv-onlink	Indicates that this prefix can be used for on-link determination. A prefix is on-link if the host with this prefix is accessible by the interface that received the advertisement.

Default

By default, Router Advertisement for IPv6 is not enabled. When it is enabled, the default value for max-interval parameter is 30 seconds and the default value for the min-interval parameter is 10 seconds. The flags prefix-adv-autonomous and prefix-adv-onlink are set to ON by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

IPv6 address must be configured at VLAN interface before setting prefix parameter (prefix-adv-autonomous or prefix-adv-onlink). The Router Advertisement interval parameters follow a specific rule: the maximum interval value must be no less than 4 seconds and no greater than 1800 seconds and the minimum time must be no less than 3 seconds and no greater than $0.75 * \text{max-interval}$.

Example

This example shows how to configure the Router Advertisement parameters on a VLAN interface.

```
DmSwitch(config-if-vlan-420)#ipv6 nd ra max-interval 1800
DmSwitch(config-if-vlan-420)#ipv6 nd ra min-interval 1350
DmSwitch(config-if-vlan-420)#ipv6 enable
DmSwitch(config-if-vlan-420)#ipv6 address 2001:db8::2/128
DmSwitch(config-if-vlan-420)#ipv6 nd ra prefix-adv-autonomous
DmSwitch(config-if-vlan-420)#ipv6 nd ra prefix-adv-onlink
DmSwitch(config-if-vlan-420)#
```

You can verify if the Router Advertisement parameters are configured on a VLAN interface by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ipv6 nd ra	Enables Router Advertisement protocol.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 authentication

```
ipv6 ospfv3 authentication message-digest { key } spi { value }
```

```
no ipv6 ospfv3 authentication message-digest
```

Description

Configures MD5 authentication for OSPFv3 packets on a VLAN.

The **no** command disables authentication on the VLAN.

Syntax

Parameter	Description
<i>key</i>	Message-digest authentication key password.
<i>value</i>	Security Parameter Index value.

Default

No authentication is enabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

To configure authentication using two switches the "key" and "spi value" must be the same in both neighbors, but each vlan in the same switch must have a unique SPI value.

Example

This example shows how to configure authentication in OSPFv3 packets on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 authentication message-digest
0123456789efabcdefabcdef14673fab spi 15000
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 bfd

```
ipv6 ospfv3 bfd
```

```
no ipv6 ospfv3 bfd
```

Description

Configures BFD support for OSPFv3 on a VLAN.

The **no** command resets the parameters to their default values.

Syntax

No parameter accepted.

Default

BFD support for OSPFv3 is disabled by default.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

This command enables or disables BFD support for OSPFv3 adjacencies that are established on this VLAN.

Example

This example shows how to configure BFD support for OSPFv3 on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 bfd
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>bfd interval</code>	Configure BFD interval parameters on a VLAN.
<code>show ipv6 bfd neighbors</code>	Shows the state of all BFD IPv6 sessions.

ipv6 ospfv3 cost

`ipv6 ospfv3 cost value`

`no ipv6 ospfv3 cost`

Description

Configures the cost of sending a packet on an OSPFv3 interface.

The **no** command resets the cost to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the cost value. (Range: 1-65535)

Default

Cost: 10.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the cost on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 cost 5
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 dead-interval

```
ipv6 ospfv3 dead-interval value
```

```
no ipv6 ospfv3 dead-interval
```

Description

Configures dead router detection time on a VLAN.

The **no** command resets the dead interval to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the dead interval (in seconds). (Range: 1-65535)

Default

Dead interval: 40 seconds.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Defines the number of seconds that a device's hello packets must not have been seen before its neighbors declare the OSPFv3 router down.

Example

This example shows how to configure the dead router detection time on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 dead-interval 20
```



```
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ipv6 ospfv3 hello-interval	Configures the hello packet interval on a VLAN.
ipv6 ospfv3 retransmit-interval	Configures the link state retransmit interval on a VLAN.
ipv6 ospfv3 transmit-delay	Configures the link state transmit delay on a VLAN.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 hello-interval

```
ipv6 ospfv3 hello-interval value
```

```
no ipv6 ospfv3 hello-interval
```

Description

Configures the hello packet interval on a VLAN.

The **no** command resets the hello interval to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the hello interval value. (Range: 1-65535)

Default

Hello interval: 10 seconds.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Defines the time between the hello packets that the DmSwitch sends on an OSPFv3 interface.

Example

This example shows how to configure the hello packet interval on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 hello-interval 20
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ipv6 ospfv3 dead-interval	Configures dead router detection time on a VLAN.
ipv6 ospfv3 retransmit-interval	Configures the link state retransmit interval on a VLAN.
ipv6 ospfv3 transmit-delay	Configures the link state transmit delay on a VLAN.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 instance-id

```
ipv6 ospfv3 instance-id instance-id area { area-id | ipv4-address_id }
```

```
no ipv6 ospfv3 instance-id instance-id
```

Description

Enables OSPFv3 routing on an instance-id.

The **no** command disables OSPFv3 routing on the specified instance-id.

Syntax

Parameter	Description
<i>instance-id</i>	Specifies the OSPFv3 instance-id. (Range: 0-255)
area	OSPFv3 area ID.
<i>area-id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ipv4-address_id</i>	Specifies the OSPF area ID in IPv4 address format.

Default

No instance-id is configured.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The OSPFv3 process will act only over the specified interface.

Example

This example shows how to specify a instance-id with the OSPFv3 routing.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 instance-id 0 area 0
DmSwitch(config-if-vlan-1)#
```

You can verify that the instance-id was associated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 mtu-ignore

```
ipv6 ospfv3 mtu-ignore
```

```
no ipv6 ospfv3 mtu-ignore
```

Description

Disables MTU checking on this interface.

The **no** command disables the mtu-ignore option.

Syntax

No parameter accepted.

Default

MTU checking is enabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

MTU check should be disabled in case there are OSPFv3 neighbors that have to use different MTU sizes.

Example

This example shows how to disable the MTU checking on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 mtu-ignore
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ipv6 ospfv3</code>	Shows the OSPFv3 process parameters.
<code>show running-config</code>	Shows the current operating configuration.

ipv6 ospfv3 neighbor

```
ipv6 ospfv3 neighbor ipv6-address [ priority priority-value ]
```

```
no ipv6 ospfv3 neighbor ipv6-address
```

Description

Defines a static neighbor router.

Entering with **no** command, it removes a configured neighbor router.

Syntax

Parameter	Description
<i>ipv6-address</i>	Specifies the neighbor IPv6 address.
priority <i>priority-value</i>	(Optional) Specifies the priority of non-broadcast neighbor. (Range: 0-255)

Default

No neighbor is configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command configures static neighbors routers attached to the interface.

A neighbor with priority 0 is considered ineligible for DR (Designated Router) election.

Example

This example shows how to define a neighbor router IPv6 address.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 neighbor 2000::203  
DmSwitch(config-if-vlan-1)#
```


You can verify that the neighbor was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ipv6 ospfv3 instance-id	Associates a instance-id with a OSPFv3 routing process.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.

ipv6 ospfv3 network

```
ipv6 ospfv3 network { broadcast | non-broadcast | point-to-multipoint |  
point-to-point }
```

```
no ipv6 ospfv3 network
```

Description

Configures the OSPFv3 network type.

The **no** command resets the network to its default type.

Syntax

Parameter	Description
broadcast	Specifies OSPFv3 broadcast multi-access networks.
non-broadcast	Specifies OSPFv3 NBMA networks.
point-to-multipoint	Specifies OSPFv3 point-to-multipoint networks.
point-to-point	Specifies OSPFv3 point-to-point networks.

Default

Network: broadcast.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

An OSPFv3 point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes.

Example

This example shows how to configure the OSPFv3 network type for a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 network point-to-multipoint
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 priority

ipv6 ospfv3 priority *value*

no ipv6 ospfv3 priority

Description

Configures the priority for a interface.

The **no** command resets the priority to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the priority value. (Range: 0-255)

Default

Priority: 1.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Defines the priority to help determine the OSPFv3 designated router for a interface.

Example

This example shows how to configure the priority on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 priority 10
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 retransmit-interval

```
ipv6 ospfv3 retransmit-interval value
```

```
no ipv6 ospfv3 retransmit-interval
```

Description

Configures the link state retransmit interval on a VLAN.

The **no** command resets the retransmit interval to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the retransmit interval (in seconds). (Range: 1-1800)

Default

Retransmit interval: 5 seconds.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Defines the number of seconds between LSA (link state advertisement) retransmissions for adjacencies belonging to an OSPFv3 interface.

Example

This example shows how to configure the link state retransmit interval on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 retransmit-interval 8
```

```
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ipv6 ospfv3 dead-interval	Configures dead router detection time on a VLAN.
ipv6 ospfv3 hello-interval	Configures the hello packet interval on a VLAN.
ipv6 ospfv3 transmit-delay	Configures the link state transmit delay on a VLAN.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ipv6 ospfv3 transmit-delay

```
ipv6 ospfv3 transmit-delay value
```

```
no ipv6 ospfv3 transmit-delay
```

Description

Configures the link state transmit delay on a VLAN.

The **no** command resets the transmit delay to its default value.

Syntax

Parameter	Description
<i>value</i>	Specifies the transmit delay (in seconds). (Range: 1-1800)

Default

Transmit delay: 1 second.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Defines the estimated number of seconds it takes to transmit a link state update packet on an OSPFv3 interface.

Example

This example shows how to configure the link state transmit delay on a VLAN.

```
DmSwitch(config-if-vlan-1)#ipv6 ospfv3 transmit-delay 2
DmSwitch(config-if-vlan-1)#
```


You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ipv6 ospfv3 dead-interval	Configures dead router detection time on a VLAN.
ipv6 ospfv3 hello-interval	Configures the hello packet interval on a VLAN.
ipv6 ospfv3 retransmit-interval	Configures the link state retransmit interval on a VLAN.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

ip igmp snooping flood-unknown

```
ip igmp snooping flood-unknown
```

```
no ip igmp snooping flood-unknown
```

Description

Configures the flood type traffic to VLAN.

The **no** command resets the parameters to their default values.

Syntax

No parameter accepted.

Default

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
14.10.2	This command was changed from global scope to vlan scope.

Usage Guidelines

This command enables or disables igmp flood-unknown on this VLAN.

Example

This example shows how to configure on a VLAN.

```
DmSwitch(config-if-vlan-12)#no ip igmp snooping flood-unknown
DmSwitch(config-if-vlan-12)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>ip pim</code>	Enables global PIM protocol.
<code>ip igmp</code>	Configures the IGMP snooping.

ip pim

```
ip pim [ dr-priority priority | hello-period seconds ]
```

```
no ip pim [ dr-priority | hello-period ]
```

Description

This command enables PIM (Protocol Independent Multicast) on a VLAN interface.

The **no** command removes the PIM configuration on a VLAN interface. Additionally with the **no** command, if **dr-priority** is given on the end of the string, the dr-priority is set to its default value. The same happens with **hello-period**.

Syntax

Parameter	Description
dr-priority <i>priority</i>	Change priority for DR (Designated Router) election. Range: 0-65535.
hello-period <i>seconds</i>	Hello period in seconds. Range: 1-104.

Default

By default, PIM is not enabled on a VLAN interface. When it is enabled, the default value for dr-priority is 1, and for hello-period is 30.

Command Modes

VLAN configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command enables PIM Multicast Routing Protocol on a VLAN interface. If all routers on the interface use the DR Priority option in their PIM Hello messages, the router with the highest value for DR priority will win the DR election. In case the values are the same, highest IP address will be used as a tie-breaker.

Example

This example shows how to configure PIM on a VLAN interface.

```
DmSwitch(config-if-vlan-420)#ip pim
DmSwitch(config-if-vlan-420)#
```

You can verify the PIM configured on a VLAN interface by entering the **show running-config**, **show ip pim config** or the **show ip pim interfaces** privileged EXEC command.

Related Commands

Command	Description
show ip pim interfaces	Shows PIM interfaces parameters.
show ip pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ipv6 pim

```
ipv6 pim [ dr-priority priority | hello-period seconds ]
```

```
no ipv6 pim [ dr-priority | hello-period ]
```

Description

This command enables PIM (Protocol Independent Multicast) for IPv6 on a VLAN interface.

The **no** command removes the IPv6 PIM configuration on a VLAN interface. Additionally with the **no** command, if **dr-priority** is given on the end of the string, the dr-priority is set to its default value. The same happens with **hello-period**.

Syntax

Parameter	Description
dr-priority <i>priority</i>	Change priority for DR (Designated Router) election. Range: 0-65535.
hello-period <i>seconds</i>	Hello period in seconds. Range: 1-104.

Default

By default, PIM for IPv6 is not enabled on a VLAN interface. When it is enabled, the default value for dr-priority is 1, and for hello-period is 30.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command enables PIM Multicast Routing Protocol for IPv6 on a VLAN interface. If all routers on the interface use the DR Priority option in their PIM Hello messages, the router with the highest value for DR priority will win the DR election. In case the values are the same, highest IPv6 address will be used as a tie-breaker.

Example

This example shows how to configure PIM for IPv6 on a VLAN interface.

```
DmSwitch(config-if-vlan-420)#ipv6 pim
DmSwitch(config-if-vlan-420)#
```

You can verify the PIM configured on a VLAN interface by entering the **show running-config**, **show ipv6 pim config** or the **show ipv6 pim interfaces** privileged EXEC command.

Related Commands

Command	Description
show ipv6 pim interfaces	Shows PIM interfaces parameters.
show ipv6 pim config	Shows global PIM configuration.
show running-config	Shows the current operating configuration.

ip proxy-arp

`ip proxy-arp`

`no ip proxy-arp`

Description

Enables proxy ARP on selected VLAN.

Inserting **no** as a prefix for this command will disable proxy ARP on selected VLAN.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

VLAN configuration.

Command History

Release	Modification
4.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate proxy ARP on the selected VLAN.

```
DmSwitch(config-if-vlan-2)#ip proxy-arp
DmSwitch(config-if-vlan-2)#
```

You can verify that the proxy ARP was enabled by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

Command	Description
<code>ip local-proxy-arp</code>	Sets Local Proxy ARP for the selected VLAN.

ipv6 ripng

ipv6 ripng

no ipv6 ripng

Description

Enables RIPng routing on this VLAN interface.

The **no** command disables RIPng routing on this interface.

Syntax

No parameter accepted.

Default

RIPng routing process is not associated with the interface.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The RIPng process will act only over the specified interface.

Example

This example shows how to specify the RIPng routing process to the specified VLAN interface.

```
DmSwitch(config-if-vlan-1)#ipv6 ripng
DmSwitch(config-if-vlan-1)#
```

You can verify that the RIPng process was associated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>clear ipv6 ripng process</code>	Clear RIPng routing data.
<code>default-metric</code>	Defines the default metric of RIPng protocol.
<code>distance</code>	Defines the administrative distance of RIPng protocol.
<code>passive-interface</code>	Suppresses RIPng routing updates on specified VLAN interfaces.
<code>redistribute</code>	Redistributes routes with a metric of RIPng protocol.
<code>router ripng</code>	Enables and accesses the RIPng configuration.
<code>show ipv6 ripng</code>	Shows the RIPng process parameters.
<code>show ipv6 ripng database</code>	Shows the RIPng database parameters.
<code>show ipv6 ripng neighbors</code>	Shows the RIPng neighbors parameters.
<code>show running-config</code>	Shows the current operating configuration.
<code>timers basic</code>	Defines the basic timers of RIPng protocol.

ip vrf forwarding

```
ip vrf forwarding vrf-name
```

```
no ip vrf forwarding
```

Description

Configures the selected VLAN to use the specified Virtual Private Network (VPN) routing and forwarding (VRF) routing table instance.

Inserting **no** as a prefix for this command will remove the configuration from the selected VLAN.

Syntax

Parameter	Description
<i>vrf-name</i>	Name assigned to a VRF.

Default

The default is to use the global routing table.

Command Modes

VLAN configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	Changed example output to fit this version.

Usage Guidelines

It's possible to assign an IP address from private internet address space (RFC 1918) to VLAN interfaces that forward according to a VRF instance. When enabling a VLAN to forward a VRF, the IP address (if any) will be automatically removed in order to avoid duplicated IP address on the same routing table.

The IP address assigned to the VLAN is placed on the VRF it forwards but not on the global routing table.

Example

This example shows how to set up a VLAN to forward a VRF instance.

```

DmSwitch(config)#interface vlan 1000
DmSwitch(config-if-vlan-1000)#ip address 192.168.1.10/24
DmSwitch(config-if-vlan-1000)#ip vrf forwarding vrf1
% Warning:
IP address 192.168.1.10/24 removed from VLAN due to enabling VRF
DmSwitch(config-if-vlan-1000)#ip address 192.168.1.10/24
DmSwitch(config-if-vlan-1000)#exit
DmSwitch(config)#show ip route vrf vrf1

```

Codes: AD - Administrative Distance

Destination/Mask	Gateway	Protocol	AD/Cost	Output Interface	Status
192.168.1.0/24	192.168.1.10	connect	0/0	VLAN 1000	Active
192.168.1.10/32	0.0.0.0	connect	0/0	-	Active

```
DmSwitch(config)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
interface vlan	Enables the VLAN configuration mode.
ip vrf	Enables the VRF configuration mode.
show ip route vrf	Shows the RIB of the specified VRF.
show ip vrf	Shows VRF general information.
show running-config	Shows the current operating configuration.

ip router isis

ip router isis *area-name*

no ip router isis *area-name*

Description

This command associates an interface to an IS-IS routing process.

Inserting **no** as a prefix for this command will remove this interface from the IS-IS routing process.

Syntax

Parameter	Description
area-name	Area name of IS-IS router to which this interface should be associated.

Default

There is no default configuration for this command.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command allows an interface to be inserted into the IS-IS routing process. This means that the interface will be able to send and receive IS-IS packets.

Example

The following example shows the ip router isis configuration:

```
DmSwitch(config)#interface vlan 100
DmSwitch(config-if-vlan-100)#ip router isis isis1
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>isis passive-interface</code>	Configure interface as a passive IS-IS interface
<code>router isis</code>	Enables and accesses the IS-IS configuration.
<code>show isis</code>	Shows the IS-IS routing table entries.

isis authentication direction recv-only

```
isis authentication direction recv-only [ level-1 | level-2 ]
```

```
no isis authentication direction recv-only [ level-1 | level-2 ]
```

Description

Use this command to configure that authentication is performed only on IS-IS packets being received in an interface.

Inserting **no** as a prefix for this command will disable the recv-only authentication direction for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the recv-only authentication direction for IS-IS level-1.
level-2	(Optional) Specifies the recv-only authentication direction for IS-IS level-2.

Default

There is no default configuration.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the isis authentication recv-only direction for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the configuration of recv-only authentication direction in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis authentication direction recv-only
```


You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in an interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for an interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for an interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for an interface.
show isis	Shows the IS-IS routing table entries.

isis authentication direction send-only

```
isis authentication direction send-only [ level-1 | level-2 ]
```

```
no isis authentication direction send-only [ level-1 | level-2 ]
```

Description

Use this command to configure that authentication is performed only on IS-IS packets being sent in an interface.

Inserting **no** as a prefix for this command will disable the send-only authentication direction for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the send-only authentication direction for IS-IS level-1.
level-2	(Optional) Specifies the send-only authentication direction for IS-IS level-2.

Default

There is no default configuration.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the isis authentication send-only direction for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the configuration of send-only authentication direction in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis authentication direction send-only
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction recv-only	Configure the IS-IS recv-only authentication direction in an interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for an interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for an interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for an interface.
show isis	Shows the IS-IS routing table entries.

isis authentication key-chain

isis authentication key-chain *key-chain name* [**level-1** | **level-2**]

no isis authentication key-chain *key-chain name* [**level-1** | **level-2**]

Description

Configures authentication for IS-IS packets and specifies the set of keys that can be used on an interface.

Inserting **no** as a prefix for this command will disable the authentication key-chain for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
key-chain name	Specifies the key-chain name.
level-1	(Optional) Specifies the authentication key-chain for IS-IS level-1.
level-2	(Optional) Specifies the authentication key-chain for IS-IS level-2.

Default

There is no default configuration.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Configures first the key-chain in the configuration mode and after enables it for the IS-IS router.

Example

The following example enables the key-chain for level-2 in an interface.

```
DmSwitch(config)#key chain isis_level_2
DmSwitch(config-keychain)#key 1
DmSwitch(config-keychain-key)#key-string datacom
```

```
DmSwitch(config-keychain-key) #exit
DmSwitch(config-keychain) #exit
DmSwitch(config) #interface vlan 1
DmSwitch(config-if-vlan-1) #isis authentication key-chain isis_level_2 level-2
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction rcv-only	Configure the IS-IS rcv-only authentication direction in an interface.
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in an interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for an interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for an interface.
show isis	Shows the IS-IS routing table entries.

isis authentication mode clear-text

```
isis authentication mode clear-text [ level-1 | level-2 ]
```

```
no isis authentication mode clear-text [ level-1 | level-2 ]
```

Description

The **isis authentication mode** command specifies the type of authentication used for an interface. The parameter **clear-text** enables the clear-text authentication.

Inserting **no** as a prefix for this command will disable the clear-text authentication mode for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the clear-text authentication mode for IS-IS level-1.
level-2	(Optional) Specifies the clear-text authentication mode for IS-IS level-2.

Default

There is no default configuration.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the clear-text authentication mode for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the clear-text authentication mode configuration in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis authentication mode clear-text level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction rcv-only	Configure the IS-IS rcv-only authentication direction in an interface.
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in an interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for an interface.
isis authentication mode hmac-md5	Configure the IS-IS hmac-md5 authentication mode for an interface.
show isis	Shows the IS-IS routing table entries.

isis authentication mode hmac-md5

```
isis authentication mode hmac-md5 [ level-1 | level-2 ]
```

```
no isis authentication mode hmac-md5 [ level-1 | level-2 ]
```

Description

The **isis authentication mode** command specifies the type of authentication used for an interface. The parameter **hmac-md5** enables the Message Digest 5 (MD5) authentication.

Inserting **no** as a prefix for this command will disable the hmac-md5 authentication mode for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the hmac-md5 authentication mode for IS-IS level-1.
level-2	(Optional) Specifies the hmac-md5 authentication mode for IS-IS level-2.

Default

There is no default configuration.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the hmac-md5 authentication mode for an interface. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the hmac-md5 authentication mode configuration in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis authentication mode hmac-md5 level-1
```


You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis authentication direction rcv-only	Configure the IS-IS rcv-only authentication direction in an interface.
isis authentication direction send-only	Configure the IS-IS send-only authentication direction in an interface.
isis authentication key-chain	Configure the IS-IS authentication key-chain for an interface.
isis authentication mode clear-text	Configure the IS-IS clear-text authentication mode for an interface.
show isis	Shows the IS-IS routing table entries.

isis circuit-type

```
isis circuit-type { level-1 | level-2 | level-1-2 }
```

```
no isis circuit-type
```

Description

This command configures the circuit-type of the IS-IS routing process on an interface.

Inserting **no** as a prefix for this command will reset the configured circuit-type to the default configuration.

Syntax

Parameter	Description
level-1	Configures this interface as level-1 only.
level-2	Configures this interface as level-2 only.
level-1-2	Configures this interface as both level-1 and level-2.

Default

The default configuration is level-1-2.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command allows the configuration of an interface's circuit type level for the IS-IS routing process independently of the IS type configured in the router, given that the desired circuit type level is possible within that router. For example, a level-1-2 router allows the configuration of circuit types level-1 only, level-2 only or level-1-2 in the interfaces that belong to its routing process. However, a level-1 router will only allow configuration of circuit type level-1 on its interfaces.

Example

The following example shows the circuit type configuration:

```
DmSwitch(config)#interface vlan 100
DmSwitch(config-if-vlan-100)#isis circuit-type level-1
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
is-type	Configure the IS-IS Level type
show isis	Shows the IS-IS routing table entries.

isis hello-interval

```
isis hello-interval hello_interval_value [ level-1 | level-2 ]
```

```
no isis hello-interval [ level-1 | level-2 ]
```

Description

Maximum period, in milliseconds, between IS-IS Hello (IIH) PDUs on multiaccess networks for LANs. The range of valid values for this field is 30 - 360000.

Inserting **no** as a prefix for this command will set this value to the default one.

Syntax

Parameter	Description
hello_interval_value	Specifies the hello interval value.
level-1	(Optional) Specifies the hello interval value for IS-IS level-1.
level-2	(Optional) Specifies the hello interval value for IS-IS level-2.

Default

The default hello interval value is 3000.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the hello interval for an interface. If neither the level-1 nor level-2 is configured, the command is applied to both levels. However, if this router is the DIS(Designated IS), the actual interval used will be 1/3 of the configured hello interval. This happens due to the need of fast failure detection for the DIS.

Example

The following example shows the hello interval configuration in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis hello interval 30
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
graceful-restart	Configure graceful restart parameters
show isis	Shows the IS-IS routing table entries.

isis metric

```
isis metric metric_value [ level-1 | level-2 ]
```

```
no isis metric [ metric_value [ level-1 | level-2 ] ]
```

Description

Use this command to configure the metric value of a circuit used for IS-IS. The range of valid values for this field is 1 - 63.

Inserting **no** as a prefix for this command will set this value to the default one for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
metric_value	Specifies the metric value.
level-1	(Optional) Specifies the metric for IS-IS level-1.
level-2	(Optional) Specifies the metric for IS-IS level-2.

Default

The default metric value is 10.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the metric for an interface. If neither the level-1 nor level-2 is configured, the command is applied to both levels.

Example

The following example shows the metric configuration in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis metric 12
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
isis metric-wide	Configure the IS-IS wide metric in a VLAN
metric-style	Configure the IS-IS metric style
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

isis metric-wide

```
isis metric-wide metric_value [ level-1 | level-2 ]
```

```
no isis metric-wide [ level-1 | level-2 ]
```

Description

Use this command to configure the wide metric value of a circuit used for IS-IS. The range of valid values for this field is 1 - 16777215.

Inserting **no** as a prefix for this command will set this value to the default one for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
metric_value	Specifies the wide metric value.
level-1	(Optional) Specifies the wide metric for IS-IS level-1.
level-2	(Optional) Specifies the wide metric for IS-IS level-2.

Default

The default wide metric value is 10.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the wide metric for an interface. It is necessary to configure the metric style for "wide" in the router isis configuration. If neither the level-1 nor level-2 is configured, the command is applied to both levels.

Example

The following example shows the wide metric configuration in a interface.


```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis metric-wide 12
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
isis metric	Configure the IS-IS metric in a VLAN
metric-style	Configure the IS-IS metric style
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

isis network point-to-point

`isis network point-to-point`

`no isis network point-to-point`

Description

This command configures an IS-IS interface as a point-to-point interface.

Inserting **no** as a prefix for this command will remove the point-to-point configuration from the interface.

Syntax

No parameter accepted.

Default

The default configuration is for point-to-point mode to be disabled. The interface uses a broadcast link mode by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command configures an interface as a point-to-point interface, but it must already be associated with an IS-IS router.

Example

The following example shows the network point-to-point configuration:

```
DmSwitch(config)#interface vlan 100
DmSwitch(config-if-vlan-100)#isis network point-to-point
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>ip router isis</code>	Associate interface to an IS-IS routing process
<code>show isis</code>	Shows the IS-IS routing table entries.

isis passive-interface

isis passive-interface *area-name*

no isis passive-interface *area-name*

Description

This command configures an interface as a passive IS-IS interface.

Inserting **no** as a prefix for this command will remove this interface from the IS-IS routing process.

Syntax

Parameter	Description
area-name	Area name of IS-IS router to which this interface should be associated.

Default

There is no default configuration for this command.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command allows an interface to be inserted into the IS-IS routing process without actually sending or receiving any IS-IS packets. This means that its IP address will be redistribute into IS-IS and, consequently, to other neighbors, removing the need to redistribute all connected routes.

Example

The following example shows the passive interface configuration:

```
DmSwitch(config)#interface vlan 100
DmSwitch(config-if-vlan-100)#isis passive-interface isisl
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>ip router isis</code>	Associate interface to an IS-IS routing process
<code>router isis</code>	Enables and accesses the IS-IS configuration.
<code>show ip route</code>	Shows the IP routing table.
<code>show isis</code>	Shows the IS-IS routing table entries.

isis priority

```
isis priority value [ level-1 | level-2 ]
```

```
no isis priority [ level-1 | level-2 ]
```

Description

Use this command to configure the priority value of designated router in a circuit used for IS-IS. The range of valid values for this field is 0 - 127.

Inserting **no** as a prefix for this command will set this value to the default one.

Syntax

Parameter	Description
value	Specifies the priority value.
level-1	(Optional) Specifies the priority for IS-IS level-1.
level-2	(Optional) Specifies the priority for IS-IS level-2.

Default

The default priority value is 64.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Execute this command to configure the priority of DIS for an interface. If neither the level-1 nor level-2 is configured, the command is applied to both levels.

Example

The following example shows the priority configuration in an interface.

```
DmSwitch(config)#interface vlan 1
DmSwitch(config-if-vlan-1)#isis priority 90
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
isis hello interval	Configure the IS-IS hello interval in a VLAN
show isis	Shows the IS-IS routing table entries.

ldp enable ^[1] ^[3] ^[6]

ldp enable

no ldp enable

Description

Enables LDP to run on the specified VLAN.

Inserting **no** as a prefix for this command will remove the configuration from the selected VLAN.

Syntax

No parameter accepted.

Default

LDP is not enabled on a VLAN by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In order to enable LDP to run over a VLAN interface, use **ldp enable** command in the vlan interface configuration mode. LDP will then be able to start the basic discovery process on the specified VLAN and establish link sessions with connected LDP neighbors.

To effectively configure LDP to establish link session with adjacent routers, a minimum configuration set is required:

- add one physical interface to the VLAN;
- assign an IP address to the VLAN interface;
- enable LDP;
- configure LSR-ID via "mpls enable" command on a loopback interface;
- exchange routes with the adjacent routers, either via IP protocols (e.g. OSPF) or via static routes.

Example

This example shows how to enable ldp capability at VLAN.

```
DmSwitch#configure
DmSwitch(config)#interface vlan 1000
DmSwitch(config-if-vlan-1000)#ldp enable
DmSwitch(config-if-vlan-1000)#end
DmSwitch#
```

You can verify the interface VLAN configuration entering the **show running-config** command. You can also verify that the VLAN interface LDP functionality has been properly enabled in the control-plane entering the **show mpls ldp parameters** user EXEC command. The IP address of the interface is listed in the "Local addresses" section of the command output.

Related Commands

Command	Description
interface loopback	Enables the interface loopback configuration mode.
mpls enable	Enables MPLS on the specified loopback interface.
show running-config	Shows the current operating configuration.
show mpls ldp database	List LSP database
show mpls ldp neighbor	Shows the status of LDP sessions.
show mpls ldp parameters	Shows current LDP parameters.

link-detect

link-detect

no link-detect

Description

Enables the VLAN link detect mode on the selected VLAN.

Inserting **no** as a prefix for this command will disable the VLAN link detect.

Syntax

No parameter accepted.

Default

The VLAN link detect mode is disabled.

Command Modes

VLAN configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Use the VLAN link detect mode to put vlan link down when all member ports are down.

Notice that the **vlan link-detect** global configuration mode command overrides the link-detect configuration set for any specific VLAN.

Example

This example shows how to enable the VLAN link detect on an specific VLAN interface.

```
DmSwitch(config)#interface vlan 1000
DmSwitch(config-if-vlan-1000)#link-detect
DmSwitch(config)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>interface vlan</code>	Enables the VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.
<code>vlan link-detect</code>	Enables the VLAN link detect.

mac-address-table learn

`mac-address-table learn`

`no mac-address-table learn`

Description

Enable MAC address learning on the selected VLAN.

Inserting **no** as a prefix for this command will disable VLAN MAC address learning.

Syntax

No parameter accepted.

Default

VLAN MAC address learning is enabled for all VLANs.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

This command can enable or disable learning of MAC addresses in the selected VLAN. Disable learning will clear MAC address table of selected VLAN.

Example

This example shows how to enable the VLAN MAC address learning for a specific VLAN interface.

```
DmSwitch(config)#interface vlan 1000
DmSwitch(config-if-vlan-1000)#mac-address-table learn
DmSwitch(config)#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
<code>interface vlan</code>	Sets the VLAN MAC address table maximum number of entries.
<code>interface vlan</code>	Enables the VLAN configuration mode.
<code>show running-config</code>	Shows the current operating configuration.
<code>show vlan</code>	Shows the Virtual LAN settings.

mac-address-table maximum ^[1] ^[3]

mac-address-table maximum *num-of-macs*

no mac-address-table maximum

Description

Use the mac-address-table maximum to configure the maximum limit of MAC address per VLAN for each unit.
The **no** command form removes the configured limit.

Syntax

Parameter	Description
<i>maximum</i>	Configure the maximum number of MAC addresses.

Default

No limit is configured.

Command Modes

VLAN configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the limit of MAC address table entries on the selected VLAN.

```
DmSwitch(config-if-vlan-2)#mac-address-table maximum 200
DmSwitch(config-if-vlan-2)#
```

You can verify that the configuration was made by entering the **show vlan id 2** privileged EXEC command.

Related Commands

Command	Description
<code>clear mac-address-table</code>	Erases entries stored in the MAC address table.
<code>mac-address-table aging-time</code>	Sets the aging time for MAC address table entries.
<code>show mac-address-table</code>	Shows the MAC address table.
<code>show running-config</code>	Shows the current operating configuration.
<code>switchport port-security maximum</code>	Configures port-security maximum.

Notes

Command not available for default VLAN.

management-mtu

management-mtu *mtu*

no management-mtu

Description

Sets the MTU (maximum transmission unit) used for management issues.

The **no** command form returns the management MTU to the default value.

Syntax

Parameter	Description
<i>mtu</i>	Defines the management mtu in bytes for the selected VLAN. (Range: 1000-9000)

Default

1500 bytes.

Command Modes

VLAN configuration.

Command History

Release	Modification
5.1	This command was introduced.

Usage Guidelines

Changing the management MTU of a VLAN interface will only affect packets to and from the CPU, such as SNMP, Telnet, routing protocols and other management issues. This will not affect switched or routed packets.

To change the MTU of an interface (ethernet or port-channel), please see the related commands below.

Example

This example shows how ping another switch with a 1900 bytes packet. Since the sent packet is smaller than the VLAN MTU, it will not be fragmented.

```
DmSwitch(config-if-vlan-1)#ip address 192.168.21.1/24
DmSwitch(config-if-vlan-1)#management-mtu 2500
DmSwitch(config-if-vlan-1)#end
```



```
DmSwitch#ping 192.168.21.2/24 size 1900
```

You can verify that the VLAN 1 MTU was changed by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show vlan	Shows the Virtual LAN settings.
switchport mtu	Configures maximum transmission unit.
show running-config	Shows the current operating configuration.

mpls bgp forwarding ^[1] ^[3] ^[5]

```
mpls bgp forwarding
```

```
no mpls bgp forwarding
```

Description

Enables MPLS forwarding on the specified VLAN, so it will be able to forward RFC3107 traffic.

Inserting **no** as a prefix for this command will remove the configuration from the selected VLAN.

Syntax

No parameter accepted.

Cross Dependencies

When **neighbor send-label** is enabled on a BGP neighbor that belongs to a network configured on a VLAN, this VLAN will have the **mpls bgp forwarding** set automatically.

Default

MPLS forwarding is not enabled on a VLAN by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

In order to enable MPLS traffic over a VLAN interface, use the **mpls bgp forwarding** in the VLAN interface configuration mode. A member and an *ip address* - with network prefix /30 or /31 - should be previously configured on this VLAN interface. Then, the interface will be able to start forwarding labeled packets on the specified VLAN.

Example

This example shows how to enable MPLS forwarding at a VLAN.

```
DmSwitch#configure
DmSwitch(config)#interface vlan 1000
```

```
DmSwitch(config-if-vlan-1000)#ip address 10.0.0.1/31
DmSwitch(config-if-vlan-1000)#set-member tagged ethernet 1/1
DmSwitch(config-if-vlan-1000)#mpls bgp forwarding
DmSwitch(config-if-vlan-1000)#end
DmSwitch#
```

To verify the VLAN configuration enter the **show vlan** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.
show mpls ldp database	List LSP database
bgp neighbor send-label	Enables Carrying Label Information in BGP-4.

mpls ldp igp sync ^[1] ^[3] ^[6]

```
mpls ldp igp sync
```

```
no mpls ldp igp sync
```

Description

Configures selective MPLS LDP-IGP Synchronization per interface.

Inserting **no** as a prefix for this command will disable the MPLS LDP-IGP Synchronization on the interface.

Syntax

No parameters accepted.

Default

MPLS LDP-IGP Synchronization is enabled on all interfaces that belong to an OSPF instance.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

When you issue the **mpls ldp sync** command, all interfaces that belong to an OSPF instance are enabled for LDP-IGP Synchronization - except on default vlan 1, where LDP-IGP Synchronization is always disabled. To remove LDP-IGP Synchronization from some interfaces, use the **no** form of the **mpls ldp igp sync** command on those interfaces.

Example

This example shows how to disable the MPLS LDP-IGP Synchronization from one interface after LDP-IGP Synchronization was configured through the **mpls ldp sync** command.

```
DmSwitch(config)#interface vlan 1000
DmSwitch(config-if-vlan-1000)#no mpls ldp igp sync
```

You can verify the configuration by issuing the **show mpls ldp igp sync** privileged EXEC command.

Related Commands

Command	Description
<code>mpls ldp sync</code>	Configures MPLS LDP Synchronization with OSPF.

mpls traffic-eng bandwidth ^[1] ^[3] ^[6]

```
mpls traffic-eng bandwidth value
```

```
no mpls traffic-eng bandwidth
```

Description

Configures the bandwidth available and still unreserved on an VLAN interface.

Inserting **no** as a prefix for this command will reset the available bandwidth to the sum of each vlan port capacity.

Syntax

Parameter	Description
<i>value</i>	Specifies the bandwidth value in Kbps.

Default

By default the bandwidth is the sum of each vlan port capacity.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the available bandwidth of an VLAN interface.

```
DmSwitch(config)#interface vlan 405
DmSwitch(config-if-vlan-405)#mpls traffic-eng bandwidth 10000
```

```
DmSwitch(config-if-vlan-4051) #
DmSwitch(config)#interface vlan 405
DmSwitch(config-if-vlan-405)#no mpls traffic-eng bandwidth 10000
DmSwitch(config-if-vlan-405) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

mtu

mtu *mtu*

no mtu

Description

Sets the MTU (maximum transmission unit) for routed packets. It can be applied for both IPv4 and IPv6 routed packets.

The **no** command form returns the MTU to the default value.

Syntax

Parameter	Description
<i>mtu</i>	Defines the MTU in bytes for the selected VLAN. (Range: 576-16383)

Default

16383 bytes.

Command Modes

VLAN configuration.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

Changing the MTU of a VLAN will only affect switched or routed packets and will only be effective if there is an IP address assigned to the VLAN or if IPv6 is enabled. This will not affect packets to and from the CPU, such as SNMP, Telnet, routing protocols and other control and management protocols. To change the management MTU or to change the MTU of an interface (ethernet or port-channel), please see the related commands below.

Example

```
DmSwitch(config-if-vlan-1)# ip address 192.168.21.1/24
DmSwitch(config-if-vlan-1)# mtu 2500
DmSwitch(config-if-vlan-1)# end
```


or

```
DmSwitch(config-if-vlan-1)# ipv6 enable
DmSwitch(config-if-vlan-1)# mtu 2500
DmSwitch(config-if-vlan-1)# end
```

You can verify that the VLAN 1 MTU was changed by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
management-mtu	Configures maximum transmission unit.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.
switchport mtu	Configures maximum transmission unit.

mvr receiver

mvr receiver

no mvr receiver

Description

Sets a VLAN as receiver of multicast traffic from Multicast Vlan Registration protocol.

Inserting **no** as a prefix for this command will reset the mvr receiver configuration.

Note: Packets must have TTL greater than 2 in order to be replicated to destination VLAN.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This feature can set a VLAN as a multicast traffic receiver from specific a VLAN source using the Multicast Vlan Registration Protocol.

To avoid replicating toward a traffic source a VLAN can be configured as source or receiver but never both. Furthermore, a port cannot belong at the same time to the source and receiver VLANs.

Example

This example shows how to set a VLAN as MVR receiver.

```
DmSwitch(config-if-vlan-580)#mvr receiver
DmSwitch(config-if-vlan-580)#
```

You can verify that the MVR receiver was set by entering the **show running-config** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
mvr	Configures the Multicast Vlan Registration.

name

name *name*

no name

Description

Specifies the VLAN name.

Inserting **no** as a prefix for this command will remove the VLAN name.

Syntax

Parameter	Description
<i>name</i>	Specifies a VLAN name.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a VLAN name.

```
DmSwitch(config-if-vlan-1)#name test
DmSwitch(config-if-vlan-1)#
```

You can verify that the name was saved by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

openflow enable

openflow enable

no openflow enable

Description

Enables VLAN usage by OpenFlow protocol.

The **no** command denies the usage of VLAN by OpenFlow protocol.

Syntax

No additional parameter is needed.

Default

VLAN is not configured as OpenFlow usage by default.

Command Modes

VLAN configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

Enabling OpenFlow in a VLAN let OpenFlow protocol use this VLAN.

Example

This example shows how to enable OpenFlow in a VLAN.

```
DmSwitch(config)#interface vlan 300
DmSwitch(config-if-vlan-300)#openflow enable
DmSwitch(config-if-vlan-300)#show this
interface vlan 300
  openflow enable
!
DmSwitch(config-if-vlan-300)#
```

Related Commands

Command	Description
<code>openflow</code>	Enables global OpenFlow protocol.
<code>openflow enable</code>	Enables the use of ethernet interface by OpenFlow protocol.
<code>show openflow</code>	Shows global OpenFlow configuration.

rsvp enable ^[1] ^[3] ^[6]

rsvp enable

no rsvp enable

Description

Enables the RSVP Protocol on the VLAN interface. The VLAN node is not able to handle (send/receive) RSVP messages when RSVP is disabled.

Inserting **no** as a prefix for this command will disable RSVP protocol on the VLAN interface.

Syntax

No parameter accepted.

Default

By default the RSVP protocol is disabled on the VLAN interface.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable and disable the RSVP Protocol on the VLAN interface.

```
DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#rsvp enable
DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp enable
```



```
DmSwitch(config-if-vlan-560)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

rsvp signalling hello refresh interval ^[1] ^[3] ^[6]

rsvp signalling hello refresh interval *milliseconds*

no rsvp signalling hello

Description

Configures the interval for sending HELLO messages on the VLAN interface.

Inserting **no** as a prefix for this command will disable sending of HELLO messages.

Syntax

Parameter	Description
<i>milliseconds</i>	Defines the interval between sending HELLO messages in milliseconds. Range 1..60000 (ms).

Default

HELLO messages are disabled by default.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the hello refresh interval on the VLAN interface.

```
DmSwitch(config)#interface vlan 560
```

```

DmSwitch(config-if-vlan-560)#rsvp signalling hello refresh interval 2000
DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp signalling hello refresh interval
DmSwitch(config-if-vlan-560)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

rsvp signalling hello refresh misses ^[1] ^[3] ^[6]

rsvp signalling hello refresh misses *misses*

no rsvp signalling hello

Description

Configures the number of missed HELLO messages before turning RSVP neighbor down.

Inserting **no** as a prefix for this command will restore the default value.

Syntax

Parameter	Description
<i>misses</i>	Number of missed HELLO messages. Range 1..10.

Default

By default the number of misses HELLO messages is 3.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the hello refresh misses on the VLAN interface.

```
DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#rsvp signalling hello refresh misses 1
```

```

DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp signalling hello refresh misses
DmSwitch(config-if-vlan-560)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

rsvp signalling link attributes ^[1] ^[3] ^[6]

rsvp signalling link attributes *value*

no rsvp signalling link attributes

Description

Defines the VLAN interface link attributes to be used as a constraint for TE tunnels establishment. The value configured by this command is used for affinity compatibility for RSVP tunnels configured with such parameters.

Inserting **no** as a prefix for this command will restore the default value.

Syntax

Parameter	Description
<i>value</i>	Link attributes based on the administrative groups. (Range: 0-4294967295)

Default

Link attributes on the VLAN interface is 0.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the link attributes on the VLAN interface.

```

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#rsvp signalling link attributes 16
DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp signalling link attributes
DmSwitch(config-if-vlan-560)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity

rsvp signalling refresh interval ^[1] ^[3] ^[6]

rsvp signalling refresh interval *milliseconds*

no rsvp signalling refresh interval

Description

Configures the average interval between refresh PATH and RESV messages on the VLAN interface. The number of times the attempts will be done is defined by command **rsvp signalling refresh misses**

Inserting **no** as a prefix for this command will set the VLAN to use rsvp global configuration.

Syntax

Parameter	Description
<i>milliseconds</i>	Refresh interval. Value in milliseconds (1-60000)

Default

By default the refresh interval follows the rsvp global configuration.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

This command has precedence over the rsvp global configuration.

Example

This example shows how to configure the RSVP messages refresh interval on the VLAN interface.

```
DmSwitch(config)#interface vlan 560
```



```

DmSwitch(config-if-vlan-560)#rsvp signalling refresh interval 20000
DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp signalling refresh interval
DmSwitch(config-if-vlan-560)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

rsvp signalling refresh misses ^[1] ^[3] ^[6]

rsvp signalling refresh misses *number*

no rsvp signalling refresh misses

Description

Configures the number of unresponded PATH or RESV refresh attempts which must be made, spaced by the refresh interval (defined by **rsvp signalling refresh interval**) before the neighbor is considered to be down.

Inserting **no** as a prefix for this command will set the VLAN to use rsvp global configuration.

Syntax

Parameter	Description
<i>number</i>	Number of missed RSVP messages (1-10)

Default

By default the refresh misses follows the rsvp global configuration.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

This command has precedence over the rsvp global configuration.

Example

This example shows how to configure the refresh misses on the VLAN interface.

```
DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#rsvp signalling refresh misses 1
DmSwitch(config-if-vlan-560)#
```

```
DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp signalling refresh misses
DmSwitch(config-if-vlan-560)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

rsvp signalling refresh reduction ^[1] ^[3] ^[6]

```
rsvp signalling refresh reduction [no-bundle] [no-req-ack]
[no-srefresh]
```

```
no rsvp signalling refresh reduction
```

Description

Enables RSVP Refresh Reduction on the VLAN interface based on RFC 2961 (RSVP Refresh Overhead Reduction Extensions).

Inserting **no** as a prefix for this command will disable RSVP Refresh Reduction on the VLAN interface.

Syntax

Parameter	Description
no-bundle	No Bundle Messages support.
no-req-ack	Message ID ACKs are not requested by this interface. Unreliable RSVP messages delivery.
no-srefresh	No SRefresh Messages support.

Default

By default the RSVP Refresh Reduction is disabled on the VLAN interface.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

After enabling RSVP Refresh Reduction the use of message IDs is also enabled.

Example

This example shows how to enable and disable the RSVP Refresh Reduction on the VLAN interface.

```
DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#rsvp signalling refresh reduction
DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#rsvp signalling refresh reduction no-req-ack
DmSwitch(config-if-vlan-560)#

DmSwitch(config)#interface vlan 560
DmSwitch(config-if-vlan-560)#no rsvp signalling refresh reduction
DmSwitch(config-if-vlan-560)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng bandwidth	Configures the available TE bandwidth for this interface.
rsvp enable	Enables RSVP protocol on the VLAN interface
rsvp signalling hello refresh interval	Configures the interval for sending HELLO messages
rsvp signalling hello refresh misses	Configures the number of HELLO messages that can be missed
rsvp signalling link attributes	Defines the VLAN interface link attributes
rsvp signalling refresh interval	Configures the refresh interval of RSVP messages
rsvp signalling refresh misses	Configures the number of missed RSVP messages before making neighbor down
rsvp signalling refresh reduction	Enables RSVP Refresh Reduction
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

set-member forbidden

```
set-member forbidden { ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member forbidden { port-channel channel-group-number }
```

```
set-member forbidden { local-tunnel endpoint {1|2} }[5][7]
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ]
```

```
no set-member [ local-tunnel endpoint {1|2} ][5][7]
```

Description

Forbids an interface to be dynamically added to a VLAN by the GVRP protocol.

Syntax

Parameter	Description
all	Forbids all ports.
[unit-number/] port-number	Forbids a specific unit and port.
range [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Forbids a range of specific units and ports.
port-channel channel-group-number	Forbids a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-32)
local-tunnel endpoint {1 2} ^{[5][7]}	Adds a specific local tunnel endpoint. The endpoint must be specified in accordance with the endpoints available in the switch. (Range: 1-2)

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to forbid adding members to selected VLAN 1 on a ethernet port range.

```
DmSwitch(config-if-vlan-1)#set-member forbidden ethernet range 1 10
DmSwitch(config-if-vlan-1)#
```

You can verify that the configuration was done by entering the **show vlan table** privileged EXEC command.

Related Commands

Command	Description
set-member tagged	Adds tagged members to selected VLAN.
set-member untagged	Adds untagged members to selected VLAN.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

set-member tagged

```
set-member tagged { ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member tagged { port-channel channel-group-number }
```

```
set-member tagged { local-tunnel endpoint {1|2} }[5][7]
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ]
```

```
no set-member [ local-tunnel endpoint {1|2} ][5][7]
```

Description

Adds tagged members to selected VLAN.

Entering with **no** command, it removes tagged members from selected VLAN.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number	Adds a range of specific units and ports.
port-channel channel-group-number	Adds a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-32)
local-tunnel endpoint {1 2} ^{[5][7]}	Adds a specific local tunnel endpoint. The endpoint must be specified in accordance with the endpoints available in the switch. (Range: 1-2)

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.0	The local-tunnel endpoint parameter was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add a ethernet port range with tagged members to selected VLAN 1.

```
DmSwitch(config-if-vlan-1)#set-member tagged ethernet range 1/25 1/28
DmSwitch(config-if-vlan-1)#
```

You can verify that the members was added by entering the **show vlan table** privileged EXEC command.

Related Commands

Command	Description
set-member forbidden	Adds via GVRP forbidden members to a selected VLAN.
set-member untagged	Adds untagged members to selected VLAN.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

set-member untagged

```
set-member untagged { ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } }
```

```
set-member untagged { port-channel channel-group-number }
```

```
set-member untagged { local-tunnel endpoint {1|2} }[5][7]
```

```
no set-member [ ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } } ]
```

```
no set-member [ port-channel channel-group-number ][5][7]
```

```
no set-member [ local-tunnel endpoint {1|2} ]
```

Description

Adds untagged members to selected VLAN.

Entering with **no** command, it removes untagged members from selected VLAN.

Syntax

Parameter	Description
all	Adds all ports.
[unit-number/] port-number	Adds a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Adds a range of specific units and ports.
port-channel channel-group-number	Adds a specific port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-32)
local-tunnel endpoint {1 2} ^{[5][7]}	Adds a specific local tunnel endpoint. The endpoint must be specified in accordance with the endpoints available in the switch. (Range: 1-2)

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.0	The local-tunnel endpoint parameter was introduced.

Usage Guidelines

Not available.

Example

This example shows how to add a ethernet port range with untagged members to selected VLAN 1.

```
DmSwitch(config-if-vlan-1)#set-member untagged ethernet range 1 10
DmSwitch(config-if-vlan-1)#
```

You can verify that the members was added by entering the **show vlan table** privileged EXEC command.

Related Commands

Command	Description
set-member forbidden	Adds via GVRP forbidden members to a selected VLAN.
set-member tagged	Adds tagged members to selected VLAN.
show running-config	Shows the current operating configuration.
show vlan	Shows the Virtual LAN settings.

shutdown

shutdown

no shutdown

Description

Deactivates the selected VLAN.

Inserting **no** as a prefix for this command will reactivate the selected VLAN.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

You can not deactivate the VLAN 1 since it is the default VLAN.

Example

This example shows how to deactivate the selected VLAN.

```
DmSwitch(config-if-vlan-2)#shutdown
DmSwitch(config-if-vlan-2)#
```

You can verify that the VLAN was deactivated by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

Command	Description
<code>show vlan</code>	Shows the Virtual LAN settings.

vrrp *group* authentication

```
vrrp group authentication { text-string | ah key-string }
```

```
no vrrp group [ authentication ]
```

Description

Configures an authentication string for VRRP group.

The **no** command disables VRRP authentication on the router group.

Syntax

Parameter	Description
<i>group</i>	Selects VRRP group to apply the configuration.
<i>text-string</i>	Uses plaint text authentication.
ah	Uses Authentication Header.
<i>key-string</i>	Hexkey authentication.

Default

No authentication is enabled.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
5.0	This command was introduced.
11.0	Was introduced limits for the options "text-string" - Plain text authentication string (min 5, max 8 characters); and "ah" - Hexkey authentication (min 5, max 14 characters).

Usage Guidelines

Not available.

Example

This example shows how to configure authentication in VRRP group.

```
DmSwitch(config-if-vlan-1)#vrrp 7 authentication secret
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show vrrp** privileged EXEC command.

Related Commands

Command	Description
vrrp ip	Configures VRRP IP on a VLAN.
vrrp ipv6	Configures VRRP IPv6 on a VLAN.
vrrp priority	Configures the priority for a VRRP group.
vrrp shutdown	Configures the VRRP group status.
vrrp preempt	Configures the VRRP group preemption mode.
show running-config	Shows the current operating configuration.
show vrrp	Shows Virtual Router Redundancy Protocol information.

vrrp group ip

vrrp group ip *ip-address* [**secondary**]

no vrrp group ip

Description

Configures the IP address for a VRRP group.

Syntax

Parameter	Description
<i>group</i>	Selects VRRP group to apply the configuration.
<i>ip-address</i>	Specifies the IP address to the selected router group.
secondary	Specifies a secondary virtual IP address to the selected router group.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
5.0	This command was introduced.
13.4	Secondary virtual IP address was added.

Usage Guidelines

Not available.

Example

This example shows how to specify a IP address to the VRRP group.

```
DmSwitch(config-if-vlan-1)#vrrp 7 ip 10.10.10.254
DmSwitch(config-if-vlan-1)#vrrp 7 ip 10.10.10.253 secondary
DmSwitch(config-if-vlan-1)#
```


You can verify that the IP address was specified by entering the **show vrrp** privileged EXEC command.

Related Commands

Command	Description
vrrp ipv6	Configures VRRP IPv6 on a VLAN.
vrrp authentication	Configures authentication on a VRRP group.
vrrp priority	Configures the priority for a VRRP group.
vrrp shutdown	Configures the VRRP group status.
vrrp preempt	Configures the VRRP group preemption mode.
show running-config	Shows the current operating configuration.
show vrrp	Shows Virtual Router Redundancy Protocol information.
show ip interface	Shows the interface information.

vrrp group ipv6

vrrp group ipv6 ipv6-address

no vrrp group ipv6

Description

Configures the IPv6 address for a VRRP group.

Syntax

Parameter	Description
<i>group</i>	Selects VRRP group to apply the configuration.
<i>ipv6 address</i>	Specifies the IPv6 address to the selected router group.

Default

No default is defined.

Command Modes

VLAN configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify a IPv6 address to the VRRP group.

```

DmSwitch(config-if-vlan-1)#vrrp 7 ipv6 2003::2
DmSwitch(config-if-vlan-1)#

```

You can verify that the IPv6 address was specified by entering the **show vrrp** privileged EXEC command.

Related Commands

Command	Description
vrrp ip	Configures VRRP IP on a VLAN.
vrrp authentication	Configures authentication on a VRRP group.
vrrp priority	Configures the priority for a VRRP group.
vrrp shutdown	Configures the VRRP group status.
vrrp preempt	Configures the VRRP group preemption mode.
show running-config	Shows the current operating configuration.
show vrrp	Shows Virtual Router Redundancy Protocol information.
show ipv6 interface	Shows IPv6 interface information.

vrp group preempt

vrp group preempt

no vrrp group [preempt]

Description

Configures the VRRP group preemption mode.

Syntax

Parameter	Description
<i>group</i>	Selects VRRP group to apply the configuration.

Default

Status: Enable

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure preemption mode on a VRRP group.

```
DmSwitch(config-if-vlan-1)#vrrp 7 preempt
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show vrrp** privileged EXEC command.

Related Commands

Command	Description
vrrp authentication	Configures authentication on a VRRP group.
vrrp ip	Configures VRRP IP on a VLAN.
vrrp ipv6	Configures VRRP IPv6 on a VLAN.
vrrp priority	Configures the priority for a VRRP group.
vrrp shutdown	Configures the VRRP group status.
show running-config	Shows the current operating configuration.
show vrrp	Shows Virtual Router Redundancy Protocol information.

vrrp group priority

vrrp group priority *value*

no vrrp group priority

Description

Configures the priority for a VRRP.

Syntax

Parameter	Description
<i>group</i>	Selects VRRP group to apply the configuration.
<i>value</i>	Specifies the priority value. (Range: 1-254)

Default

Priority: 150

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Defines the priority to help determine the VRRP master router for a group.

Example

This example shows how to configure the priority on a VRRP group.

```
DmSwitch(config-if-vlan-1)#vrrp 2 priority 175
DmSwitch(config-if-vlan-1)#
```

You can verify the configuration by entering the **show vrrp** privileged EXEC command.

Related Commands

Command	Description
vrrp authentication	Configures authentication on a VRRP group.
vrrp ip	Configures VRRP IP on a VLAN.
vrrp ipv6	Configures VRRP IPv6 on a VLAN.
vrrp shutdown	Configures the VRRP group status.
vrrp preempt	Configures the VRRP group preemption mode.
show running-config	Shows the current operating configuration.
show vrrp	Shows Virtual Router Redundancy Protocol information.

vrrp group shutdown

vrrp group shutdown

no vrrp group [shutdown]

Description

Configures the VRRP group status.

The **no** command starts the VRRP group.

Syntax

Parameter	Description
<i>group</i>	Selects VRRP group to apply the configuration.

Default

Status: Enable

Command Availability

Only on models with Layer 3 functionality.

Command Modes

VLAN configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the OSPF network type for a VLAN.

```
DmSwitch(config-if-vlan-1)#vrrp 7 shutdown
DmSwitch(config-if-vlan-1)#
```


You can verify the configuration by entering the **show vrrp** privileged EXEC command.

Related Commands

Command	Description
vrrp authentication	Configures authentication on a VRRP group.
vrrp ip	Configures VRRP IP on a VLAN.
vrrp ipv6	Configures VRRP IPv6 on a VLAN.
vrrp priority	Configures the priority for a VRRP group.
vrrp preempt	Configures the VRRP group preemption mode.
show running-config	Shows the current operating configuration.
show vrrp	Shows Virtual Router Redundancy Protocol information.

Chapter 30. Interface Management Commands

ipv6 enable

ipv6 enable

no ipv6 enable

Description

Enable IPv6 support for the MGMT-ETH interface and assign a Link-Local address.

Inserting **no** as a prefix for this command will disable IPv6 support for the MGMT-ETH.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

MGMT-ETH configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable IPv6 in the MGMT-ETH interface.

```
DmSwitch(config-if-mgmt-eth)#ipv6 enable
DmSwitch(config-if-mgmt-eth)#
```

You can verify that the IPv6 feature was enabled in MGMT-ETH interface by entering the **show running-config** user EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

ipv6 address

ipv6 address { *ipv6-address/prefix-length* }

ipv6 address { *ipv6-prefix/prefix-length* | **eui-64** }

no ipv6 address

Description

Sets an IPv6 address for the MGMT-ETH port.

Inserting **no** as a prefix for this command, it will delete the IPv6 address from the MGMT-ETH port.

Syntax

Parameter	Description
<i>ipv6-address/prefix-length</i>	Specifies the IPv6 address and prefix length to the MGMT-ETH port.
<i>ipv6-prefix/prefix-length</i>	Specifies the IPv6 address prefix and prefix length to the MGMT-ETH port.
eui-64	Complete the IPv6 address prefix with a suffix in EUI-64 format.

Default

No default is defined.

Command Modes

MGMT-ETH configuration.

Usage Guidelines

IPv6 feature must be enabled in MGMT-ETH to be able to set an IPv6 address.

Example

This example shows how to specify an IPv6 address to the MGMT-ETH port.

```
DmSwitch(config-if-mgmt-eth)#ipv6 address 2001:DB8::1234/64
DmSwitch(config-if-mgmt-eth)#
```

This other example show how to specify an IPv6 address in EUI-64 format to the MGMT-ETH port.

```
DmSwitch(config-if-mgmt-eth)#ipv6 address 2001:DB8::/64 eui-64
DmSwitch(config-if-mgmt-eth)#
```

You can verify that the IPv6 address was specified by entering the **show ip** privileged EXEC command.

Related Commands

Command	Description
<code>ipv6 default-gateway</code>	Configures the IPv6 default gateway for DmSwitch.
<code>show ip</code>	Shows the IP configuration.
<code>show running-config</code>	Shows the current operating configuration.

Chapter 31. IP Route PBR Commands

action

```
action { l3-routing | next-hop ip-address}
```

```
no action
```

Description

Defines the action to be applied in PBR sequence.

Inserting **no** for this command will remove this configuration.

Syntax

Parameter	Description
l3-routing	Sets an action to perform the standard l3 routing.
next-hop <i>ip-address</i>	Sets an action to change the next hop to a specific IP address despite of standard l3 routing defined by IGP or EGP protocols and static routes.

Default

There is no default configuration.

Command Modes

IP Route PBR configuration.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

The user must create a sequence for PBR before inserting the rules associated to it.

The **action** parameter is required for correct PBR sequence installation on HW.

Example

The examples show how to configure an action in a PBR sequence.

Ex.1 - action l3-routing : This action ensures that all L3 incoming traffic matching the PBR will not be redirected. The traffic will be routed according to the current routing table.

```
DmSwitch(config)#ip route pbr seq 1
DmSwitch(config-ip-route-pbr)#action l3-routing
DmSwitch(config-ip-route-pbr)#match src-interface ethernet all
DmSwitch(config-ip-route-pbr)#match src-ip 10.10.10.0/24
DmSwitch(config-ip-route-pbr)#match dest-ip 20.20.10.0/24
```

Ex.2 - action next-hop : This action changes the next-hop of all L3 incoming traffic matching the PBR. The traffic is effectively redirected to another path, as long as the specified next-hop exists in the current routing table and it is resolved in the host-table.

```
DmSwitch(config)#ip route pbr seq 1
DmSwitch(config-ip-route-pbr)#action next-hop 10.1.5.2
DmSwitch(config-ip-route-pbr)#match src-interface ethernet all
DmSwitch(config-ip-route-pbr)#match src-ip 10.10.10.0/24
DmSwitch(config-ip-route-pbr)#match dest-ip 20.20.20.0/24
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip route pbr	Enables the IP Route PBR configuration mode.
description	Set description for PBR sequence.
match dest-ip	Set destination IP address for PBR sequence.
match src-interface	Set source interface for PBR sequence.
match src-ip	Set source IP address for PBR sequence.
show ip route pbr	Shows the PBR entries.

description

description *text*

no description

Description

Specifies a text for the PBR sequence.

Inserting **no** for this command will remove this configuration.

Syntax

Parameter	Description
<i>text</i>	Adds a text for PBR sequence.

Default

There is no default configuration.

Command Modes

IP Route PBR configuration.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

The user can add a description with up to 32 characters for a PBR sequence.

The **description** parameter is optional.

Example

The example shows how to add a description in a PBR sequence.

```
DmSwitch(config)#ip route pbr seq 10
DmSwitch(config-ip-route-pbr)#description feature pbr
```


You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip route pbr	Enables the IP Route PBR configuration mode.
action	Set action rule for PBR sequence.
match dest-ip	Set destination IP address for PBR sequence.
match src-interface	Set source interface for PBR sequence.
match src-ip	Set source IP address for PBR sequence.
show ip route pbr	Shows the PBR entries.

match dest-ip

```
match dest-ip ip-address/mask
```

```
no match dest-ip
```

Description

Destination IP address that will be used as a rule to trigger the specified action in a PBR sequence.

Inserting **no** for this command will remove this configuration.

Syntax

Parameter	Description
<i>ip-address/mask</i>	Destination IP address for PBR rule matching.

Default

There is no default configuration.

Command Modes

IP Route PBR configuration.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

The user must create a sequence for PBR before inserting the rules associated to it.

The **match dest-ip** parameter is optional. If the parameter is not added, the PBR action is performed independent from destination IP address.

Example

The example shows how to configure a destination IP address rule in a PBR sequence.

```
DmSwitch(config)#ip route pbr seq 10
DmSwitch(config-ip-route-pbr)#match dest-ip 100.100.100.0/24
```

```
DmSwitch(config-ip-route-pbr)#
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip route pbr	Enables the IP Route PBR configuration mode.
action	Set action rule for PBR sequence.
description	Set description for PBR sequence.
match src-interface	Set source interface for PBR sequence.
match src-ip	Set source IP address for PBR sequence.
show ip route pbr	Shows the PBR entries.

match src-interface

```
match src-interface ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

```
no match src-interface ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ] last-port-number } }
```

Description

Sets the interfaces where the PBR sequence will be applied on.

Inserting **no** for this command will remove this configuration.

Syntax

Parameter	Description
all	Enables for all ports.
[unit-number/] port-number	Enables for a specific unit and port.
range { [first-unit-number/] first-port-number [last-unit-number/] last-port-number }	Enables for a range of units and ports.

Default

There is no default configuration.

Command Modes

IP Route PBR configuration.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

The user must create a sequence for PBR before inserting the rules associated to it.

The **match src-interface ethernet** parameter is required for correct PBR sequence installation on HW.

Example

The example shows how to enable the PBR sequence rules for port range 1 to 10 of unit 1.

```
DmSwitch(config-ip-route-pbr)#match src-interface ethernet range 1/1 1/10
DmSwitch(config-ip-route-pbr)#
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip route pbr	Enables the IP Route PBR configuration mode.
action	Set action rule for PBR sequence.
description	Set description for PBR sequence.
match dest-ip	Set destination IP address for PBR sequence.
match src-ip	Set source IP address for PBR sequence.
show ip route pbr	Shows the PBR entries.

match src-ip

```
match src-ip ip-address/mask
```

```
no match src-ip
```

Description

Source IP address that will be used as a rule to trigger the specified action in a PBR sequence.

Inserting **no** for this command will remove this configuration.

Syntax

Parameter	Description
<i>ip-address/mask</i>	Source IP address for PBR rule matching.

Default

There is no default configuration.

Command Modes

IP Route PBR configuration.

Command History

Release	Modification
12.4.6	This command was introduced.

Usage Guidelines

The user must create a sequence for PBR before inserting the rules associated to it.

The **match src-ip** parameter is optional. If the parameter is not added, the PBR action is performed independent from source IP address.

Example

The following example shows how to configure a host as source IP address rule in a PBR sequence:

```
DmSwitch(config)#ip route pbr seq 10
DmSwitch(config-ip-route-pbr)#match src-ip 172.16.96.34/32
```

```
DmSwitch(config-ip-route-pbr)#
```

And the following configuration matches a whole /29 subnet:

```
DmSwitch(config)#ip route pbr seq 11
DmSwitch(config-ip-route-pbr)#match src-ip 172.16.96.32/29
DmSwitch(config-ip-route-pbr)#
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip route pbr	Enables the IP Route PBR configuration mode.
action	Set action rule for PBR sequence.
description	Set description for PBR sequence.
match dest-ip	Set destination IP address for PBR sequence.
match src-ip	Set source IP address for PBR sequence.
show ip route pbr	Shows the PBR entries.

Chapter 32. IPFIX Commands

ipfix host

```
ipfix host index { address ipaddress | port udpport }
```

```
no ipfix host index { address | port }
```

Description

Configures an IPFIX collector.

Inserting **no** as a prefix for this command will remove the specified IPFIX configuration.

Syntax

Parameter	Description
host	Configure an IPFIX collector.
<i>index</i>	Sets the IPFIX collector index. (Range 1-2)
address	Configure an IPFIX collector IPv4 address.
<i>ipaddress</i>	The IPFIX collector IPv4 address.
port	Configure an IPFIX collector UDP port.
<i>udpport</i>	The IPFIX collector UDP port. (Range 1-65535)

Default

udpport: 4739

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Example

This example shows how to configure an IPFIX collector port and IPv4 address.

```
DmSwitch(config)#ipfix host 1 address 172.16.0.1
DmSwitch(config)#ipfix host 1 port 4739
```

To verify the IPFIX configuration enter the **show ipfix** command.

Related Commands

Command	Description
ipfix flow-trigger	Configures IPFIX flow monitoring parameters.
ipfix	Enables IPFIX on an Ethernet Interface.
show ipfix	Shows IPFIX configuration.

ipfix flow-trigger

```
ipfix flow-trigger ingress sample-rate rate
```

```
no ipfix flow-trigger
```

Description

Configures IPFIX flow monitoring parameters.

Inserting **no** as a prefix for this command will remove the specified IPFIX configuration.

Syntax

Parameter	Description
flow-trigger	Specify IPFIX flows triggering parameters.
ingress	Monitor ingress traffic.
sample-rate	Specify the sample-rate.
<i>rate</i>	Sampling rate in packet/s. Range (1-8191)

Default

ingress

sample-rate: 100

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.0	This command was introduced.

Example

This example shows how to configure the IPFIX flows sample-rate.

```
DmSwitch(config)#ipfix flow-trigger ingress sample-rate 100
```

To verify the IPFIX configuration enter the **show ipfix** command.

Related Commands

Command	Description
<code>ipfix host</code>	Configures an IPFIX collector.
<code>ipfix</code>	Enables IPFIX on an Ethernet Interface.
<code>show ipfix</code>	Shows IPFIX configuration.

Chapter 33. IP VRF Commands

import-map

import-map *name*

no import-map *name*

Description

Associates an import route map with the VRF instance.

Inserting **no** as a prefix for this command will remove this configuration.

Syntax

Parameter	Description
<i>name</i>	Specifies the name of the route map to be associate with the VRF instance.

Default

There is no default configuration.

Command Modes

IP VRF configuration.

Command History

Release	Modification
8.0	This command was introduced.
10.0	This command was deprecated.

Usage Guidelines

The route map must be created before associate it with the VRF.

The route map rules will be applied at the importation of a route to the VRF instance.

Example

The example shows how to associate the route map IN_VPN1 with the VRF instance VPN1.

```
DmSwitch(config)#ip vrf VPN1
DmSwitch(config-ip-vrf)#import-map IN_VPN1
```

You can verify the fill here by entering the **show ip vrf** command.

Related Commands

Command	Description
ip vrf	Enables the VRF configuration mode.
rd	Specifies the route distinguisher for a VRF instance.
route-target	Creates a route-target extended community for a VRF instance.
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address	Matches ip address by prefix-list values from routing table.
prefix-list	
match ip next-hop	Matches next-hop ip values from routing table.
prefix-list	
match ip route-source	Matches route-source ip values from routing table.
prefix-list	
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show ip vrf	Shows VRF general information.
show running-config	Shows the current operating configuration.

maximum routes

maximum routes *limit*

no maximum routes

Description

Configures the maximum number of routes allowed in a VRF table.

Inserting **no** as a prefix for this command will remove the limit on the maximum number of routes allowed.

Syntax

Parameter	Description
<i>limit</i>	Specifies the maximum number of routes allowed in a VRF. The valid range is from 1 to 4,294,967,295

Default

No default is defined.

Command Modes

IP VRF configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **maximum routes** command to limit the number of routes allowed in a VRF. This command prevents a provider edge (PE) from importing too many routes into a VRF.

Example

This example shows how to configure the maximum number of VRF routes allowed to 100.

```
DmSwitch(config-ip-vrf)#maximum routes 100
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>ip vrf</code>	Enables the VRF configuration mode.
<code>show running-config</code>	Shows the current operating configuration.

rd [1] [3] [5]

rd { *AS:number* | *ip-address:number* }

no rd

Description

Specifies the route distinguisher (RD) for a VRF instance.

Inserting **no** as a prefix for this command will remove the route distinguisher value.

Syntax

Parameter	Description
<i>AS:number</i>	Composed of a 4-byte Autonomous System (AS) number followed by an arbitrary number.
<i>ip-address:number</i>	Composed of an IP address assigned to a router's interface followed by an arbitrary number.

Default

There is no default. A suitable RD must be configured for a VRF be functional.

Command Modes

IP VRF configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

A single router distinguisher (RD) must be assigned to a VRF. The RD is then added to the beginning of customer's IPv4 prefixes to compose a globally unique VPNv4 prefixes on network.

There are two ways to specify a route distinguisher:

4-byte autonomous-system-number:user 2-byte number, for example 65123:1

4-byte ip-address:user 2-byte number, for example 10.1.2.3:13

Example

This example shows how to configure an RD for a VRF instance.

```
DmSwitch(config)#ip vrf vrf1
DmSwitch(config-ip-vrf)#rd 65123:1
DmSwitch(config)#
```

To verify the RD assigned to a VRF enter the **show ip vrf vrf-name** command.

Related Commands

Command	Description
ip vrf	Enables the VRF configuration mode.
import-map	Associates an import route map with the VRF instance.
route-target	Creates a route-target extended community for a VRF instance.
show ip vrf	Shows VRF general information.

route-target ^[1] ^[3] ^[5]

```
route-target { both | export | import } { AS:number | ip-address:number }
```

```
no route-target { both | export | import } { AS:number | ip-address:number }
```

Description

Creates a route-target extended community for a VRF instance.

Inserting **no** as a prefix for this command will remove the route-target configuration.

Syntax

Parameter	Description
both	Exports and import routing information from the target VPN extended community.
export	Exports routing information from the target VPN extended community.
import	Imports routing information from the target VPN extended community.
<i>AS:number</i>	Composed of a 4-byte Autonomous System (AS) number followed by an arbitrary number.
<i>ip-address:number</i>	Composed of an IP address assigned to a router's interface followed by an arbitrary number.

Default

There is no default. A suitable route-target must be configured in order to include the VRF into an L3VPN.

Command Modes

IP VRF configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The route-target command creates import and export route target extended communities for the specified VRF. Routes learned via MP-BGP that has an extended community that matches one of the import rules will be imported into the VRF.

Routes learned from Customer Edge (CE) router via BGP, or static routes added to the VRF, will be advertised to all MP-BGP neighbors carrying the extended community configured by export rules added to the VRF.

There are two ways to specify an extended community:

4-byte autonomous-system-number:user 2-byte number, for example 65123:1

4-byte ip-address:user 2-byte number, for example 10.1.2.3:13

Example

This example shows how to configure a route-target for a VRF instance.

```
DmSwitch(config)#ip vrf vrf1
DmSwitch(config-ip-vrf)#route-target both 65123:3
DmSwitch(config-ip-vrf)#
```

To verify the route-target configuration of a VRF enter the **show ip vrf vrf-name** command.

Related Commands

Command	Description
ip vrf	Enables the VRF configuration mode.
import-map	Associates an import route map with the VRF instance.
rd	Specifies the route distinguisher for a VRF instance.
show ip vrf	Shows VRF general information.

Chapter 34. IP DHCP Server Commands

enable

enable

no enable

Description

Enables the DHCP server globally.

Syntax

No parameter accepted.

Default

The default value is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.

Command	Description
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

excluded-address

excluded-address { *ip-address* | **range** *start-ip-address end-ip-address* }

no excluded-address *ip-address*

no excluded-address range *start-ip-address* [*end-ip-address*]

Description

Exclude addresses from DHCP pools.

Syntax

Parameter	Description
<i>ip-address</i>	The IPv4 address to be excluded from all DHCP pools.
<i>start-ip-address</i>	Sets the range start address to be excluded from all DHCP pools.
<i>end-ip-address</i>	Sets the range start address to be excluded from all DHCP pools.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure IPv4 addresses as excluded from DHCP pools.

Ex.1 - **excluded-address** : This command will exclude a single IPv4 address from the pool, in this case the DHCP server will consider as a usable range: 192.168.0.2 - 192.168.0.254.

```
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
```

```
DmSwitch(config-dhcp-pool-test)#exit
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#excluded-address 192.168.0.1
```

Ex.2 - **excluded-address range** : This command will exclude a range of IPv4 addresses from the pool, in this case the DHCP server will consider as a usable range: 192.168.0.11 - 192.168.0.254.

```
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#exit
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#excluded-address range 192.168.0.1 192.168.0.10
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

fixed-address

fixed-address **hostname** *name* **ip-address** *ip* **mac-address** *mac*

no fixed-address **hostname** *name*

Description

Define host/ip mappings for DHCP pools.

Syntax

Parameter	Description
<i>name</i>	Sets hostname of the entry.
<i>ip</i>	Sets IPv4 address of the entry.
<i>mac</i>	Sets MAC address of the entry.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a host with static mapped IPv4 address.

Ex.1 - **fixed-address** **hostname** *name* **ip-address** *ip* **mac-address** *mac* : This will make the DHCP server always offer the same IPv4 address to the associated MAC address.

```
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#exit
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#fixed-address hostname name ip-address 192.168.0.100 mac-address 00:01:02:03:04:05
```


You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

Chapter 35. IP DHCP Pool Commands

network

network *prefix/mask*

no network

Description

Configure the IPv4/prefix for the DHCP pool.

Syntax

Parameter	Description
<i>prefix/mask</i>	Sets prefix/mask of the pool.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool prefix/mask.

Ex.1 - **network** *192.168.0.0/24* : This will create an address pool, so that the DHCP server will offer addresses within the range of 192.168.0.1 - 192.168.0.254 to requesting clients.

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
```

```
DmSwitch(config-dhcp-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

default-router

default-router *ip-address* [**secondary**]

no default-router *ip-address*

Description

Configure default routers for the DHCP pool.

Syntax

Parameter	Description
<i>ip-address</i>	The IPv4 address of the router.
secondary	Sets this address as secondary, so it will have lower preference.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool prefix/mask and it's default routers.

Ex.1 - **default-router** *192.168.0.1* : This will create an address pool and set it's primary and secondary default-routers.

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#default-router 192.168.0.1
DmSwitch(config-dhcp-pool-test)#default-router 192.168.0.2 secondary
DmSwitch(config-dhcp-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

dns-server

dns-server *ip-address* [**secondary**]

no dns-server *ip-address*

Description

Configure DNS servers for the DHCP pool.

Syntax

Parameter	Description
<i>ip-address</i>	The IPv4 address of the server.
secondary	Sets this address as secondary, so it will have lower preference.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool prefix/mask and it's DNS servers.

Ex.1 - **dns-server** *192.168.0.1* : This will create an address pool and set it's primary and secondary dns-servers.

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#dns-server 192.168.0.1
DmSwitch(config-dhcp-pool-test)#dns-server 192.168.0.2 secondary
DmSwitch(config-dhcp-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

netbios-name-server

netbios-name-server *ip-address* [**secondary**]

no netbios-name-server *ip-address*

Description

Configure NetBios name servers for the DHCP pool.

Syntax

Parameter	Description
<i>ip-address</i>	The IPv4 address of the server.
secondary	Sets this address as secondary, so it will have lower preference.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool prefix/mask and it's Netbios name servers.

Ex.1 - **netbios-name-server** *192.168.0.1* : This will create an address pool and set it's primary and secondary netbios-name-servers.

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#netbios-name-server 192.168.0.1
DmSwitch(config-dhcp-pool-test)#netbios-name-server 192.168.0.2 secondary
DmSwitch(config-dhcp-pool-test)#exit
```


You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

netbios-node-type

```
netbios-node-type { b-node | p-node | m-node | h-node }
```

```
no netbios-node-type
```

Description

Configure the NetBios node type option (RFC 2132) for the DHCP pool.

Syntax

Parameter	Description
b-node	Sets the NetBios node type option to 0x01 Broadcast.
p-node	Sets the NetBios node type option to 0x02 Peer (WINS only).
m-node	Sets the NetBios node type option to 0x04 Mixed (broadcast, then WINS).
h-node	Sets the NetBios node type option to 0x08 Hybrid (WINS, then broadcast).

Default

The default value is h-node.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool and set its NetBios node type option.

Ex.1 - **netbios-node-type b-node** : This will create an address pool and set the netbios node type option

to b-node.

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#netbios-node-type b-node
DmSwitch(config-dhcp-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

domain-name

domain-name *name*

no domain-name

Description

Configure the domain name option (RFC 2132) for the DHCP pool.

Syntax

Parameter	Description
<i>name</i>	Sets domain name option of the pool.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool and set its domain name option.

Ex.1 - **domain-name** *datacom.net* : This will create an address pool and set the domain name option to "datacom.net".

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#domain-name datacom.net
DmSwitch(config-dhcp-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

lease

lease days *num-days* [**hours** *num-hours* [**minutes** *num-minutes*]]

no lease

Description

Configure the maximum lease time for this DHCP pool.

Syntax

Parameter	Description
<i>num-days</i>	Number of days.
<i>num-hours</i>	Number of hours.
<i>num-minutes</i>	Number of minutes.

Default

The default value is 1 day.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool and set it's maximum lease time.

Ex.1 - **lease days 30** : This will create an address pool and set it's maximum lease time to 30 days.

```
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
```

```
DmSwitch(config-dhcp-pool-test)#lease days 30
DmSwitch(config-dhcp-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server enable	Enables the DHCP server configuration mode.
excluded-address	Enables the DHCP server globally.
fixed-address	Exclude addresses from DHCP pools.
ip dhcp pool	Define host/ip mappings for DHCP pools.
network	Enables the DHCP pool configuration mode.
default-router	Configure the prefix/mask for the DHCP pool.
dns-server	Configure default routers for the DHCP pool.
netbios-name-server	Configure DNS servers for the DHCP pool.
netbios-node-type	Configure NetBios name servers for the DHCP pool.
domain-name	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
lease	Configure the domain name option (RFC 2132) for the DHCP pool.
deny-unknown-clients	Configure the maximum lease time for this DHCP pool.
show ip dhcp server	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp pool	Shows the DHCP server settings and status.
clear ip dhcp server	Shows the DHCP pool settings.
	Clear DHCP server leases database.

deny-unknown-clients

deny-unknown-clients

no deny-unknown-clients

Description

Configure this pool to deny DHCP requests to unknown clients.

Default

The default value is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCP pool and change it's behavior to deny DHCP request to unknown clients. Then it creates a fixed-address entry so that specific client can receive IP leases from the pool.

Ex.1 - **deny-unknown-clients** : This will create an address pool and set it's maximum lease time to 30 days.

```
DmSwitch(config)#ip dhcp pool test
DmSwitch(config-dhcp-pool-test)#network 192.168.0.0/24
DmSwitch(config-dhcp-pool-test)#deny-unknown-clients
DmSwitch(config-dhcp-pool-test)#exit
DmSwitch(config)#ip dhcp server
DmSwitch(config-dhcp-server)#enable
DmSwitch(config-dhcp-server)#fixed-address hostname name ip-address 192.168.0.100 mac-address 00:01:02:03:04:05
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ip dhcp server	Enables the DHCP server configuration mode.
enable	Enables the DHCP server globally.
excluded-address	Exclude addresses from DHCP pools.
fixed-address	Define host/ip mappings for DHCP pools.
ip dhcp pool	Enables the DHCP pool configuration mode.
network	Configure the prefix/mask for the DHCP pool.
default-router	Configure default routers for the DHCP pool.
dns-server	Configure DNS servers for the DHCP pool.
netbios-name-server	Configure NetBios name servers for the DHCP pool.
netbios-node-type	Configure the NetBios node type option (RFC 2132) for the DHCP pool.
domain-name	Configure the domain name option (RFC 2132) for the DHCP pool.
lease	Configure the maximum lease time for this DHCP pool.
deny-unknown-clients	Configure this pool to deny DHCP requests to unknown clients.
show ip dhcp server	Shows the DHCP server settings and status.
show ip dhcp pool	Shows the DHCP pool settings.
clear ip dhcp server	Clear DHCP server leases database.

Chapter 36. IPv6 DHCPv6 Server Commands

enable

enable

no enable

Description

Enables the DHCPv6 server globally.

Syntax

No parameter accepted.

Default

The default value is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.

Command	Description
<code>domain-search</code>	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
<code>show ipv6 dhcp server</code>	Shows the DHCPv6 server settings and status.
<code>show ipv6 dhcp pool</code>	Shows the DHCPv6 pool settings.

Chapter 37. IPv6 DHCPv6 Pool Commands

network

network *ipv6-prefix/prefix-length*

no network

Description

Configure the IPv6/prefix for the DHCPv6 pool.

Syntax

Parameter	Description
<i>ipv6-prefix/prefix-length</i>	Sets ipv6-prefix/prefix-length of the pool.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCPv6 pool prefix/mask.

Ex.1 - **network 2000::/64** : This will create a DHCPv6 pool, so the server can offer the configured options to hosts within 2000::/64 prefix.

```
DmSwitch(config)#ipv6 dhcp server
DmSwitch(config-dhcpv6-server)#enable
DmSwitch(config)#ipv6 dhcp pool test
DmSwitch(config-dhcpv6-pool-test)#network 2000::/64
```

```
DmSwitch(config-dhcpv6-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

sip-address

sip-address *ipv6-address* [**secondary**]

no sip-address *ipv6-address*

Description

Configure SIP addresses for the DHCPv6 pool. Option code 22 - RFC 3319.

Syntax

Parameter	Description
<i>ipv6-address</i>	The IPv6 address of the SIP Server.
secondary	Sets this address as secondary, so it will have lower preference.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCPv6 pool prefix/mask and it's SIP addresses.

Ex.1 - **sip-address 2000::1** : This will create a DHCPv6 pool and set it's primary and secondary sip-address.

```
DmSwitch(config)#ipv6 dhcp server
DmSwitch(config-dhcpv6-server)#enable
DmSwitch(config)#ipv6 dhcp pool test
DmSwitch(config-dhcpv6-pool-test)#network 2000::/64
DmSwitch(config-dhcpv6-pool-test)#sip-address 2000::1
DmSwitch(config-dhcpv6-pool-test)#sip-address 2000::2 secondary
DmSwitch(config-dhcpv6-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

sip-domain

sip-domain *name* [**secondary**]

no sip-domain *name*

Description

Configure SIP Domain Names for the DHCPv6 pool. Option code 21 - RFC 3319.

Syntax

Parameter	Description
<i>name</i>	The Domain Name of the SIP Server.
secondary	Sets this name as secondary, so it will have lower preference.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCPv6 pool prefix/mask and it's SIP Domain Names.

Ex.1 - **sip-domain** *a.sip.com* : This will create a DHCPv6 pool and set it's primary and secondary sip-domains.

```
DmSwitch(config)#ipv6 dhcp server
DmSwitch(config-dhcpv6-server)#enable
DmSwitch(config)#ipv6 dhcp pool test
DmSwitch(config-dhcpv6-pool-test)#network 2000::/64
DmSwitch(config-dhcpv6-pool-test)#sip-domain a.sip.com
DmSwitch(config-dhcpv6-pool-test)#sip-domain b.sip.com secondary
DmSwitch(config-dhcpv6-pool-test)#exit
```


You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

dns-server

dns-server *ipv6-address* [**secondary**]

no dns-server *ipv6-address*

Description

Configure DNS servers for the DHCPv6 pool. Option code 23 - RFC 3646.

Syntax

Parameter	Description
<i>ipv6-address</i>	The IPv6 address of the server.
secondary	Sets this address as secondary, so it will have lower preference.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCPv6 pool prefix/mask and it's DNS servers.

Ex.1 - **dns-server 2000::1** : This will create a DHCPv6 pool and set it's primary and secondary dns-servers.

```
DmSwitch(config)#ipv6 dhcp server
DmSwitch(config-dhcpv6-server)#enable
DmSwitch(config)#ipv6 dhcp pool test
DmSwitch(config-dhcpv6-pool-test)#network 2000::/64
DmSwitch(config-dhcpv6-pool-test)#dns-server 2000::1
DmSwitch(config-dhcpv6-pool-test)#dns-server 2000::2 secondary
DmSwitch(config-dhcpv6-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

domain-name

domain-search *name*

no domain-search

Description

Configure the domain search option (RFC 3646) for the DHCPv6 pool.

Syntax

Parameter	Description
<i>name</i>	Sets domain search option of the pool.

Command Modes

Global configuration.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

The examples show how to configure a DHCPv6 pool and set its domain search option.

Ex.1 - **domain-search** *datacom.net* : This will create a DHCPv6 pool and set the domain search option to "datacom.net".

```
DmSwitch(config)#ipv6 dhcp server
DmSwitch(config-dhcpv6-server)#enable
DmSwitch(config)#ipv6 dhcp pool test
DmSwitch(config-dhcpv6-pool-test)#network 2000::/64
DmSwitch(config-dhcpv6-pool-test)#domain-search datacom.net
DmSwitch(config-dhcpv6-pool-test)#exit
```

You can verify the fill here by entering the **show this** command during the sequence edition.

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server configuration mode.
enable	Enables the DHCPv6 server globally.
ipv6 dhcp pool	Enables the DHCPv6 pool configuration mode.
network	Configure the IPv6/prefix for the DHCPv6 pool.
sip-address	Configure SIP addresses for the DHCPv6 pool.
sip-domain	Configure SIP domain names for the DHCPv6 pool.
dns-server	Configure DNS servers for the DHCPv6 pool.
domain-search	Configure the domain search option (RFC 3646) for the DHCPv6 pool.
show ipv6 dhcp server	Shows the DHCPv6 server settings and status.
show ipv6 dhcp pool	Shows the DHCPv6 pool settings.

Chapter 38. Key Commands

key-string

key-string *text*

no key-string

Description

Configures the text string for a key identifier.

The **no** command removes the configured key string.

Syntax

Parameter	Description
<i>text</i>	Specifies the text string for the key.

Default

No key string is configured.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Key configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to specify the text string for the key.

```
DmSwitch(config-keychain-key) #key-string string_test
DmSwitch(config-keychain-key) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
key chain name	Configures a key chain.
key id	Specifies a key identifier.
show running-config	Shows the current operating configuration.

Chapter 39. Keychain Commands

key *id*

key *id*

no key *id*

Description

Specifies a key identifier.

The **no** command removes the configured key identifier.

Syntax

Parameter	Description
<i>id</i>	Specifies the key identifier.

Default

No key identifier is configured.

Command Availability

Only on models with Layer 3 functionality.

Command Modes

Keychain configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a key for the keychain.

```
DmSwitch(config-keychain)#key 1
DmSwitch(config-keychain-key)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
key chain name	Configures a key chain.
key-string	Configures the text string for a key identifier.
show running-config	Shows the current operating configuration.

Chapter 40. Link-state Tracking

enable

enable

no enable

Description

Enables Link-State Tracking Group.

Syntax

No parameter accepted.

Default

no enable

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to enable a Link-State Tracking Group.

```
DmSwitch(config)#link-state-tracking 0
DmSwitch(config-lst-0)#enable
DmSwitch(config-lst-0)#
```

Related Commands

Command	Description
<code>show link-state-tracking</code>	Shows Link-State Tracking status.
<code>link-state-tracking</code>	Creates and configures a Link-State Tracking Group.
<code>set-member</code>	Adds an interface to a Link-State Tracking Group.

set-member

```
set-member {upstream | downstream} {ethernet [unit-number/] port-number |  
port-channel port-channel-number }
```

```
no set-member ethernet [unit-number/] port-number | port-channel  
port-channel-number
```

Description

Adds an interface to a Link-State Tracking Group.

Syntax

Parameter	Description
<i>upstream</i>	Adds the interface as an Upstream member
<i>downstream</i>	Adds the interface as a Downstream member
ethernet <i>port-number</i>	Interface ethernet to add to LST Group
port-channel <i>port-channel-number</i>	Port-channel to add to LST Group

Default

no enable

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.6	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to create a Link-State Tracking Group.

```
DmSwitch(config)#link-state-tracking 0  
DmSwitch(config-lst-0)#set-member upstream ethernet 2/2  
DmSwitch(config-lst-0)#set-member downstream port-channel 2
```

Related Commands

Command	Description
<code>show link-state-tracking</code>	Shows Link-State Tracking status.
<code>link-state-tracking</code>	Creates and configures a Link-State Tracking Group.
<code>enable</code>	Enables Link-State Tracking Group.

Chapter 41. Monitor Commands

destination

destination [*unit-number/*] *port-number*

no destination

Description

Configures the traffic monitoring destination interface.

Inserting **no** as a prefix for this command will remove monitor's destination interface.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>port-number</i>	Specifies the monitor destination unit (optional) and port.

Default

No monitoring destination is configured.

Command Modes

Monitor configuration.

Command History

Release	Modification
3.1	This command was introduced.
13.0	This command was moved to inside monitor configuration mode.

Usage Guidelines

Not available.

Example

This example shows how to configure a monitor destination port.

```
DmSwitch(config-monitor)#destination 1/2
DmSwitch(config-monitor)#
```

You can verify that the port was configured by entering the **show monitor** privileged EXEC command.

Related Commands

Command	Description
rspan (Monitor configuration)	Configures RSPAN over the traffic monitoring.
source (Monitor configuration)	Configures the traffic monitoring filtered sources.
monitor (Interface configuration)	Sets the interface as a monitoring source.
show monitor	Shows traffic monitoring configuration.
show running-config	Shows the current operating configuration.

rspan

rspan *vlan-id*

no rspan

Description

Configures Remote Switched Port Analyzer (RSPAN) over the traffic monitoring.

Inserting **no** as a prefix for this command will return configuration to the default value.

Syntax

Parameter	Description
<i>vlan-id</i>	Appends vlan-id to head of packet, allowing remote monitoring of this traffic. Feature is known as Remote SPAN, or RSPAN.

Default

No VLAN id is added to packet.

Limitations and differences between series

RSPAN is unavailable at DmSwitch 3000 series.

Command Modes

Monitor configuration.

Command History

Release	Modification
3.1	This command was introduced.
10.0	RSPAN was introduced.
13.0	This command was moved to inside monitor configuration mode.

Usage Guidelines

Not available.

Example

This example shows how to configure RSPAN.

```
DmSwitch(config-monitor)#rspan vlan 100
DmSwitch(config-monitor)#
```

You can verify that the RSPAN was configured by entering the **show monitor** privileged EXEC command.

Related Commands

Command	Description
destination (Monitor configuration)	Configures the traffic monitoring destination interface.
source (Monitor configuration)	Configures the traffic monitoring filtered sources.
monitor (Interface configuration)	Sets the interface as a monitoring source.
show monitor	Shows traffic monitoring configuration.
show running-config	Shows the current operating configuration.

source

source { **new** | **id** } **ethernet** *parameters* { **all** | **rx** | **tx** } **match** *parameters*

no source [**id**]

Description

Configures a filtered traffic monitoring source.

Inserting **no** as a prefix for this command without any ID will remove all monitor filtered sources. Using **no** with an ID will remove the specified monitor filtered source.

Syntax

Parameter	Description
new	Creates a filtered monitor source
id	Create/edit a filtered monitor by ID
ethernet [<i>unit-number/</i>] <i>port-number</i>	Sets the interface as a source of monitored traffic
ethernet range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Sets the interface range as a source of monitored traffic
all	Monitor all filtered traffic
rx	Monitor only received filtered traffic
tx	Monitor only transmitted filtered traffic
Match parameters	Sets a packet field to be monitored
802.1p <i>priority</i>	Specifies 802.1p priority value (for outer or single tag)
dscp <i>ip-dscp-value</i>	Specify IP DSCP field
vlan <i>vlan-id</i>	Specify single VLAN ID (outer/single tag)
vlan range <i>first-vlan-id last-vlan-id</i>	Specify range of VLAN ID (outer/single tag)

Default

No monitoring filtered source is configured.

Command Modes

Monitor configuration.

Command History

Release	Modification
---------	--------------

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a monitor filtered source.

```
DmSwitch(config-monitor)#source new ethernet range 1/2 1/4 rx match vlan 100 802.1p 5
DmSwitch(config-monitor)#
```

You can verify that the filtered monitor was configured by entering the **show monitor** privileged EXEC command.

Related Commands

Command	Description
destination	Configures the traffic monitoring destination interface.
rspan (Monitor configuration)	Configures RSPAN over the traffic monitoring.
monitor (Interface configuration)	Sets the interface as a monitoring source.
show monitor	Shows traffic monitoring configuration.
show running-config	Shows the current operating configuration.

Chapter 42. MPLS EXPL-PATH Commands

explicit-path identifier ^[1] ^[3] ^[6]

explicit-path identifier *identifier*

no explicit-path identifier *identifier*

Description

Specifies the explicit path identifier. Under this command context, hops will be defined via **tsp-hop** command (Please refer **tsp-hop** command for further configurations).

Inserting **no** as a prefix for this command will delete the specified explicit-path identifier.

Syntax

Parameter	Description
<i>identifier</i>	Identifier to be used for any RSVP tunnel that needs such a path. Range 1..65535.

Default

No default is defined.

Command Modes

MPLS EXPL-PATH configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the MPLS explicit path identifier.

```

DmSwitch(config)#mpls expl-path
DmSwitch(config-mpls-expl-path)#explicit-path identifier 3
DmSwitch(config-mpls-expl-path)#

DmSwitch(config)#mpls expl-path
DmSwitch(config-mpls-expl-path)#no explicit-path identifier 3
DmSwitch(config-mpls-expl-path)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls expl-path	Enters on Explicit Path Configuration Mode
description	Configures the description of the set of hops that belongs to an explicit path
tsp-hop	Configures individually each hop that belongs to an explicit path
tunnel mpls traffic-eng path-option explicit-path identifier	Configures the path-option index and the explicit path identifier
Configure a description for the explicit-path	Configures the path-option index and the explicit path identifier

description ^[1] ^[3] ^[6]

description *set name*

no description

Description

Configures the description of the set of hops that belongs to an explicit path

Inserting **no** as a prefix for this command will remove the description.

Syntax

Parameter	Description
<i>description</i>	Configure a description.

Default

No default is defined.

Command Modes

MPLS EXPL-PATH configuration.

Command History

Release	Modification
14.10	First release. Command introduced.

Usage Guidelines

Use **description** to define a description for the set of hops that belongs to the explicit path.

Examples

This example shows how to use the **description**.

```
DmSwitch(config)#mpls expl-path
DmSwitch(config-mpls-expl-path)#explicit-path identifier 3
DmSwitch(config-mpls-expl-path-3)#description CWB->POA
DmSwitch(config-mpls-expl-path-3)#tsp-hop 1 path-option 1 next-address ipv4 172.16.88.131 strict
DmSwitch(config-mpls-expl-path-3)#tsp-hop 2 path-option 1 next-address ipv4 172.16.90.65 strict
DmSwitch(config-mpls-expl-path-3)#tsp-hop 3 path-option 2 exclude-address ipv4 172.16.88.131 strict
DmSwitch(config-mpls-expl-path-3)#
```

```
DmSwitch(config)#mpls expl-path
DmSwitch(config-mpls-expl-path)#explicit-path identifier 3
DmSwitch(config-mpls-expl-path-3)#no description
DmSwitch(config-mpls-expl-path-3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls expl-path	Enters on Explicit Path Configuration Mode
explicit-path identifier	Configures an explicit path
tsp-hop	Configures individually each hop that belongs to an explicit path

tsp-hop ^[1] ^[3] ^[6]

```
tsp-hop hop-index path-option option-index {exclude-address | next-address}  
ipv4 ip-address {loose | strict} {remark} comment
```

```
no tsp-hop {hop-index | all | range first-index last-index}
```

Description

Configures hops that an MPLS tunnel passes through, or excludes hops from the tunnel path.

Hops are grouped into a path-option. Each explicit-path supports up to 8 different path options. Each explicit-path supports up to 32 tsp-hops.

Inserting **no** as a prefix for this command will remove the specified tsp-hop index.

Syntax

Parameter	Description
<i>hop-index</i>	Hop index. (Range: 1-32)
path-option <i>option-index</i>	path-option index.
exclude-address	Excludes the specified hop.
next-address	Includes the specified hop.
ipv4 <i>ip-address</i>	Hop IP address.
loose	Sets the hop as loose.
strict	Sets the hop as strict.
remark	Sets a hop comment.
all	Specifies all hops.
range <i>first-index</i> <i>last-index</i>	Specifies a range (1-32) of hops.

Default

No default is defined.

Command Modes

MPLS EXPL-PATH configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Use explicit-path configuration to define an ordered list of hops through which an MPLS tunnel must be routed.

Each explicit-path can have multiple path options. Each path option is a list of hops. To each hop is associated a rule to include or exclude it from the MPLS tunnel path.

A hop can be loose or strict. For loose hops, the IGP determines a route from the tunnel headend to the first loose hop in the path-option list, or from one loose hop to the next.

For strict hops, they identify a segment of the path, in the right order and without gaps, that an MPLS tunnel must be routed through.

Examples

This example shows how to configure the hops for an specific explicit path.

```
DmSwitch(config)#mpls expl-path
DmSwitch(config-mpls-expl-path)#explicit-path identifier 3
DmSwitch(config-mpls-expl-path-3)#description CWB->POA
DmSwitch(config-mpls-expl-path-3)#tsp-hop 1 path-option 1 next-address ipv4 1.1.8.1 strict remark FLO
DmSwitch(config-mpls-expl-path-3)#tsp-hop 2 path-option 1 next-address ipv4 1.1.9.6 strict remark CXS
DmSwitch(config-mpls-expl-path-3)#tsp-hop 3 path-option 2 exclude-address ipv4 1.1.8.3 strict remark POA
DmSwitch(config-mpls-expl-path-3)#

DmSwitch(config)#mpls expl-path
DmSwitch(config-mpls-expl-path)#explicit-path identifier 3
DmSwitch(config-mpls-expl-path-3)#no tsp-hop 3
DmSwitch(config-mpls-expl-path-3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls expl-path	Enters on Explicit Path Configuration Mode
explicit-path identifier	Configures an explicit path
tunnel mpls traffic-eng path-option explicit-path identifier	Configures the path-option index and the explicit path identifier
description	Configures the description of the set of hops that belongs to an explicit path

Chapter 43. MPLS RSVP Commands

mpls traffic-eng fast-reroute revertive global ^[1] ^[3] ^[6]

```
mpls traffic-eng fast-reroute revertive global
```

```
no mpls traffic-eng fast-reroute revertive global
```

Description

Configures data plane to revert traffic from backup tunnel to protected tunnel once it is operational again.

Inserting **no** as a prefix for this command will disable fast-reroute revertive behavior.

Syntax

No parameter accepted.

Default

By default the Global Revertive Behavior is enabled.

Command Modes

MPLS RSVP Global configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

The revertive behavior is used together with the FRR (Fast Reroute). In case of link or node failures data packets will be forwarded via backup path (Facility N:1 or Detour 1:1). If global revertive is enabled, data packets will return to be forwarded by the protected LSP. Otherwise, traffic will remain in the backup LSP despite the fact that the protected LSP become operational again.

Example

This example shows how to enable and disable the Global Revertive behavior.

```
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#mpls traffic-eng fast-reroute revertive global
```

```

DmSwitch(config-mpls-rsvp) #

DmSwitch(config) #mpls rsvp
DmSwitch(config-mpls-rsvp) #no mpls traffic-eng fast-reroute revertive global
DmSwitch(config-mpls-rsvp) #

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
rsvp enable	Enables RSVP protocol
signalling hello graceful-restart	Enables RSVP hello graceful restart indication
signalling refresh interval	Configures the interval at which RSVP messages (PATH/RESV) are sent to each neighbor
signalling refresh misses	Configures the number of missed RSVP messages (PATH/RESV) before making neighbor down
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

signalling refresh interval ^[1] ^[3] ^[6]

signalling refresh interval *milliseconds*

no signalling refresh interval

Description

Configures globally average interval between refresh PATH and RESV messages.

Inserting **no** as a prefix for this command will restore the default value.

Syntax

Parameter	Description
<i>milliseconds</i>	Refresh interval. Values in milliseconds (1-60000)

Default

The default value is 30000 ms.

Command Modes

MPLS RSVP Global configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the Refresh Interval in the rsvp global mode.

```
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#signalling refresh interval 10000
DmSwitch(config-mpls-rsvp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mpls traffic-eng fast-reroute revertive global</code>	Globally enables fast-reroute revertive behavior
<code>rsvp enable</code>	Enables RSVP protocol
<code>signalling hello graceful-restart</code>	Enables RSVP hello graceful restart indication
<code>signalling refresh misses</code>	Configures the number of missed RSVP messages (PATH/RESV) before making neighbor down
<code>show mpls rsvp</code>	Show counters of RSVP messages
<code>show mpls te traffic-eng tunnels</code>	Shows Traffic Engineering Tunnel Information

signalling refresh misses ^[1] ^[3] ^[6]

signalling refresh misses *number*

no signalling refresh misses

Description

Configures the number of unresponded PATH or RESV refresh attempts which must be made, spaced by the refresh interval before the neighbor is considered to be down.

Inserting **no** as a prefix for this command will restore the default value.

Syntax

Parameter	Description
<i>number</i>	Number of missed RSVP messages (1-10)

Default

The default value is 3.

Command Modes

MPLS RSVP Global configuration.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the Hello Refresh Interval.

```
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#signalling refresh misses 1
DmSwitch(config-mpls-rsvp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mpls traffic-eng fast-reroute revertive global</code>	Globally enables fast-reroute revertive behavior
<code>rsvp enable</code>	Enables RSVP protocol
<code>signalling hello graceful-restart</code>	Enables RSVP hello graceful restart indication
<code>signalling refresh interval</code>	Configures the interval at which RSVP messages (PATH/RESV) are sent to each neighbor
<code>show mpls rsvp</code>	Show counters of RSVP messages
<code>show mpls te traffic-eng tunnels</code>	Shows Traffic Engineering Tunnel Information

Chapter 44. MPLS TE Commands

interface te-tunnel [1] [3] [6]

```
interface te-tunnel tunnelId
```

```
no interface te-tunnel {tunnelId | range first_tnl_idx last_tnl_idx}
```

Description

Enters on Tunnel Configuration Mode.

Inserting **no** as a prefix for this command will remove a single tunnel or a range of tunnels.

Syntax

Parameter	Description
<i>tunnelId</i>	Tunnel Identifier.
range <i>first_tnl_idx</i> <i>last_tnl_idx</i>	Tunnel index range to be deleted.

Default

No default is defined.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to enter on the configuration mode and how to delete an RSVP tunnel.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#no interface te-tunnel 10
DmSwitch(config-mpls-te)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls destination ^[1] ^[3] ^[6]

tunnel mpls destination *ip-address*

no tunnel mpls destination *ip-address*

Description

Configures the RSVP tunnel egress (destination).

Inserting **no** as a prefix for this command will delete the RSVP tunnel destination.

Syntax

Parameter	Description
destination <i>ip-address</i>	Tunnel Egress IP Address

Default

No default is defined.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the RSVP tunnel egress.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls destination 10.1.3.51
DmSwitch(config-mpls-te-if-10)#
```

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls destination 10.1.3.51
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng affinity ^[1] ^[3] ^[6]

tunnel mpls traffic-eng affinity *include-any include-all exclude-any*

no tunnel mpls traffic-eng affinity

Description

Configures the affinity (the properties the tunnel requires in its links) for an RSVP tunnel.

Inserting **no** as a prefix for this command will revert affinity configuration.

Syntax

Parameter	Description
<i>include-any</i>	A link satisfies the include-any constraint if and only if the constraint is zero (in the tunnel-te), or the link and the constraint have any administrative groups in common. (Range: 0-4294967295)
<i>include-all</i>	A link satisfies the include-all constraint if and only if the link contains all of the administrative groups specified in the constraint. (Range: 0-4294967295)
<i>exclude-any</i>	A link satisfies the exclude-any constraint if and only if the link contains none of the administrative groups specified in the constraint. (Range: 0-4294967295)

Default

No default is defined.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the RSVP Tunnel affinity.

```

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng affinity 1 0 0
DmSwitch(config-mpls-te-if-10)#

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng affinity
DmSwitch(config-mpls-te-if-10)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng autoroute announce ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng autoroute announce
```

```
no tunnel mpls traffic-eng autoroute announce
```

Description

Allows the Interior Gateway Protocol (IGP) to use the tunnel as a point-to-point link between tunnel headend and tailend.

Inserting **no** as a prefix for this command will revert tunnel announcement configuration.

Syntax

No parameter accepted.

Default

By default the autoroute announce is disabled.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

If OSPF is being used as the IGP, the tunnel is considered by the enhanced Shortest Path First (SPF) calculation and advertised as a point-to-point link between tunnel headend and tailend.

Example

This example shows how to enable and disable the autoroute announce.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng autoroute announce
DmSwitch(config-mpls-te-if-10)#

DmSwitch(config)#mpls te
```

```
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng autoroute announce
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng autoroute metric ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng autoroute metric absolute metric
```

```
no tunnel mpls traffic-eng autoroute metric
```

Description

Configures the metric assigned to the tunnel into Interior Gateway Protocol (IGP).

Inserting **no** as a prefix for this command will revert metric configuration.

Syntax

Parameter	Description
<i>metric</i>	Absolute metric value for RSVP tunnel (1..7)

Default

The default metric is 1.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

If OSPF is being used as the IGP, the tunnel is considered by the enhanced Shortest Path First (SPF) calculation and advertised as a point-to-point link between tunnel headend and tailend.

Example

This example shows how to configure and revert the metric assigned to the tunnel within IGP.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng autoroute metric absolute 5
DmSwitch(config-mpls-te-if-10)#
```



```

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng autoroute metric
DmSwitch(config-mpls-te-if-10)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng bandwidth ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng bandwidth bandwidth
```

```
no tunnel mpls traffic-eng bandwidth bandwidth
```

Description

Defines the traffic characteristics of a sender data flow required in a Path message (SENDER_TSPEC RFC2205, Object Formats). The RSVP SENDER_TSPEC object carries information about a data source generated traffic. The required RSVP SENDER_TSPEC object contains a global TOKEN_BUCKET_TSPEC parameter (RFC2215). This TSPEC carries traffic information usable by either the Guaranteed or Controlled-Load QoS control services.

Inserting **no** as a prefix for this command will restore the default values.

Syntax

Parameter	Description
<i>bandwidth</i>	Bandwidth value in Kbps

Default

Bandwidth value is 0 Kbps.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the RSVP tunnel bandwidth.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
```

```

DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng bandwidth 1000
DmSwitch(config-mpls-te-if-10)#

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng bandwidth 1000
DmSwitch(config-mpls-te-if-10)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng igp ospf area

```
tunnel mpls traffic-eng igp ospf area area
```

```
no tunnel mpls traffic-eng area
```

Description

Defines the OSPF area associated with the RSVP tunnel. This will enable the tunnel to be announced on the configured area.

Inserting **no** as a prefix for this command will remove the OSPF area configuration from the RSVP tunnel. The tunnel will then belong to the OSPF area its source loopback interface belongs to.

Syntax

Parameter	Description
<i>area</i>	OSPF area ID (as number or in IP notation).

Default

Announces the RSVP tunnel as route in the same area as the source loopback address with **mpls enable**.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
12.6	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the OSPF area for the RSVP tunnel.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#shutdown
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng igp ospf area 10
DmSwitch(config-mpls-te-if-10)#no shutdown
```

```

DmSwitch(config-mpls-te-if-10) #

DmSwitch(config) #mpls te
DmSwitch(config-mpls-te) #interface te-tunnel 10
DmSwitch(config-mpls-te-if-10) #shutdown
DmSwitch(config-mpls-te-if-10) #tunnel mpls traffic-eng igp ospf area 0.0.0.10
DmSwitch(config-mpls-te-if-10) #no shutdown
DmSwitch(config-mpls-te-if-10) #

DmSwitch(config) #mpls te
DmSwitch(config-mpls-te) #interface te-tunnel 10
DmSwitch(config-mpls-te-if-10) #shutdown
DmSwitch(config-mpls-te-if-10) #no tunnel mpls traffic-eng igp ospf area
DmSwitch(config-mpls-te-if-10) #no shutdown
DmSwitch(config-mpls-te-if-10) #

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng fast-reroute ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng fast-reroute one-to-one [bw-prot bandwidth]
[node-prot] [priority setup_prio hold_prio] [hop-limit number_hops]
[affinity include-any include-all exclude-any]
```

```
no tunnel mpls traffic-eng fast-reroute
```

Description

Enables the creation of alternative paths (known as detour or bypass paths depending on the chosen mode) allowing data traffic to be immediately (within 50 milliseconds) moved from a protected path in case of failures. The backup path is deployed based on CSPF calculation and is link and node disjoint.

The Fast-Reroute feature (FRR) is fully described by RFC4090.

Inserting **no** as a prefix for this command will disable Fast-Reroute configuration.

Syntax

Parameter	Description
one-to-one	Activates Fast-Reroute Detour mode.
bw-prot <i>bandwidth</i>	Bandwidth to be protected in kbps.
node-prot	Enables node protection.
priority <i>setup_prio</i> <i>hold_prio</i>	The setup priority and hold priority for the backup tunnel.
hop-limit <i>number_hops</i>	The maximum number of extra hops the backup path is allowed to take, from current Point of Local Repair (PLR) node to an Merge Point (MP) node, with PLR and MP excluded from the count. For example, hop-limit of 0 means that only direct links between PLR and MP can be considered.
affinity <i>include-any</i> <i>include-all</i> <i>exclude-any</i>	Configures the affinity for the backup tunnel. An integer from 0 to 65535. A link satisfies the include-any constraint if and only if the constraint is zero, or the link and the constraint have a resource class in common. An integer from 0 to 65535. A link satisfies the include-all constraint if and only if the link contains all of the administrative groups specified in the constraint. An integer from 0 to 65535. A link satisfies the exclude-any constraint if and only if the link contains none of the administrative groups specified in the constraint.

Default

No Fast-Reroute mode is configured.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Record-route is mandatory for Fast-Reroute.

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the Hello Refresh Interval.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng fast-reroute one-to-one
DmSwitch(config-mpls-te-if-10)#
```

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng fast-reroute
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel

Command	Description
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng path-option ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng path-option path_option explicit-path identifier  
identifier
```

```
no tunnel mpls traffic-eng path-option path_option explicit-path  
identifier identifier
```

Description

Associates to the specified tunnel a path option set, which fully or partially configures hops along the tunnel.

Inserting **no** as a prefix for this command will revert configuration.

Syntax

Parameter	Description
<i>path_option</i>	Path option number.
<i>identifier</i>	Explicit-path identifier defined prior to this command.

Default

No default value is defined.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.
15.2	Increased number of path options per tunnel.

Usage Guidelines

Explicit Path must be defined first. Please refer command **explicit-path identifier**.

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Up to four different path options can be associated with the same RSVP tunnel. The priority among them is the creation sequence.

Example

This example shows how to associate the path-option of an explicit identifier to the RSVP tunnel.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng path-option 1 explicit-path identifier 4
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng path-option 2 explicit-path identifier 4
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng path-option 3 explicit-path identifier 4
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng path-option 4 explicit-path identifier 4
DmSwitch(config-mpls-te-if-10)#

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng path-option 1 explicit-path identifier 4
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls expl-path	Configures an explicit path
tsp-hop	Configures individually each hop that belongs to an explicit path
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng priority ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng priority setup_prio hold_prio
```

```
no tunnel mpls traffic-eng priority
```

Description

Configures setup priority and hold priority for the specified tunnel.

Inserting **no** as a prefix for this command will restore the default values.

Syntax

Parameter	Description
<i>setup_prio</i>	Setup priority of protected tunnel. Range: 0-7.
<i>hold_prio</i>	Holding priority of protected tunnel. Range: 0-7.

Default

The default RSVP tunnel setup and hold priority is 0.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the RSVP tunnel priority.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng priority 3 3
DmSwitch(config-mpls-te-if-10)#
```

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng priority
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel mpls traffic-eng record-route ^[1] ^[3] ^[6]

```
tunnel mpls traffic-eng record-route
```

```
no tunnel mpls traffic-eng record-route
```

Description

It allows the routes used by a tunnel to be recorded via the RECORD_ROUTE object (RFC3209, RRO). Labels are also recorded.

Inserting **no** as a prefix for this command will remove the configuration.

Syntax

No parameter accepted.

Default

By default the record route is enabled.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Record-route is used for loop detection and is mandatory when Fast-Reroute is in use.

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the Record Route.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng record-route
DmSwitch(config-mpls-te-if-10)#
```

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
```

```
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng record-route
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

tunnel name ^[1] ^[3] ^[6]

tunnel name *name*

no tunnel name

Description

Configures the RSVP tunnel name

Inserting **no** as a prefix for this command will delete the RSVP tunnel name.

Syntax

Parameter	Description
<i>name</i>	Tunnel name with maximum of 20 characters.

Default

No default is defined.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the RSVP tunnel name.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel name DMSwitch_T10
DmSwitch(config-mpls-te-if-10)#
```

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
```

```
DmSwitch(config-mpls-te-if-10)#no tunnel name
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

shutdown ^[1] ^[3] ^[6]

shutdown

no shutdown

Description

Disables administratively an RSVP tunnel for maintenance purposes. All services and traffic associated to the specified tunnel will be disabled.

Inserting **no** as a prefix for this command will turn the tunnel administrative state to UP, reestablishing the services.

Syntax

No parameter accepted.

Default

By default the RSVP tunnel administrative status is down (shutdown).

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the RSVP tunnel administrative status.

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#shutdown
DmSwitch(config-mpls-te-if-10)#
```

```
DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no shutdown
DmSwitch(config-mpls-te-if-10)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng bypass	Configures the RSVP Tunnel as a bypass tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

Chapter 45. MPLS VPWS Commands

vpn [1] [3] [6]

```
vpn id [enable | disable]
```

```
vpn new [enable | disable]
```

```
vpn all {enable | disable}
```

```
vpn range id1 id2 {enable | disable}
```

```
no vpn { id | range id1 id2 | all }
```

Description

Create, disable or enable a VPWS VPN.

Inserting **no** as prefix for this command will delete the VPWS VPN.

Syntax

Parameter	Description
<i>id</i>	VPN number.(Range: 1-Depends on board)
enable	Enable the VPN <i>id</i> if it was already created or create the VPN <i>id</i> enabled.
disable	Disable the VPN <i>id</i> if it was already created or create the VPN <i>id</i> disabled.
range <i>id1 id2</i>	Initial and end VPWS VPN's numbers in the range to be enabled, disabled or deleted. (Range: 1-Depends on board)
all	All configured VPWS VPN's can be deleted, enabled or disabled.

Default

Default value is *enabled* in VPWS VPN creation.

Command Modes

MPLS VPWS configuration.

Command History

Release	Modification
10.0	These commands were introduced.

Usage Guidelines

To use this command, the equipment must support MPLS feature. When using range of VPN id's, the affected VPNs are the same type of current configuration mode. Disabling a VPN, or range of VPNs, their PW status will go to admin down.

Example

This example shows how to create a VPWS VPN.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-vpws)#vpn new
% VPN 1 is being created...
DmSwitch(config-vpws-vpn-1)#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.

name [1] [3] [6]

name *text*

no name

Description

Set the VPWS VPN name.

Inserting **no** as prefix for this command will delete the VPWS VPN name.

Syntax

Parameter	Description
<i>text</i>	The VPN name.(Max:32 chars)

Default

No default is defined.

Command Modes

MPLS VPWS VPN configuration.

Command History

Release	Modification
10.0	The VPN name was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS feature.

Example

This example shows how to set VPWS VPN name.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-vpws)#vpn 1
DmSwitch(config-vpws-vpn-1)#name CWB-RT-3
DmSwitch(config-vpws-vpn-1)#
```

You can verify the VPN name configured by entering the **show running-config** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.

xconnect vlan ^[1] ^[3] ^[6]

```
xconnect vlan id [access-interface { local-tunnel endpoint {1|2}[5][7] | ethernet  
[unit/]port | port-channel port-channel_num | pwe3[9] | ptp[9] } ] [vc-type {ethernet |  
vlan} ]
```

```
no xconnect vlan id
```

Description

Creates an Attachment Circuit (AC) for the VPWS VPN.

Inserting **no** as prefix for this command will delete the attachment circuit of VPWS VPN.

Syntax

Parameter	Description
vlan <i>id</i>	VLAN <i>id</i> of attachment circuit (AC).
access-interface	Specify access interface when VPWS access VLAN has more than one port member.
local-tunnel endpoint ^[5] ^[7] <i>{1 2}</i>	Specify Local-tunnel endpoint interface to be used as VPWS access port.
ptp	VLAN is connected to a CESoP/PTP interface
pwe3	VLAN is connected to a CESoP/PWE3 interface
ethernet <i>[unit/]port</i>	Specify Ethernet interface to be used as VPWS access port.
port-channel <i>port-channel_num</i>	Specify port-channel interface to be used as VPWS access port.
vc-type	Specify the VC type of attachment circuit.
ethernet	VC type is Ethernet.
vlan	VC type is VLAN.

Default

The **vc-type** default value is **vlan**.

Command Modes

MPLS VPWS VPN configuration.

Command History

Release	Modification
9.0	This command was introduced.
10.0	The vc-type parameter was introduced.
11.2	The access-interface parameter was introduced.

Release	Modification
13.0	The local-tunnel endpoint parameter was introduced.
13.2	Parameters ptp and pwe3 were introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS feature. The VPN attachment circuit (VLAN) must have only one interface Ethernet or port-channel, unless **access-interface** is configured. To delete an attachment circuit of VPWS VPN, you must delete all neighbors or disable the VPN first.

Example

This example shows how to create an attachment circuit for VPWS VPN.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-vpws)#vpn 1
DmSwitch(config-vpws-vpn-1)#xconnect vlan 100
DmSwitch(config-vpws-vpn-1)#
```

The example above the vc-type is not specified. In this case the default value **vlan** is assumed.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-vpws)#vpn 1
DmSwitch(config-vpws-vpn-1)#xconnect vlan 100 vc-type ethernet
DmSwitch(config-vpws-vpn-1)#
```

The example above the vc-type is **ethernet** and all PWs are configured with this parameter (protocol signalization exchange this information). Configuring this parameter could be useful for interoperability issues with others vendors.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.

neighbor ^[1] ^[3] ^[6]

```
neighbor ip-address { pwid number | pwidfec pwid number groupid number mplstype  
[ non-te | te-tunnel tunnelId ] }
```

```
no neighbor ip-address { pwid number | pwidfec pwid number groupid number }
```

Description

Configures a VPWS with the specified neighbor.

Inserting **no** as a prefix for this command will remove the circuit from configuration.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the peer IP address.
pwid <i>number</i>	Specifies the PW ID that identifies this particular circuit.
groupid <i>number</i>	Specifies the Group ID that the circuit belongs to.
mplstype	Specifies the LSP encapsulation type of the circuit.
non-te	The circuit will be encapsulated by LSPs created via LDP.
te-tunnel <i>tunnelId</i>	The circuit will be encapsulated by LSPs created via RSVP, the tunnelId must be specified.

Default

No default is defined.

Command Modes

MPLS VPWS VPN configuration.

Command History

Release	Modification
8.0	This command was introduced.
11.2	The command was splitted in several subcommands.

Usage Guidelines

In MPLS VPWS configuration mode the user can create VPWS circuits according to RFC 4447. After having specified the attachment circuit with **xconnect vlan** command, the user should enter this **neighbor** command that specifies not only the peer to establish the circuit with, but also the PWid FEC Element attributes

which identifies the circuit. On this level more options for the neighbor configuration are available.

Example

This example shows how to enter in MPLS VPWS configuration mode and create a VPWS mplstype te with peer 10.1.14.53.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#xconnect vlan 100
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 10.1.14.53 pwid 153 mplstype te-tunnel 12
DmSwitch(config-mpls-vpws-vpn-1-pwid-153)#no shutdown
```

The following example shows an alternate method, mplstype non-te, of configuring a peer.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 2000
DmSwitch(config-mpls-vpws-vpn-2000)#xconnect vlan 100
DmSwitch(config-mpls-vpws-vpn-2000)#neighbor 10.1.14.53 pwidfec pwid 153 groupid 0 mplstype non-te
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpws	Configure Virtual Private Wire Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
xconnect vlan	Creates an access VLAN interface for the VPWS VPN.
backup-peer	Configures the backup peer for a primary VPN neighbor.
backup-delay	Configures a backup delay for a VPN backup VC.
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode

mplstype ^[1] ^[3] ^[6]

mplstype [**non-te** | **te-tunnel** *tunnelId*]

Description

This command specifies the VC encapsulation type to be used with a VPN neighbor.

Syntax

Parameter	Description
non-te	Specifies that the circuit will be encapsulated by LSPs created via LDP.
te-tunnel <i>tunnelId</i>	Specifies that the circuit will be encapsulated by LSPs created via RSVP. The <i>tunnelId</i> must be configured.

Default

non-te type.

Command Modes

MPLS VPWS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPWS VPN PWID configuration mode and configure the VC encapsulation type.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#xconnect vlan 50
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 100.100.100.1 pwid 1 mplstype non-te
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#no shutdown
DmSwitch(config-mpls-vpws)#vpn 2
DmSwitch(config-mpls-vpws-vpn-2)#xconnect vlan 100
DmSwitch(config-mpls-vpws-vpn-2)#neighbor 10.1.14.53 pwid 153 mplstype te-tunnel 12
DmSwitch(config-mpls-vpws-vpn-2-pwid-153)#backup-peer 100.100.100.2 pwid 2 mplstype te-tunnel 15
DmSwitch(config-mpls-vpws-vpn-2-pwid-153)#no shutdown
```

```
DmSwitch(config-mpls-vpws)#vpn 3
DmSwitch(config-mpls-vpws-vpn-3)#xconnect vlan 200
DmSwitch(config-mpls-vpws-vpn-3)#neighbor 10.1.14.53 pwid 154 mpls type non-te
DmSwitch(config-mpls-vpws-vpn-3-pwid-154)#backup-peer 100.100.100.7 pwid 7 mpls type non-te
DmSwitch(config-mpls-vpws-vpn-3-pwid-154)#no shutdown
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpws	Configure Virtual Private Wire Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
neighbor	Configures a VPWS with the specified neighbor.
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode

backup-peer [1] [3] [6]

backup-peer *ip-address* **pwid** *number* **mplstype** [**non-te** | **te-tunnel** *tunnelId*]

no backup-peer

Description

This command specifies a redundant peer for a primary VPN neighbor. The **mplstype** must be from same type for the neighbor and backup-peer.

Inserting **no** as a prefix for this command will remove the backup peer configuration from neighbor.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the backup peer IP address.
pwid <i>number</i>	Specifies the PW ID that identifies this particular circuit.
mplstype	Specifies the LSP encapsulation type of the circuit.
non-te	The circuit will be encapsulated by LSPs created via LDP.
te-tunnel <i>tunnelId</i>	The circuit will be encapsulated by LSPs created via RSVP, the <i>tunnelId</i> must be specified.

Default

No default is defined.

Command Modes

MPLS VPWS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPWS VPN PWID configuration mode and create a backup peer.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 100.100.100.1 pwid 1
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#backup-peer 100.100.100.2 pwid 2 mplstype non-te
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#
DmSwitch(config-mpls-vpws)#vpn 2
DmSwitch(config-mpls-vpws-vpn-2)#xconnect vlan 100
DmSwitch(config-mpls-vpws-vpn-2)#neighbor 10.1.14.53 pwid 153 mplstype te-tunnel 12
DmSwitch(config-mpls-vpws-vpn-2-pwid-153)#backup-peer 100.100.100.2 pwid 2 mplstype te-tunnel 15
DmSwitch(config-mpls-vpws-vpn-2-pwid-153)#no shutdown
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpws	Configure Virtual Private Wire Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
neighbor	Configures a VPWS with the specified neighbor.
backup-delay	Configures a backup delay for a VPN backup VC.
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode

backup-delay ^[1] ^[3] ^[6]

backup-delay *switchover-delay* { **never** | *revertive-delay* }

no backup-delay

Description

Specifies how long the backup PW VC should wait before executing a switchover or switchback operation, in response to a state change (from Up to Down or Down to Up, respectively) of the active PW VC.

Inserting **no** as a prefix for this command will remove the backup delay configuration from neighbor.

Syntax

Parameter	Description
<i>switchover-delay</i>	Specifies the delay for the switchover between active and backup PW VC. Value in seconds (0-180).
never	The secondary PW VC does not switch back to the primary PW VC if the primary PW VC becomes available again, unless the secondary PW VC fails.
<i>revertive-delay</i>	Specifies the revertive delay for the PW VC to switch back to the primary PW VC if the primary PW VC becomes available again.

Default

The default value is *switchover-delay* 0 and *revertive-delay* 0.

Command Modes

MPLS VPWS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPWS VPN PWID configuration mode and create a backup peer,

as well as configure it's delay and mode parameters.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 100.100.100.1 pwid 1
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#backup-peer 100.100.100.2 pwid 2
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#backup-delay 50 never
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#backup-delay 50 15
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpws	Configure Virtual Private Wire Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
neighbor	Configures a VPWS with the specified neighbor.
backup-peer	Configures the backup peer for a primary VPN neighbor.

vlanmode [1] [3] [6]

vlanmode changevlan *vlan*

no vlanmode changevlan *vlan*

Description

This command changes the internal VLAN identifier of encapsulated access VPN packets.

Syntax

Parameter	Description
<i>vlan</i>	VLAN ID

Default

No default is defined.

Command Modes

MPLS VPWS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPWS VPN PWID configuration mode and configure the internal VLAN identifier of an VC encapsulated packet for a specified neighbor.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 100.100.100.1 pwid 1
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#vlanmode changevlan 200
DmSwitch(config-mpls-vpws-vpn-1-pwid-1)#
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mpls vpws</code>	Configure Virtual Private Wire Service.
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.
<code>show running-config</code>	Shows the current operating configuration.
<code>neighbor</code>	Configures a VPWS with the specified neighbor.

statistics [1] [2] [3] [4] [5] [6] [7]

statistics

no statistics

Description

Enables statistics on the VPWS VPN, allowing usage of L2VPN counters.

Inserting **no** as prefix for this command will disable statistics on the VPWS VPN.

Default

statistics is disabled by default.

Command Modes

MPLS VPWS VPN configuration.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

On DM4100 Enduro, statistics must be enabled on a VPN in order to check its L2VPN counters (due to hardware restrictions, only RX counters are available). Whenever this command is enabled on a VPN, hardware resources (filters and counters) are consumed proportionately to the number of ports of the VPN. For that reason, it's recommended to only activate it during L2VPN troubleshooting. This command might fail in a system where a great amount of filters and/or counters are configured. In such case, a few filters and/or counters must be deleted from the system configuration in order to allow the proper operation of the command.

Example

This example shows how to activate statistics on a VPWS VPN.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-vpws)#vpn 1
DmSwitch(config-vpws-vpn-1)#statistics
DmSwitch(config-vpws-vpn-1)#
```

Related Commands

Command	Description
<code>statistics</code>	Enables statistics on the VPLS VPN.
<code>show running-config</code>	Shows the current operating configuration.
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.

exp-ingress-mapping ^[1] ^[3] ^[6]

exp-ingress-mapping

no exp-ingress-mapping

Description

The command **exp-ingress-mapping** enables the use of MPLS EXP to PRI Ingress mapping table rules to be followed. This is the default system option. The command **no exp-ingress-mapping** disables the use of MPLS EXP to PRI Ingress mapping table rules. This is needed when QoS egress filtering rules are associated with VPN access ports and/or local-tunnels.

Default

exp-ingress-mapping is enabled by default.

Command Modes

MPLS VPWS configuration.

Command History

Release	Modification
15.2.2	This command was introduced.

Usage Guidelines

Create a VPN first **neighbor** command.

Example

The examples below show how to enter in MPLS VPWS VPN configuration mode and disable/enable the EXP to PRI Ingress mapping mode.

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#no exp-ingress-mapping
DmSwitch(config-mpls-vpws-vpn-1)#xconnect vlan 100 vc-type vlan
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 200.200.200.1 pwid 12 mplstype non-te
DmSwitch(config-mpls-vpws-vpn-1-pwid-12)#no shutdown
```

```
DmSwitch(config)#mpls vpws
DmSwitch(config-mpls-vpws)#vpn 1
DmSwitch(config-mpls-vpws-vpn-1)#exp-ingress-mapping
DmSwitch(config-mpls-vpws-vpn-1)#xconnect vlan 100 vc-type vlan
DmSwitch(config-mpls-vpws-vpn-1)#neighbor 200.200.200.1 pwid 12 mplstype non-te
DmSwitch(config-mpls-vpws-vpn-1-pwid-12)#no shutdown
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpws	Configure Virtual Private Wire Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
filter	Creates or configures a traffic filter
meter	Configures a meter to be used by a filter
mpls exp-map egress	Configures the table mapping for COS priority to EXP egress packets.
mpls exp-map ingress	Configures the table mapping for EXP to COS priority ingress packets.
show mpls exp-map ingress	Shows MPLS EXP to COS priority mapping table for ingress packets.
show mpls exp-map egress	Shows MPLS COS priority to EXP mapping table for egress packets.

Chapter 46. MPLS VPLS Commands

vpn [1] [3] [6]

```
vpn id [enable | disable]
```

```
vpn new [enable | disable]
```

```
vpn all {enable | disable}
```

```
vpn range id1 id2 {enable | disable}
```

```
no vpn { id | range id1 id2 | all }
```

Description

Create, disable or enable a VPLS VPN.

Inserting **no** as prefix for this command will delete the VPLS VPN.

Syntax

Parameter	Description
<i>id</i>	VPN number.(Range: 1-Depends on board)
enable	Enable the VPN <i>id</i> if it was already created or create the VPN <i>id</i> enabled.
disable	Disable the VPN <i>id</i> if it was already created or create the VPN <i>id</i> disabled.
range <i>id1 id2</i>	Initial and end VPLS VPN's numbers in the range to be enabled, disabled or deleted.(Range: 1-Depends on board)
all	All configured VPLS VPN's can be deleted, enabled or disabled.

Default

Default value is *enabled* in VPLS VPN creation.

Command Modes

MPLS VPLS configuration.

Command History

Release	Modification
10.0	These commands were introduced.

Usage Guidelines

To use this command, the equipment must support MPLS/VPLS feature. When using range of VPN id's, the affected VPNs are the same type of current configuration mode. Disabling a VPN, or range of VPNs, their PW status will go to admin down.

Example

This example shows how to create a VPLS VPN.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#vpn new
% VPN 1 is being created...
DmSwitch(config-vpls-vpn-1)#
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.

name [1] [3] [6]

name *text*

no name

Description

Set the VPLS VPN name.

Inserting **no** as prefix for this command will delete the VPLS VPN name.

Syntax

Parameter	Description
<i>text</i>	The VPN name.(Max:32 chars)

Default

No default is defined.

Command Modes

MPLS VPLS VPN configuration.

Command History

Release	Modification
10.0	The VPN name was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS/VPLS feature.

Example

This example shows how to set VPLS VPN name.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#vpn 1
DmSwitch(config-vpls-vpn-1)#name CWB-RT-3
DmSwitch(config-vpls-vpn-1)#
```

You can verify the VPN name configured by entering the **show running-config** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.

mac-address limit ^[1] ^[3] ^[6]

mac-address limit *number*

no mac-address limit

Description

Set the VPLS mac-address limit for VPLS VPN.

Inserting **no** as prefix for this command will unset the VPLS VPN mac-address limit.

Syntax

Parameter	Description
<i>number</i>	The mac-address limit for VPLS VPN.(Range:1-Depends on board and external memory).

Default

If global L2VPN mac-address limit was defined before, all VPN's are created with that default value.

Command Modes

MPLS VPLS VPN configuration.

Command History

Release	Modification
10.0	The VPN mac-address limit was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS/VPLS feature. If global L2VPN mac-address limit was defined before, all VPN's are created with that default value. This command creates a mac-addres limit for the current VPN, overriding the global one. If global L2VPN mac-addres limit was not set and this command is not executed, the mac-address limit for VPLS VPN is shared with total L2 table.

Example

This example shows how to set the mac-address limit for the VPLS VPN.

```
DmSwitch(config)#mpls vpls  
DmSwitch(config-vpls)#vpn 1
```

```
DmSwitch(config-vpls-vpn)#mac-address limit 1000
DmSwitch(config-vpls-vpn)#
```

You can verify the VPLS/VPN mac-address limit configured by entering the **show running-config** command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
mpls vpls mac-address limit global	Set the global default mac-address limit for VPLS VPNs.

xconnect vlan ^[1] ^[3] ^[6]

```
xconnect vlan id [vc-type {ethernet | vlan}]
```

```
no xconnect vlan id
```

Description

Creates an Attachment Circuit (AC) for the VPLS VPN.

Inserting **no** as prefix for this command will delete the attachment circuit of VPLS VPN.

Syntax

Parameter	Description
vlan <i>id</i>	VLAN <i>id</i> of attachment circuit (AC).
vc-type	Specify the VC type of attachment circuit.
ethernet	VC type is Ethernet.
vlan	VC type is VLAN.

Default

The **vc-type** default value is **vlan**.

Command Modes

MPLS VPLS VPN configuration.

Command History

Release	Modification
9.0	This command was introduced.
10.0	The vc-type parameter was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS/VPLS feature. The VPN attachment circuit (VLAN) must have at maximum eight interfaces ethernet or portchannels being the same type tagged or untagged. To delete an attachment circuit of VPLS VPN, you must delete all neighbors or disable the VPN first.

Example

This example shows how to create an attachment circuit for VPLS VPN.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#vpn 1
DmSwitch(config-vpls-vpn-1)#xconnect vlan 100
DmSwitch(config-vpls-vpn-1)#
```

The example above the vc-type is not specified. In this case the default value **vlan** is assumed.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#vpn 1
DmSwitch(config-vpls-vpn-1)#xconnect vlan 100 vc-type ethernet
DmSwitch(config-vpls-vpn-1)#
```

The example above the vc-type is **ethernet** and all PWs are configured with this parameter (protocol signalization exchange this information). Configuring this parameter could be useful for interoperability issues with others vendors.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.

neighbor [1] [3] [6]

```
neighbor ip-address { pwid number | pwidfec pwid number groupid number mplstype  
[ non-te | te-tunnel tunnelId ] [ split-horizon | no-split-horizon ] [ vlanmode  
changevlan number ] }
```

```
no neighbor ip-address { pwid number | pwidfec pwid number groupid number }
```

Description

Configures a VPLS with the specified neighbor.

Inserting **no** as a prefix for this command will remove the circuit from configuration.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the peer IP address.
pwid <i>number</i>	Specifies the PW ID that identifies this particular circuit.
groupid <i>number</i>	Specifies the Group ID that the circuit belongs to.
mplstype	Specifies the LSP encapsulation type of the circuit.
non-te	The circuit will be encapsulated by LSPs created via LDP.
te-tunnel <i>tunnelId</i>	The circuit will be encapsulated by LSPs created via RSVP, the tunnelId must be specified.
split-horizon	Enables VPLS to use the split horizon forwarding mechanism.
no-split-horizon	Enables VPLS to not use the split horizon forwarding mechanism.
changevlan <i>number</i>	Change de internal VLAN identifier of encapsuled VPN packet.

Default

No default is defined.

Command Modes

MPLS VPLS VPN configuration.

Command History

Release	Modification
9.0	This command was introduced.
10.0	This command was extended for VPLS VPNs.
11.2	The command was splitted in several subcommands.

Usage Guidelines

In MPLS VPLS configuration mode the user can create VPLS circuits according to RFC 4762. After having specified the attachment circuit with **xconnect vlan** command, the user should enter this **neighbor** command that specifies not only the peers to establish the circuit with, but also the PWi FEC Element attributes which identifies the circuit. The maximum neighbors peers for each VPN is eight.

Example

This example shows how to enter in MPLS VPLS configuration mode and create a VPLS with peers 100.100.100.13 and 100.100.100.15.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 2000
DmSwitch(config-mpls-vpls-vpn-2000)#xconnect vlan 100
DmSwitch(config-mpls-vpls-vpn-2000)#neighbor 100.100.100.13 pwid 623 mplstype non-te
DmSwitch(config-mpls-vpls-vpn-2000-pwid-623)#no shutdown
DmSwitch(config-mpls-vpls-vpn-2000-pwid-623)#exit
DmSwitch(config-mpls-vpls-vpn-2000)#neighbor 100.100.100.15 pwid 625 mplstype te-tunnel 12
DmSwitch(config-mpls-vpls-vpn-2000-pwid-625)#no shutdown
DmSwitch(config-mpls-vpls-vpn-2000-pwid-625)#exit
```

The following example shows an alternate method of configuring a peer.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 2000
DmSwitch(config-mpls-vpls-vpn-2000)#xconnect vlan 100
DmSwitch(config-mpls-vpls-vpn-2000)#neighbor 100.100.100.13 pwidfec pwid 623 groupid 0 mplstype non-te
DmSwitch(config-mpls-vpls-vpn-2000-pwid-623)#no shutdown
DmSwitch(config-mpls-vpls-vpn-2000-pwid-623)#exit
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpls	Configure Virtual Private LAN Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
xconnect vlan	Creates an access VLAN interface for the VPLS VPN.
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode

transparent-lan-service [1] [3] [6]

transparent-lan-service

no transparent-lan-service

Description

Enable Transparent LAN Service mode for VPLS VPN.

Inserting **no** as prefix for this command will disable Transparent LAN Service mode for VPLS VPN.

Syntax

No parameter accepted.

Default

no transparent-lan-service

Command Modes

MPLS VPLS VPN configuration.

Command History

Release	Modification
11.6	The Transparent LAN Service mode was introduced.

Usage Guidelines

To use this command, the equipment must support the MPLS/VPLS feature.

Up to 128 Transparent LAN Service enabled are supported.

Example

This example shows how to enable VPLS Transparent LAN Service mode.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#vpn 5
DmSwitch(config-vpls-vpn-5)#transparent-lan-service
DmSwitch(config-vpls-vpn-5)#
```

You can verify if Transparent LAN Service is configured by entering the **show mpls l2vpn detail** or **show running-config** commands.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.

mplstype ^[1] ^[3] ^[6]

mplstype [**non-te** | **te-tunnel** *tunnelId*]

Description

This command specifies the VC encapsulation type to be used with a VPN neighbor.

Syntax

Parameter	Description
non-te	Specifies that the circuit will be encapsulated by LSPs created via LDP.
te-tunnel <i>tunnelId</i>	Specifies that the circuit will be encapsulated by LSPs created via RSVP. The <i>tunnelId</i> must be configured.

Default

non-te type.

Command Modes

MPLS VPLS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPLS VPN PWID configuration mode and configure the VC encapsulation type.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 1
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 100.100.100.1 pwid 1 mplstype te-tunnel 14
DmSwitch(config-mpls-vpls-vpn-1-pwid-1)#no shutdown
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 100.100.100.2 pwid 2 mplstype non-te
DmSwitch(config-mpls-vpls-vpn-1-pwid-2)#no shutdown
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 100.100.100.3 pwid 3 mplstype te-tunnel 13
DmSwitch(config-mpls-vpls-vpn-1-pwid-3)#no shutdown
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 100.100.100.4 pwid 4 mplstype non-te
DmSwitch(config-mpls-vpls-vpn-1-pwid-4)#no shutdown
```

```
DmSwitch(config-mpls-vpls-vpn-1-pwid-1)#end
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpls	Configure Virtual Private LAN Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
neighbor	Configures a VPLS with the specified neighbor.
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode

split-horizon ^[1] ^[3] ^[6]

split-horizon

no-split-horizon

Description

This command specifies if split horizon forwarding mode is enabled or not on a VPLS service.

Default

Split horizon enabled.

Command Modes

MPLS VPLS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPLS VPN PWID configuration mode and enable/disable the split horizon mode for a specified neighbor.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 1
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 100.100.100.1 pwid 1
DmSwitch(config-mpls-vpls-vpn-1-pwid-1)#split-horizon
DmSwitch(config-mpls-vpls-vpn-1-pwid-1)#

DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 2
DmSwitch(config-mpls-vpls-vpn-2)#neighbor 100.100.100.3 pwid 3
DmSwitch(config-mpls-vpls-vpn-2-pwid-3)#no-split-horizon
DmSwitch(config-mpls-vpls-vpn-2-pwid-3)#
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mpls vpls</code>	Configure Virtual Private LAN Service.
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.
<code>show running-config</code>	Shows the current operating configuration.
<code>neighbor</code>	Configures a VPLS with the specified neighbor.

vlanmode [1] [3] [6]

vlanmode changevlan *vlan*

no vlanmode changevlan *vlan*

Description

This command changes the internal VLAN identifier of encapsulated access VPN packets.

Syntax

Parameter	Description
<i>vlan</i>	VLAN ID

Default

No default is defined.

Command Modes

MPLS VPLS VPN PWID configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Create a neighbor first using **neighbor** command.

Example

This example shows how to enter in MPLS VPLS VPN PWID configuration mode and configure the internal VLAN identifier of an VC encapsulated packet for a specified neighbor.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 1
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 100.100.100.1 pwid 1
DmSwitch(config-mpls-vpls-vpn-1-pwid-1)#vlanmode changevlan 200
DmSwitch(config-mpls-vpls-vpn-1-pwid-1)#
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mpls vpls</code>	Configure Virtual Private LAN Service.
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.
<code>show running-config</code>	Shows the current operating configuration.
<code>neighbor</code>	Configures a VPLS with the specified neighbor.

statistics ^[1] ^[2] ^[3] ^[4] ^[5] ^[6] ^[7]

statistics

no statistics

Description

Enables statistics on the VPLS VPN, allowing usage of L2VPN counters.

Inserting **no** as prefix for this command will disable statistics on the VPLS VPN.

Default

statistics is disabled by default.

Command Modes

MPLS VPLS VPN configuration.

Command History

Release	Modification
14.2	This command was introduced.

Usage Guidelines

On DM4100 Enduro, statistics must be enabled on a VPN in order to check its L2VPN counters (due to hardware restrictions, only RX counters are available). Whenever this command is enabled on a VPN, hardware resources (filters and counters) are consumed proportionately to the number of ports of the VPN. For that reason, it's recommended to only activate it during L2VPN troubleshooting. This command might fail in a system where a great amount of filters and/or counters are configured. In such case, a few filters and/or counters must be deleted from the system configuration in order to allow the proper operation of the command.

Example

This example shows how to activate statistics on a VPLS VPN.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-vpls)#vpn 1
DmSwitch(config-vpls-vpn-1)#statistics
DmSwitch(config-vpls-vpn-1)#
```

Related Commands

Command	Description
<code>statistics</code>	Enables statistics on the VPWS VPN.
<code>show running-config</code>	Shows the current operating configuration.
<code>show mpls l2vpn</code>	Show L2VPN (VPWS/VPLS) information.

exp-ingress-mapping ^[1] ^[3] ^[6]

exp-ingress-mapping

no exp-ingress-mapping

Description

The command **exp-ingress-mapping** enables the use of MPLS EXP to PRI Ingress mapping table rules to be followed. This is the default system option. The command **no exp-ingress-mapping** disables the use of MPLS EXP to PRI Ingress mapping table rules. This is needed when QoS egress filtering rules are associated with VPN access ports and/or local-tunnels.

Default

exp-ingress-mapping is enabled by default.

Command Modes

MPLS VPLS configuration.

Command History

Release	Modification
15.2.2	This command was introduced.

Usage Guidelines

Create a VPN first **neighbor** command.

Example

The examples below show how to enter in MPLS VPLS VPN configuration mode and disable/enable the EXP to PRI Ingress mapping mode.

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 1
DmSwitch(config-mpls-vpls-vpn-1)#no exp-ingress-mapping
DmSwitch(config-mpls-vpls-vpn-1)#xconnect vlan 100 vc-type vlan
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 200.200.200.1 pwid 12 mplstype non-te
DmSwitch(config-mpls-vpls-vpn-1-pwid-12)#no shutdown
```

```
DmSwitch(config)#mpls vpls
DmSwitch(config-mpls-vpls)#vpn 1
DmSwitch(config-mpls-vpls-vpn-1)#exp-ingress-mapping
DmSwitch(config-mpls-vpls-vpn-1)#xconnect vlan 100 vc-type vlan
DmSwitch(config-mpls-vpls-vpn-1)#neighbor 200.200.200.1 pwid 12 mplstype non-te
DmSwitch(config-mpls-vpls-vpn-1-pwid-12)#no shutdown
```

You can verify the VPN configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls vpls	Configure Virtual Private LAN Service.
show mpls l2vpn	Show L2VPN (VPWS/VPLS) information.
show running-config	Shows the current operating configuration.
filter	Creates or configures a traffic filter
meter	Configures a meter to be used by a filter
mpls exp-map egress	Configures the table mapping for COS priority to EXP egress packets.
mpls exp-map ingress	Configures the table mapping for EXP to COS priority ingress packets.
show mpls exp-map ingress	Shows MPLS EXP to COS priority mapping table for ingress packets.
show mpls exp-map egress	Shows MPLS COS priority to EXP mapping table for egress packets.

Chapter 47. Network Policy Commands

voice vlan

```
voice vlan vlan_id cos l2-prio-level [ dscp dscp-value | mac-list { auto | manual } ]
```

```
voice vlan vlan_id dscp dscp-value
```

```
voice vlan dot1p { cos l2-prio-level [ dscp dscp-value ] | dscp dscp-value }
```

```
voice vlan native { cos l2-prio-level [ dscp dscp-value ] | dscp dscp-value }
```

```
voice vlan untagged dscp dscp-value
```

Description

Configure Voice VLAN feature.

Syntax

Parameter	Description
<i>vlan_id</i>	Specify voice VLAN ID number (Range 0-4094).
dot1p	Specify IEEE 802.1p priority tagging.
untagged	Specify voice VLAN untagged.
<i>cos l2-prio-level</i>	Specify Layer 2 priority (Range 0-7).
dscp <i>dscp-value</i>	Specify DiffServ value (Range 0-63).
mac-list <i>mode</i>	Specify mac-list mode.

Default

No default is defined.

Command Modes

Network-Policy configuration.

Command History

Release	Modification
13.0	This command was introduced.
13.2	Option mac-list introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure Voice VLAN in network policy profile 1.

```
DmSwitch#network-policy profile 1
DmSwitch(config-network-policy)#voice vlan 100 cos 3
DmSwitch(config-network-policy)
```

You can verify that the information was configured by entering the **show this** or **show network-policy** in the new prompt.

Related Commands

Command	Description
network-policy	Enters on Network Policy configuration mode.
voice-signaling vlan	Configure Voice-Signaling VLAN feature.
show network-policy	Shows Network Policy settings.
show running-config	Shows the current operating configuration.

voice-signaling vlan

```
voice-signaling vlan vlan_id { cos l2-prio-level [ dscp dscp-value ] | dscp dscp-value }
```

```
voice-signaling vlan dot1p { cos l2-prio-level [ dscp dscp-value ] | dscp dscp-value }
```

```
voice-signaling vlan native { cos l2-prio-level [ dscp dscp-value ] | dscp dscp-value }
```

```
voice-signaling vlan untagged dscp dscp-value
```

Description

Configure Voice-Signaling VLAN feature.

Syntax

Parameter	Description
<i>vlan_id</i>	Specify voice VLAN ID number (Range 0-4094).
dot1p	Specify IEEE 802.1p priority tagging.
untagged	Specify voice VLAN untagged.
<i>cos l2-prio-level</i>	Specify Layer 2 priority (Range 0-7).
dscp <i>dscp-value</i>	Specify DiffServ value (Range 0-63).

Default

No default is defined.

Command Modes

Network-Policy configuration.

Command History

Release	Modification
13.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure Voice VLAN in network policy profile 1.

```
DmSwitch#network-policy profile 1
DmSwitch(config-network-policy)#voice-signaling vlan dot1p cos 4
DmSwitch(config-network-policy)
```

You can verify that the information was configured by entering the **show this** or **show network-policy** in the new prompt.

Related Commands

Command	Description
network-policy	Enters on Network Policy configuration mode.
voice vlan	Configure Voice VLAN feature.
show network-policy	Shows Network Policy settings.
show running-config	Shows the current operating configuration.

Chapter 48. OpenFlow

clear-flows

clear-flows

Description

Clear all OpenFlow flows installed in hardware.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to clear OpenFlow flows.

```
DmSwitch(config-openflow)#clear-flows
DmSwitch(config-openflow)#
```

Verify that OpenFlow flows were cleared by entering the **show openflow flows** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show openflow</code>	Shows global OpenFlow configuration.
<code>show openflow flows</code>	Shows global OpenFlow configuration.
<code>openflow</code>	Enables global OpenFlow protocol.

controller

controller { *ip-address* } { *port-number* } [**ssl** | **tcp**]

Description

Configure OpenFlow controller, informing the IP address of host that is running OpenFlow controller, as well as the host's tcp-port number that OpenFlow should use for communication.

Syntax

Parameter	Description
<i>ip-address</i>	The IP address of host where the OpenFlow controller is running.
<i>port-number</i>	TCP port that OpenFlow protocol should use for communication.
ssl	OpenFlow will communicate using SSL (Secure Socket Layer) connection.
tcp	OpenFlow will communicate using TCP connection. This is the default value if no connection type is informed

Default

No default is defined.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to clear OpenFlow flows.

```
DmSwitch(config-openflow)#controller 10.1.32.101 6633
DmSwitch(config-openflow)#
```

You can verify the OpenFlow controller configurations entering the **show openflow** privileged EXEC command.

Related Commands

Command	Description
openflow	Enables global OpenFlow protocol.
show openflow	Shows global OpenFlow configuration.

filter-group-prio

filter-group-priority { *priority* }

Description

Reserve a Filter Group Priority for OpenFlow.

Syntax

Parameter	Description
<i>priority</i>	An integer number. In boards of 4001 family priority must be between 0 and 14. In boards of 4100 family priority must be between 0 and 4.

Default

If no value is configured, it will be automatically choosen.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to configure the filter group priority.

```
DmSwitch(config-openflow)#filter-group-prio 0
DmSwitch(config-openflow)#
```

You can verify the OpenFlow filter group priority by entering the **show openflow** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>openflow</code>	Enables global OpenFlow protocol.
<code>show openflow</code>	Shows global OpenFlow configuration.

mode

mode [proactive | reactive]

Description

Configures OpenFlow mode. It has two possible configurations: proactive and reactive mode. In the proactive mode, if a packet has no matching flow then it will be dropped. In the reactive mode, if a packet has no matching flow then it will be sent to the controller.

Syntax

Parameter	Description
proactive	Packets without a matching flow are dropped.
reactive	Packets without a matching flow are sent to controller.

Default

Reactive is the default OpenFlow mode.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to configure OpenFlow proactive mode.

```
DmSwitch(config-openflow)#mode proactive
DmSwitch(config-openflow)#
```

You can verify the OpenFlow mode configurations entering the **show openflow** privileged EXEC command.

Related Commands

Command	Description
<code>openflow</code>	Enables global OpenFlow protocol.
<code>show openflow</code>	Shows global OpenFlow configuration.

native-vlan

native-vlan { *index* }

Description

Configure the OpenFlow native VLAN.

To work properly, it is strongly recommended that users configure a native VLAN. This guarantees the correct work of the equipment in a hybrid scenario, i.e., when router is being used both with OpenFlow and other protocols.

Note: a VLAN configured as a native-vlan OpenFlow will not accept any user configurations.

Syntax

Parameter	Description
<i>index</i>	VLAN index.

Default

No default is defined.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to configure the OpenFlow native VLAN.

```
DmSwitch(config-openflow)#native-vlan 4000
DmSwitch(config-openflow)#show this
!
openflow
  native-vlan 4000
```

!

Related Commands

Command	Description
<code>show openflow</code>	Shows global OpenFlow configuration.
<code>openflow</code>	Enables global OpenFlow protocol.

rem-ssl-file

```
rem-ssl-file [all | ca-cert | cert | privkey]
```

Description

Remove the certificate and private key files used by OpenFlow when connecting to a controller using SSL (Secure Socket Layer).

Syntax

Parameter	Description
all	Remove all certificate and private key files.
ca-cert	Remove only the certification authority certificate.
cert	Remove only the switch certificate.
privkey	Remove only the switch private key.

Default

No default is defined.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.5	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode, in shutdown state.

Related Commands

Command	Description
openflow	Enables global OpenFlow protocol.
controller	Configure OpenFlow controller.

shutdown

shutdown

no shutdown

Description

Deactivates OpenFlow.

Inserting **no** as a prefix for this command will reactivate OpenFlow.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to deactivate OpenFlow.

```
DmSwitch(config-openflow)#shutdown
DmSwitch(config-openflow)#
```

You can verify that OpenFlow was deactivated by entering the **show openflow** privileged EXEC command.

Related Commands

Command	Description
openflow	Enables global OpenFlow protocol.

Command	Description
<code>show openflow</code>	Shows global OpenFlow configuration.

strip-fcs

strip-fcs

no strip-fcs

Description

Enables strip of FCS (Frame Check Sequence) in OpenFlow Packet-in packets.

The **no** command will disable strip of FCS (Frame Check Sequence), i.e., the OpenFlow packets will arrive with the FCS.

Syntax

No parameter accepted.

Default

The **strip-fcs** is enabled by default when OpenFlow is enabled.

Command Modes

OpenFlow configuration.

Command History

Release	Modification
OF-1.0.4	This command was introduced.

Usage Guidelines

To use this command you must be in OpenFlow configuration mode.

Example

This example shows how to enable the strip of FCS in OpenFlow packets.

```
DmSwitch(config-openflow)#strip-fcs
DmSwitch(config-openflow)#show this
!
openflow
  strip-fcs
!
DmSwitch(config-openflow)#no strip-fcs
DmSwitch(config-openflow)#show this
!
openflow
!
```

```
DmSwitch(config-openflow) #
```

Related Commands

Command	Description
show openflow	Shows global OpenFlow configuration.
openflow	Enables global OpenFlow protocol.

Chapter 49. Route-map Commands

continue

continue *sequence-number*

no continue

Description

Allows the configuration and organization of more modular policy definitions to reduce the number of policy configurations that are repeated within the same route map.

Syntax

Parameter	Description
<i>sequence-number</i>	Specifies the route-maps's sequence to be executed.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

Using a continue clause allows the route map continue evaluating and executing match clauses in the specified route-map entry after a successful match occurs. The clause can be configured to jump to a specific route-map entry by specifying the sequence number. If a match clause exists, the continue clause is executed only if a match occurs. If no successful matches occur, the continue clause is ignored.

Example

The following example shows that the routes matching community list 1 will enable 'continue' clause to go to

route-map sequence 30.

```
DmSwitch(config-route-map)#route-map set_weight 10 permit
DmSwitch(config-route-map)#match community-list 1
DmSwitch(config-route-map)#set weight 50
DmSwitch(config-route-map)#continue 30
```

You can verify the configurations by entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address	Matches ip address by prefix-list values from routing table.
prefix-list	
match ip next-hop	Matches next-hop ip values from routing table.
prefix-list	
match ip route-source	Matches route-source ip values from routing table.
prefix-list	
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
show running-config	Shows the current operating configuration.

match as-path

match as-path *regexp*

no match as-path

Description

Match as-path values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
<i>regexp</i>	Regular expressions that matches the desired BGP AS-path list.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

Regular Expressions Overview and Example

Regular expressions can be used for defining AS-path access lists and community lists to more easily filter routes. It is not intended here to explain in detail how Regular Expressions do work, but rather a brief overview of their syntax and how they can be applied to match AS-Path-, Community- and ExtCommunity-Lists.

AS-Path Lists

A regular expression uses special characters often referred to as metacharacters to define a pattern that is compared with an input string. For an AS-path access list, the input string is the AS path of the routes to which the list is applied via the route-map or neighbor filter-list commands. If the AS path matches the regular expression in the access list, then the route matches the access list. The following commands apply access list to routes inbound from BGP peer 172.16.15.2. Access list defined under Route-Map 7 uses a regular expression to deny routes originating in AS 55.

```
DmSwitch(config-router-bgp)#neighbor 172.16.15.2 remote-as 55
DmSwitch(config-router-bgp)#neighbor 172.16.15.2 filter-list 1 in
DmSwitch(config-router)#exit
DmSwitch(config)#route-map 7 deny 20
DmSwitch(config)#match as-path 55$
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Metacharacters

Each regular expression consists of one or more metacharacters and zero or more complete or partial AS or community numbers. Following table describes the metacharacters supported for regular expression pattern-matching. Please refer to specific Regular-Expressions literature for detailed explanation.

Supported Regular Expression Metacharacters

Metacharacter	Description
^	Matches the beginning of the input string. Alternatively, when used as the first character within brackets [^] matches any number except the ones specified within the brackets.
\$	Matches the end of the input string.
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the immediately previous character or pattern.
+	Matches 1 or more sequences of the immediately previous character or pattern.
?	Matches 0 or 1 sequence of the immediately previous character or pattern.
()	Specifies patterns for multiple use when followed by one of the multiplier metacharacters: asterisk *, plus sign +, or question mark ?
[]	Matches any enclosed character; specifies a range of single characters.
- (hyphen)	Used within brackets to specify a range of AS or community numbers.
_ (underscore)	Matches a ^, a \$, a comma, a space, a {, or a }. Placed on either side of a string to specify a literal and disallow substring matching. Numerals enclosed by underscores can be preceded or followed by any of the characters listed above.
 	Matches characters on either side of the metacharacter; logical OR.

Related Commands

Command	Description
<code>route-map</code>	Create route-map or enter route-map command mode.
<code>match community</code>	Matches community values from routing table.
<code>match extcommunity</code>	Matches extcommunity values from routing table.
<code>match ip address prefix-list</code>	Matches ip address by prefix-list values from routing table.
<code>match ip next-hop prefix-list</code>	Matches next-hop ip values from routing table.
<code>match ip route-source prefix-list</code>	Matches route-source ip values from routing table.
<code>match metric</code>	Matches metric values from routing table.
<code>set as-path</code>	Sets as-path values in destination routing protocol.
<code>set as-path-limit</code>	Sets as-path-limit values in destination routing protocol.
<code>set community</code>	Sets community values in destination routing protocol.
<code>set extcommunity</code>	Sets extcommunity values in destination routing protocol.
<code>set local-preference</code>	Sets local-preference value in destination routing protocol.
<code>set metric</code>	Sets metric value in destination routing protocol.
<code>set next-hop</code>	Sets next_hop value in destination routing protocol.
<code>set origin</code>	Sets origin value in destination routing protocol.
<code>set weight</code>	Sets weight value in destination routing protocol.
<code>continue</code>	Executes additional entries in a route map.
<code>show running-config</code>	Shows the current operating configuration.

match community

match community *regexp*

no match community

Description

Match community values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
<i>regexp</i>	Regular expression that matches the desired community list.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
9.4	Command match community use POSIX regular-expressions as parameters.
8.0	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

Regular Expressions Overview and Example

Regular expressions can be used for defining AS-path access lists and community lists to more easily filter routes. It is not intended here to explain in detail how Regular Expressions do work, but rather a brief overview of their syntax and how they can be applied to match AS-Path-, Community- and ExtCommunity-Lists.

Community Lists

For a community list, the input string is the community attribute of the routes to which the list is applied via a route-map command. If the community attribute matches the regular expression in the community list, then the route matches the community list. The following commands apply route map 5 to routes forwarded to BGP peer 172.16.15.4. Route map 5 uses a regular expression to match community numbers ending with 705, setting the weight of matching routes to 150.

```
DmSwitch(config-router-bgp)#neighbor 172.16.15.4 remote-as 625
DmSwitch(config-router-bgp)#neighbor 172.16.15.4 route-map 5 out
DmSwitch(config-router-bgp)#exit
DmSwitch(config)#route-map 5 permit 10
DmSwitch(config-route-map)#match community 705$
DmSwitch(config-route-map)#set weight 150
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Community Numbers

Appropriate format for the community number in the community list should be used when using a regular expression to match a community number. In the case of ip bgp-community new-format command, the community number has the format AA:NN where AA is a number that identifies the autonomous system, and NN is a number that identifies the community within the autonomous system. Otherwise, the community number is an integer in the range 1-4294967295.

Metacharacters

Each regular expression consists of one or more metacharacters and zero or more complete or partial AS or community numbers. Following table describes the metacharacters supported for regular expression pattern-matching. Please refer to specific Regular-Expressions literature for detailed explanation.

Supported Regular Expression Metacharacters

Metacharacter	Description
^	Matches the beginning of the input string. Alternatively, when used as the first character within brackets [^] matches any number except the ones specified within the brackets.
\$	Matches the end of the input string.
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the immediately previous character or pattern.
+	Matches 1 or more sequences of the immediately previous character or pattern.
?	Matches 0 or 1 sequence of the immediately previous character or pattern.
()	Specifies patterns for multiple use when followed by one of the multiplier metacharacters: asterisk *, plus sign +, or question mark ?
[]	Matches any enclosed character; specifies a range of single characters.
- (hyphen)	Used within brackets to specify a range of AS or community numbers.

Metacharacter	Description
_ (underscore)	Matches a ^, a \$, a comma, a space, a {, or a }. Placed on either side of a string to specify a literal and disallow substring matching. Numerals enclosed by underscores can be preceded or followed by any of the characters listed above.
 	Matches characters on either side of the metacharacter; logical OR.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address	Matches ip address by prefix-list values from routing table.
prefix-list	
match ip next-hop	Matches next-hop ip values from routing table.
prefix-list	
match ip route-source	Matches route-source ip values from routing table.
prefix-list	
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

match extcommunity

match extcommunity *regex*

no match extcommunity

Description

Match extcommunity values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
<i>regex</i>	Regular expression that matches the desired extended community list.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
9.4	Command match extcommunity use POSIX regular-expressions as parameters.
8.0	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

Regular Expressions Overview and Example

Regular expressions can be used for defining AS-path access lists and community lists to more easily filter routes. It is not intended here to explain in detail how Regular Expressions do work, but rather a brief overview of their syntax and how they can be applied to match AS-Path-, Community- and ExtCommunity-Lists.

Extcommunity Lists

For an extcommunity list, the input string is the extcommunity attribute of the routes to which the list is applied via a route-map command. If the extcommunity attribute matches the regular expression in the community list, then the route matches the extcommunity list. The following commands apply route map 5 to routes forwarded to BGP peer 172.16.15.4. Route map 5 uses a regular expression to match extcommunity numbers ending with 705, setting the weight of matching routes to 150.

```
DmSwitch(config-router-bgp)#neighbor 172.16.15.4 remote-as 625
DmSwitch(config-router-bgp)#neighbor 172.16.15.4 route-map 5 out
DmSwitch(config-router-bgp)#exit
DmSwitch(config)#route-map 5 permit 10
DmSwitch(config-route-map)#match extcommunity 705$
DmSwitch(config-route-map)#set weight 150
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Extcommunity Values

Appropriate format for the extcommunity number or ip in the extcommunity list should be used when using a regular expression to match an extcommunity value. The extcommunity number has the format AA:NN where AA is a number that identifies the autonomous system, and NN is a number that identifies the extcommunity within the autonomous system. The extcommunity value can be expressed also by an ip address A.A.A.A:NN where A value varies from 0 to 255 and NN from 0 to 65535 that identifies the autonomous system.

Metacharacters

Each regular expression consists of one or more metacharacters and zero or more complete or partial AS or community numbers. Following table describes the metacharacters supported for regular expression pattern-matching. Please refer to specific Regular-Expressions literature for detailed explanation.

Supported Regular Expression Metacharacters

Metacharacter	Description
^	Matches the beginning of the input string. Alternatively, when used as the first character within brackets [^] matches any number except the ones specified within the brackets.
\$	Matches the end of the input string.
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the immediately previous character or pattern.
+	Matches 1 or more sequences of the immediately previous character or pattern.
?	Matches 0 or 1 sequence of the immediately previous character or pattern.
()	Specifies patterns for multiple use when followed by one of the multiplier metacharacters: asterisk *, plus sign +, or question mark ?
[]	Matches any enclosed character; specifies a range of single characters.
- (hyphen)	Used within brackets to specify a range of AS or community numbers.

Metacharacter	Description
_ (underscore)	Matches a ^, a \$, a comma, a space, a {, or a }. Placed on either side of a string to specify a literal and disallow substring matching. Numerals enclosed by underscores can be preceded or followed by any of the characters listed above.
 	Matches characters on either side of the metacharacter; logical OR.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match ip address	Matches ip address by prefix-list values from routing table.
prefix-list	
match ip next-hop	Matches next-hop ip values from routing table.
prefix-list	
match ip route-source	Matches route-source ip values from routing table.
prefix-list	
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

match ip address

```
match ip address prefix-list prefix-list-name
```

```
no match ip address prefix-list
```

Description

Match ip address values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
prefix-list <i>prefix-list-name</i>	Name of prefix list containing the desired entries of prefix.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
ip prefix-list	Configure a prefix list.
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

match ip next-hop

```
match ip next-hop prefix-list prefix-list-name
```

```
no match ip next-hop prefix-list
```

Description

Match ip next-hop values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
prefix-list <i>prefix-list-name</i>	Name of prefix list containing the desired entries of prefix.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
ip prefix-list	Configure a prefix list.
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

match ip route-source

```
match ip route-source prefix-list prefix-list-name
```

```
no match ip source-route prefix-list
```

Description

Match ip source-route values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
prefix-list <i>prefix-list-name</i>	Name of prefix list containing the desired entries of prefix.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
ip prefix-list	Configure a prefix list.
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

match metric

match metric *value*

no match metric

Description

Match metric values from routing table.

Inserting **no** as a prefix for this command will remove the previous configuration.

Syntax

Parameter	Description
<i>value</i>	Matches the desired metric of route.

Default

No default is defined.

Command Modes

ROUTE-MAP configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Define condition to be checked in route map. The match commands specify the conditions under which redistribution is allowed for the current route-map command. The commands may be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands.

Example

The following commands apply access list to routes inbound from BGP peer 172.16.15.2. Access list defined under Route-Map 7 uses a regular expression to deny routes originating in AS 55.

```
DmSwitch(config-router-bgp)#neighbor 172.16.15.2 remote-as 55
DmSwitch(config-router-bgp)#neighbor 172.16.15.2 filter-list 1 in
```

```
DmSwitch(config-router)#exit
DmSwitch(config)#route-map 7 deny 20
DmSwitch(config)#match as-path 55$
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address	Matches ip address by prefix-list values from routing table.
prefix-list	
match ip next-hop	Matches next-hop ip values from routing table.
prefix-list	
match ip route-source	Matches route-source ip values from routing table.
prefix-list	
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set as-path

```
set as-path prepend local-as times
```

```
no set as-path
```

Description

Set as-path value in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
prepend local-as times	Prepend to the as-path the local AS, specifying the number of times.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

The set as-path command specify the number of times the local-as should be prepended onto route's as-path if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the as-path prepended with local-as twice.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set as-path prepend local-as 2
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set as-path-limit

set as-path-limit *limit*

no set as-path-limit

Description

Set as-path-limit value in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
as-path-limit <i>limit</i>	Sets BGP AS-path upper limit size.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

The set as-path-limit command specifies the route's as-path upper limit size to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the as-path limited to 3 AS values.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set as-path-limit 3
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set community

```
set community { none | { aa:nn | internet | local-AS | no-advertise | no-export  
[additive] }}
```

```
no set community
```

Description

Set community values in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
none	No BGP community attribute.
<i>aa:nn</i>	Set Community attribute to number in aa:nn format.
internet	Set Community attribute to Internet (well-known community).
local-AS	Set Community attribute to not send outside local AS (well-known community).
no-advertise	Set Community attribute to not advertise to any peer (well-known community).
no-export	Set Community attribute to not export to next AS (well-known community).
additive	(Optional) Adds to the existing community.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The set commands specify the set actions to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the community overwritten to 101:1 102:1 103:1. Routes that pass IP address prefix list list IN_B have the community appended with 104:1 105:1.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set community 101:1 102:1 103:1

DmSwitch(config-route-map)#route-map set_community 20 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_B
DmSwitch(config-route-map)#set community 104:1 105:1 additive
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set extcommunity

```
set extcommunity { none | rt { ip-address:nn | aa:nn } [additive] | soo { ip-address:nn | aa:nn } }
```

```
no set extcommunity
```

Description

Set extcommunity values in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
none	No BGP extended community attribute.
rt	Route Target extended community.
soo	Site-of-Origin extended community.
<i>aa:nn</i>	VPN extended community attribute in 'AS number': 'any number' format.
<i>ip-address:nn</i>	VPN extended community attribute in 'IP address': 'any number' format.
additive	(Optional) Adds to the existing extcommunity.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The set extcommunity command specify the extcommunity values to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the extcommunity set to route-target 60000:1 1.1.1.1:1 2.2.2.2:1. Routes that pass IP address prefix list list IN_B have the extcommunity set to site-of-origin 8.8.8.8:1.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set extcommunity rt 60000:1 1.1.1.1:1 2.2.2.2:1

DmSwitch(config-route-map)#route-map set_community 20 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_B
DmSwitch(config-route-map)#set extcommunity soo 8.8.8.8:1
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set local-preference

set local-preference *value*

no set local-preference

Description

Set local-preference value in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
<i>value</i>	Sets a preference value for the BGP local preference path attribute. (Range: 0-4294967295)

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The set local-preference command specify the local-preference value to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the local-preference set to 200.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set local-preference 200
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set metric

set metric *value*

no set metric

Description

Set metric value in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
<i>value</i>	Sets a metric value for destination routing protocol. (Range: 0-4294967294)

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The set metric command specify the metric value to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the metric set to 555.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set metric 555
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set next-hop

set next-hop *ip-address*

no set next-hop

Description

Set next-hop values in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of next-hop.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
9.4	Deprecated parameters: ip next-hop
9.4	New parameters: next-hop .
8.0	This command was introduced.

Usage Guidelines

The set next-hop command specify the next-hop address to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the next-hop set to 192.168.1.1.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
```

```
DmSwitch(config-route-map)#set next-hop 192.168.1.1
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set origin

```
set origin { egp | igp | incomplete }
```

```
no set origin
```

Description

Set origin value in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
egp	Remote EGP.
igp	Local IGP.
incomplete	Unknown heritage.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	
8.0	This command was introduced.

Usage Guidelines

The set origin command specify the origin to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the origin set to egp.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set origin egp
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address	Matches ip address by prefix-list values from routing table.
prefix-list	
match ip next-hop	Matches next-hop ip values from routing table.
prefix-list	
match ip route-source	Matches route-source ip values from routing table.
prefix-list	
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

set weight

set weight *value*

no set { weight

Description

Set weight value in destination routing protocol.

Inserting **no** as a prefix for this command will remove the previously set configuration.

Syntax

Parameter	Description
<i>value</i>	Sets a BGP weight value for routing table. (Range: 0-4294967295)

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The set weight command specify the weight to be applied if the conditions specified by the match commands are met.

Example

In the following example, routes that pass the IP address prefix list list IN_A have the weight set to 999.

```
DmSwitch(config-route-map)#route-map set_community 10 permit
DmSwitch(config-route-map)#match ip address prefix-list IN_A
DmSwitch(config-route-map)#set weight 999
```

You can verify that the configuration was made by entering the **show this** command while configuring route-map or entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

Chapter 50. Router BGP Commands

address-family

```
address-family { ipv4 | ipv4 vrf vrf-name | vpnv4 }
```

```
no address-family { ipv4 | ipv4 vrf vrf-name | vpnv4 }
```

Description

Enters the specified BGP address family configuration mode.

Inserting **no** as a prefix for this command will disable address family configuration mode.

Syntax

Parameter	Description
ipv4 [1] [3] [5]	Places the router in address family configuration mode for configuring routing sessions that use IP Version 4 address family configuration mode commands.
ipv4 vrf <i>vrf-name</i>	Specifies the name of the VRF instance to associate with subsequent IP Version 4 address family configuration mode commands.
vpnv4 [1] [3] [5]	Places the router in address family configuration mode for configuring routing sessions that use standard VPN Version 4 address prefixes.

Default

There is no default configuration.

Command Modes

Router BGP configuration.

Command History

Release	Modification
8.0	This command was introduced.
12.4	The ipv4 parameter was introduced.

Usage Guidelines

To enter address family configuration mode for configuring IP version 4

Use the address-family ipv4 vrf vrf-name command to enter address family configuration mode for IPv4 VRF address family sessions. To disable address family ipv4 vrf configuration mode, use the no form of this command.

To enter address family configuration mode for configuring routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes, use the address-family vpnv4 command in router configuration mode.

Example

The following example places the router in address family configuration mode for the VPN Version 4 address family.

```
DmSwitch(config)#router bgp 1
DmSwitch(config-router-bgp)#address-family vpnv4
DmSwitch(config-router-bgp-af-vpnv4)#
```

The following example places the router in address family configuration mode for the IP Version 4 address family.

```
DmSwitch(config)#router bgp 1
DmSwitch(config-router-bgp)#address-family ipv4
DmSwitch(config-router-bgp-af-ipv4)#
```

The following example places the router in address family configuration mode and specifies vpn1 as the name of the VRF instance to associate with subsequent IP Version 4 address family configuration mode commands.

```
DmSwitch(config)#router bgp 1
DmSwitch(config-router-bgp)#address-family ipv4 vrf vpn1
DmSwitch(config-router-bgp-af-vrf)#
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
maximum routes	Configures the maximum number of routes allowed in a VRF table inside BGP.
network	Specify a network to announce via BGP.
redistribute	Redistributes routes with a metric of BGP protocol.
show ip bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

aggregate-address

```
aggregate-address { ip address/mask | ipv6 address/prefix } [do-as-set] [do-summary-only]  
[map-advertise map-tag] [map-attribute map-tag] [map-suppress map-tag]
```

```
no aggregate-address { ip address/mask | ipv6 address/prefix } [do-as-set]  
[do-summary-only] [map-advertise map-tag] [map-attribute map-tag] [map-suppress  
map-tag]
```

Description

This command allows the creation of an aggregate entry using pre-defined rules, aggregating specific routes into one route.

Inserting **no** as a prefix for this command will revert aggregate-address configuration.

Syntax

Parameter	Description
<i>ip-address/mask</i> <i>ipv6-address/prefix</i>	Specifies the aggregate network.
do-as-set	(Optional) Generates AS set path information.
do-summary-only	(Optional) Filters all more-specific routes from updates.
map-advertise <i>map-tag</i>	(Optional) Name of the route map used to select the routes to create AS-SET origin communities.
map-attribute <i>map-tag</i>	(Optional) Name of the route map used to set the attribute of the aggregate route.
map-supress <i>map-tag</i>	(Optional) Name of the route map used to select the routes to be suppressed.

Default

There is no default configuration.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.
12.4	Added extra restrictions for map-supress and do-summary-only.

Usage Guidelines

When a route is aggregated by an AS, the route will be announced as been created by that AS although the route was created by other AS.

Original information from aggregated route can be modified using the parameters defined in the command.

You can configure aggregate-address in BGP either by redistributing an aggregate route into BGP, or by using the conditional aggregate routing feature using route-map definition.

The **do-as-set** keyword establishes the same rules that the command follows without the keyword. However, the path advertised route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

The **do-summary-only** keyword aggregates the specified route (for example, 10.10.*.*) and suppresses advertisements of more specific routes to all neighbors.

The **map-suppress map-tag** keyword aggregates the route but suppresses advertisement of specified routes defined at *map-tag*.

The **map-advertise map-tag** keyword selects specific routes that will NOT be used to build different components of the aggregate route, such as AS_SET or community. This form of the aggregate-address command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems.

Using the **map-attribute map-tag** keyword allows attributes of the aggregate route to be changed. This form of the aggregate-address command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

Usage Restrictions

The following restrictions are applied to the aggregate-address:

- 1) The prefix of the parameter **ip-address/mask** must be between 0 and 31 for IPv4 and between 0 and 127 for IPv6. Prefixes /32 and /128 are not allowed.
- 2) The **map-attribute** parameter must be used with an existing route-map that contains only one sequence. Route-maps with more than one sequence are not allowed.
- 3) The **map-suppress** parameter is not allowed when used in combination with parameter **do-summary-only**.

Example

The following example shows how to configure aggregate-address together with route-map configuration:

```
DmSwitch(config)#route-map MAP permit 10
DmSwitch(config-route-map)#match as-path 62550
DmSwitch(config-route-map)#exit
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#aggregate-address 172.16.30.0/29
DmSwitch(config-router-bgp)#aggregate-address 172.16.30.8/29 do-as-set map-advertise MAP
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
route-map	Create route-map or enter route-map command mode.
show running-config	Shows the current operating configuration.

bgp always-compare-med

```
bgp always-compare-med
```

```
no bgp always-compare-med
```

Description

This command allows comparison of Multi Exit Discriminator (MED) for paths from peers in different AS.
Inserting **no** as a prefix for this command will revert **always-compare-med** configuration.

Syntax

No parameter accepted.

Default

By default, the equipment only compares the MED for paths from the same AS.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

The MED is used for selecting the best path among alternative paths. Its comparison becomes necessary when the paths belong to the same AS. However, the command **always-compare-med** enforces the comparison independently of the AS from which the paths are received.

Example

The following example shows how to configure the MED comparison:

```
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#bgp always-compare-med
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>bgp deterministic-med</code>	Enables deterministic MED comparison

bgp client-to-client reflection

`bgp client-to-client reflection`

`no bgp client-to-client reflection`

Description

Use **bgp client-to-client reflection** to enable or restore route reflection from a BGP route reflector to clients.

Inserting **no** as a prefix for this command will revert client-to-client reflection configuration.

Syntax

No parameter accepted.

Default

BGP client-to-client reflection is enable by default. When a route reflector is configured, it reflects routes from one client to other clients.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

When the route reflector (RR) is enabled, it reflects routes from one client to other clients. This is useful because clients do not need to be fully meshed in order to distribute their routes.

If the clients are fully meshed, route reflection is not required. Use the **no bgp client-to-client reflection** to disable client-to-client reflection.

Example

The following example illustrates a route reflector local router which has clients fully meshed. Since client-to-client is enabled by default, it must be disabled with the **no bgp client-to-client reflection** command.

```
DmSwitch(config)#router bgp 65000
```

```
DmSwitch(config-router-bgp)#neighbor 2.3.4.5 route-reflector-client
DmSwitch(config-router-bgp)#neighbor 3.4.5.6 route-reflector-client
DmSwitch(config-router-bgp)#neighbor 4.5.6.7 route-reflector-client
DmSwitch(config-router-bgp)#no bgp client-to-client reflection
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
neighbor <i>ip-address</i>	Configure a neighbor as Route Reflector client.
route-reflector-client	

bgp cluster-id

```
bgp cluster-id router-id
```

```
no bgp cluster-id
```

Description

Use **bgp cluster-id** to set the cluster ID on a route reflector in a route reflector cluster.

To remove the cluster ID, use the **no** form of this command.

Syntax

Parameter	Description
<i>router-id</i>	Cluster ID of the router acting as a route reflector. This ID can be specified either in dotted or in decimal format. Maximum of 4 bytes.

Default

When no ID is specified or when the **no** form of this command is entered the local router ID of the route reflector is used as the cluster ID .

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

Multiple route reflectors may be deployed to increase redundancy and avoid a single point of failure. To make it possible to have multiple route reflectors (RR) in the same cluster, the **bgp cluster-id** is used to assign the same cluster ID to all RRs in the cluster, so that an RR can discard routes from other RRs in the same cluster (RFC 4456).

Example

The following example illustrates a local router as one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
DmSwitch(config)#router bgp 65000
DmSwitch(config-router-bgp)#neighbor 2.3.4.5 route-reflector-client
DmSwitch(config-router-bgp)#bgp cluster-id 1.2.3.4
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
bgp client-to-client reflection	Configures BGP client-to-client route reflection
show running-config	Shows the current operating configuration.

bgp confederation identifier

bgp confederation identifier *as-number*

no bgp confederation identifier

Description

Use **bgp confederation identifier** to create a BGP confederation and set its identifier.

Use the **no** form of this command to destroy a BGP confederation.

Syntax

Parameter	Description
<i>as-number</i>	AS number to be configured as the BGP confederation identifier.

Default

No default value is defined.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

BGP protocol requires that all BGP routers within a given AS are fully-meshed. Such requirement leads to serious scalability problems. AS confederations for BGP avoid such problems by breaking down a large AS into a set of smaller AS's (sub-AS), which are still seen from the outside as a single AS, thus neutralizing the BGP fully-meshed routers requirement. The present command defines a confederation and its identifier to group a set of sub-AS's.

Just one confederation is allowed in a router. The identifier can be overwritten by repeating this command with a different identifier.

Please, notice that a BGP stack process restart is required upon configuration.

Example

This examples shows how to configure an AS confederation for BGP. The confederation is identified by the AS number 20.

```
DmSwitch#configure
DmSwitch(config)#router bgp
DmSwitch(config)#router bgp 2
DmSwitch(config-router-bgp)#bgp confederation identifier 20
% Warning:
  This command changes an attribute which may
  cause a flap of BGP process.
  Do you wish to continue? <y/N> y
DmSwitch(config-router-bgp)#exit
DmSwitch#
```

You can verify configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
bgp confederation peers	Set BGP confederation peers
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

bgp confederation peers

```
bgp confederation peers as-number [ ... as-number ]
```

```
no bgp confederation peers as-number [ ... as-number ]
```

Description

Use **bgp confederation peers** to configure a sub-AS that belongs to a BGP confederation.

Use the **no** form of this command to remove a sub-AS from the BGP confederation.

Syntax

Parameter	Description
<i>as-number</i>	AS number for BGP peers that will belong to the BGP confederation.

Default

No default value is defined.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

BGP protocol requires that all BGP routers within a given AS are fully-meshed. Such requirement leads to serious scalability problems. AS confederations for BGP avoid such problems by breaking down a large AS into a set of smaller AS's (sub-AS), which are still seen from the outside as a single AS, thus neutralizing the BGP fully-meshed routers requirement. The present command defines peers (sub-AS's) to be grouped into the confederation.

A confederation must have been previously configured, in order to be able to set a peer (sub-AS). For further information, please refer **bgp confederation identifier**.

Please, notice that a BGP stack process restart is required upon configuration.

Example

This examples shows how to configure peers (sub-AS's) into the confederation for BGP. The confederation is identified by the AS number 200, and the sub-AS's being configured are identified by the AS numbers 20, 21 and 22.

```
DmSwitch#configure
DmSwitch(config)#router bgp
DmSwitch(config)#router bgp 2
DmSwitch(config-router-bgp)#bgp confederation peers 21 22
% Warning:
  This command changes an attribute which may
  cause a flap of BGP process.
  Do you wish to continue? <y/N> y
DmSwitch(config-router-bgp)#exit
DmSwitch#
```

You can verify configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
bgp confederation identifier	Set BGP confederation identifier
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

bgp dampening

bgp dampening

no bgp dampening

Description

This command enables BGP route dampening. The router assesses a penalty each time a route flaps and adds this to any previously accumulated penalty value. Penalties are cumulative.

The **no** command disables **bgp dampening**.

Syntax

No parameter accepted.

Default

BGP Dampening is disabled by default.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Route dampening is a way to suppress flapping routes so that they are **suppressed** instead of being advertised. An unstable network leads BGP routes to flap, which can cause other BGP routers in the network to constantly reconverge. This wastes valuable CPU cycles and can cause severe problems in the network. As a good practice, most ISPs use route dampening regularly.

Use this command to enable the BGP dampening to an already created route-map.

Example

This example shows how to activate BGP dampening using the default values. Instructions to assign BGP dampening for a route-map are described in the **bgp dampening route-map** command description.

```
DmSwitch#config
DmSwitch(config)#router bgp 10
```

```
DmSwitch(config-router-bgp)#bgp dampening
```

You can verify the configuration by entering the **show ip bgp dampening parameters show ipv6 bgp dampening parameters** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

bgp dampening half-life

bgp dampening half-life *value*

no bgp dampening half-life

Description

A route that flaps gets a penalty of 100 for each flap. This command sets the time after which a penalty is decreased by half.

The **no** command disables **bgp dampening half-life**.

Syntax

Parameter	Description
<i>value</i>	Defines the half-life time in seconds (Range: 1 to 65535).

Default

The value is 300 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the BGP dampening half-life parameter value.

Example

This example shows how to configure half-life value of BGP dampening.

```
DmSwitch#config
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#bgp dampening half-life 400
```

You can verify the configuration by entering the **show ip bgp dampening parameters** and **show ipv6 bgp dampening parameters** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

bgp dampening max-suppress-time

bgp dampening max-suppress-time *seconds*

no bgp dampening max-suppress-time

Description

This command configures the maximum time in seconds that a route can remain as suppressed in case of instability.

The **no** command disables **bgp dampening max-suppress-time** .

Syntax

Parameter	Description
<i>seconds</i>	Defines the maximum suppress time value from 1 to 3600 seconds.

Default

Time value is 900 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the BGP dampening max-suppress-time parameter value.

Example

This example shows how to configure maximum suppress time for BGP dampening.

```
DmSwitch#config
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#bgp dampening max-suppress-time 1000
```


You can verify the configuration by entering the **show ip bgp dampening parameters show ipv6 bgp dampening parameters** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

bgp dampening reuse

bgp dampening reuse *value*

no bgp dampening reuse

Description

A route that flaps gets a penalty of 100 for each flap. The **reuse** parameter sets the threshold expressed as a number of route withdrawals. When the penalty falls below the reuse limit, the route is unsuppressed.

The **no** command disables **bgp dampening reuse**.

Syntax

Parameter	Description
<i>value</i>	Defines the reuse threshold (Range: 1 to 3600).

Default

The value is 50.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the BGP dampening reuse parameter value.

Example

This example shows how to configure reuse value of BGP dampening.

```
DmSwitch#config
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#bgp dampening reuse 40
```

In this case, if penalty is less than 40 (due to **half-life**), routes become unsupressed. You can verify the configuration by entering the **show ip bgp dampening parameters** **show ipv6 bgp dampening parameters** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

bgp dampening route-map

bgp dampening route-map *route-map-name*

no bgp dampening route-map *route-map-name*

Description

Specifies that dampening can be applied to routes according to the route map behaviour. If the route-map allows a route, the route is subject to dampening. Otherwise, the route is not subject to dampening.

The **no** command removes the already assigned route-map.

Syntax

Parameter	Description
<i>route-map-name</i>	Name of previously created route-map.

Default

No assigned Route-Map.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to assign a previously created Route-Map to suppress the BGP neighbor's advertisements in case of instability.

Example

This example shows how to assign a route-map for BGP dampening.

```
DmSwitch#config
DmSwitch(config)#route-map map1 permit 5
DmSwitch(config-route-map)#match as-path 100
DmSwitch(config-route-map)#set metric 5
DmSwitch(config-route-map)#exit
```

```
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 route-map map1 in
DmSwitch(config-router-bgp)#bgp dampening route-map map2
```

You can verify the configuration by entering the **show ip bgp dampening parameters show ipv6 bgp** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

bgp dampening suppress

bgp dampening suppress *value*

no bgp dampening suppress

Description

This command configures the numeric value that is compared with the penalty. If the penalty exceeds this suppress limit, the route will be suppressed. This value must be greater than or equal to reuse. The scale used is 100 times that is used in the RFC 2439.

The **no** command disables **bgp dampening suppress**.

Syntax

Parameter	Description
<i>value</i>	Defines the cutoff threshold to suppress the route (Range: 1 to 3600).

Default

Value 125.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the BGP dampening suppress parameter value.

Example

This example shows how to configure suppress value of BGP dampening.

```
DmSwitch#config
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#bgp dampening suppress 200
```

In this case, routes will be suppressed if the BGP session flaps twice, in the case dampening penalty is equal 100. You can verify the configuration by entering the **show ip bgp dampening parameters show ipv6 bgp dampening parameters** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

bgp default local-preference

bgp default local-preference *number*

no bgp default local-preference

Description

This command changes the default local-preference number.

Inserting **no** as a prefix for this command will set the local-preference number to its default value.

Syntax

Parameter	Description
<i>number</i>	Local preference value from 0 to 4294967294.

Default

By default, the local preference value is 0.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

The local preference attribute sets the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.

Example

The following example shows how to configure the local preference:

```
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#bgp default local-preference 200
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

bgp deterministic-med

bgp deterministic-med

no bgp deterministic-med

Description

This command establishes the deterministic Multi Exit Discriminator (MED) comparison for paths received inside the same AS.

Inserting **no** as a prefix for this command will disable the comparison.

Syntax

No parameter accepted.

Default

By default, deterministic MED comparison is active.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

The MED is used for selecting the best path among alternative paths. Its comparison becomes necessary when the paths belong to the same AS. The command **deterministic-med** enforces the comparison between routes from the same AS.

Example

The following example shows how to configure the deterministic MED comparison:

```
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#bgp deterministic-med
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>bgp always-compare-med</code>	Enables comparison of Multi Exit Discriminator (MED)

bgp_enforce_first_as

bgp enforce-first-as

no bgp enforce-first-as

Description

This command discards updates when peer's AS number is not the first one in AS_PATH.

The **no** will disable this command.

Default

enabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.6	This command was introduced.

Usage Guidelines

This command discards updates when peer's AS number is not the first in AS_PATH and by default it is always activated.

Example

This example shows how to disable this configuration.

```
DmSwitch(config-router-bgp) #no bgp enforce-first-as
DmSwitch(config-router-bgp) #
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

bgp graceful-restart

```
bgp graceful-restart [ {stalepath-time seconds | restart-time seconds |  
update-delay seconds} ]
```

```
no bgp graceful-restart [stalepath-time | restart-time | update-delay]
```

Description

This command enables and configures BGP graceful restart capability.

Inserting **no** as a prefix for this command will disable the BGP graceful restart. If **stalepath-time**, **restart-time** or **update-delay** is specified, inserting **no** prefix will restore the default value for these parameters.

Syntax

Parameter	Description
stalepath-time <i>seconds</i>	Defines the stalepath time value from 1 to 3600 seconds.
restart-time <i>seconds</i>	Defines the restart time value from 1 to 3600 seconds.
update-delay <i>seconds</i>	Defines the update delay (also know as deferral timer) value from 1 to 3600 seconds.

Default

By default, graceful-restart is disabled. Stalepath-time default value is 360 seconds. Restart-time default value is 120 seconds. Update-delay default value is 120 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.
12.2	Parameter "update-delay" was introduced.

Usage Guidelines

The `bgp graceful restart` command enables the capability of supporting non-stop-forwarding (NSF) between routers in a network. The timers values are optimal by default for most networks. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. Also, the update delay should not be set to a value smaller than the restart timer.

Example

The following example shows how to configure the graceful restart features using stalepath-time and restart-time:

```
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#bgp graceful-restart
DmSwitch(config-router-bgp)#bgp graceful-restart stalepath-time 300
DmSwitch(config-router-bgp)#bgp graceful-restart restart-time 100
DmSwitch(config-router-bgp)#bgp graceful-restart update-delay 130
```

You can verify the fill here by entering the **show running-config** or **show this** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

bgp log-neighbor-changes

bgp log-neighbor-changes

no bgp log-neighbor-changes

Description

Enables logging of BGP neighbor resets.

The **no** command cancel the logging.

Syntax

No parameter accepted.

Default

The command is disabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.6	This command was introduced.
9.4	This command was removed.
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to log neighbor changes for BGP.

```
DmSwitch(config-router-bgp)#bgp log-neighbor-changes
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip bgp</code>	Shows the BGP routing table entries.
<code>show running-config</code>	Shows the current operating configuration.

bgp router-id

bgp router-id *ip-address*

no bgp router-id

Description

Configures a static BGP router ID.

The **no** command restores the router ID to its default value.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of the router.

Default

The IP address configured on the loopback interface or the highest IP address configured on a VLAN interface.

Command Modes

Router BGP configuration.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Use this command to configure a static router ID as an identifier of the BGP process. A configured loopback interface is a better identifier than a fixed interface, since there is no physical link to go down.

Example

This example shows how to configure a fixed router ID for BGP.

```
DmSwitch(config-router-bgp) #bgp router-id 192.168.11.2
DmSwitch(config-router-bgp) #
```

You can verify the configuration by entering the **show ip bgp** privileged EXEC command.

Related Commands

Command	Description
<code>show ip bgp</code>	Shows the BGP routing table entries.
<code>show ipv6 bgp</code>	Shows the BGP routing table entries.

default-metric

default-metric *number*

no default-metric

Description

This command sets a metric for routes redistributed from other protocols (e.g. OSPF) into BGP.

Inserting **no** as a prefix for this command will set the metric to its default value.

Syntax

Parameter	Description
<i>number</i>	Default metric value from 0 to 4294967294.

Default

By default, the default-metric value is 0.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

This command is useful when routes from other protocols (e.g. OSPF) must be redistributed into BGP. After **redistribute** command, some routes can have incompatible metrics. By setting the default-metric, it establishes a default value for all routes.

Example

The following example shows how to configure the default metric:

```
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#default-metric 1024
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>redistribute</code>	Redistributes routes with a metric of BGP protocol.

distance

distance **bgp** *external_route* *internal_route*

no distance **bgp**

Description

This command sets the administrative distance for external and internal routes.

Inserting **no** as a prefix for this command will set the administrative distances to their default values.

Syntax

Parameter	Description
<i>external_route</i>	Administrative distance for external routes.
<i>internal_route</i>	Administrative distance for internal routes.

Default

By default, the external distance is 20 and the internal distance is 200.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.2	This command was introduced.

Usage Guidelines

This command sets the administrative distance for external and internal routes

Example

The following example shows how to configure the administrative distance:

```
DmSwitch(config)#router bgp 62551
DmSwitch(config-router-bgp)#distance bgp 30 190
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>router bgp</code>	Enables and accesses the BGP configuration.

neighbor activate

neighbor ip address activate

no neighbor ip address activate

Description

The command **neighbor activate** allows the exchange of information with a BGP neighbor.

Use the **no** for of this command to disable the exchange of information with a BGP neighbor.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of the neighboring router.

Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Address exchange for all other address families is disabled.

Command Modes

address-family vpnv4

Command History

Release	Modification
10.0	This command was introduced.
12.2	This command was deprecated.

Usage Guidelines

Use this command to advertise address information to a BGP neighbor. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

Example

The following example shows how to enable address exchange for address family vpnv4 for the neighbor 1.2.3.4:

```
DmSwitch(config-router-bgp) #address-family vpnv4
DmSwitch(config-router-bgp-af-vpnv4) #neighbor 1.2.3.4 activate
```

You can verify that the neighbor is activated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
show running-config	Shows the current operating configuration.

neighbor advertisement-interval

neighbor {*ip-address* | *ipv6-address*} **advertisement-interval** *seconds*

no neighbor {*ip-address* | *ipv6-address*} **advertisement-interval**

Description

Configures the advertisement interval of UPDATE message to BGP neighbor.

The **no** command resets the interval value to default value.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the router.
advertisement-interval <i>seconds</i>	Advertisement interval of UPDATE message to BGP neighbor.

Default

30 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

Use this command to configure the interval of UPDATE messages to be sent to the BGP neighbor.

Example

This example shows how to configure an advertisement interval of 60 seconds for BGP Update messages.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 advertisement-interval 60
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 advertisement-interval 60
```

```
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show ip bgp** or the **show ipv6 bgp** privileged EXEC command.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.

neighbor bfd enable

neighbor {*ip-address* | *ipv6-address*} **bfd enable**

no neighbor {*ip-address* | *ipv6-address*} **bfd enable**

Description

Enables or disables BFD support for this BGP neighbor.

The **no** command disables the BFD support.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.

Default

BFD support is disabled by default.

Command Modes

Router BGP configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

This command is used to enable or disable BFD support for a BGP neighbor. This configuration causes the BGP session to be reset.

Example

This example shows how to configure BFD support for a neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 bfd enable
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 bfd enable
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
neighbor bfd interval	Configure BFD interval parameters for a BGP neighbor.
show ip bfd neighbors	Show the state of all BFD IPv4 sessions.
show ipv6 bfd neighbors	Shows the state of all BFD IPv6 sessions.

neighbor bfd interval

neighbor {*ip-address* | *ipv6-address*} **bfd interval** *interval* **minrx** *minrx* **multiplier** *multiplier*

no neighbor {*ip-address* | *ipv6-address*} **bfd interval**

Description

Configures BFD interval parameters for this BGP neighbor.

The **no** command resets the parameters to their default values.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>interval</i>	Specifies the minimum desired interval to transmit BFD packets (in milliseconds). The ranges for the equipments DM4001, DM4004 and DM4008 are from 300 through 1000 and for DM4100 is 1000.
<i>minrx</i>	Specifies the minimum required interval to transmit BFD packets (in milliseconds). The ranges for the equipments DM4001, DM4004 and DM4008 are from 300 through 1000 and for DM4100 is 1000.
<i>multiplier</i>	Specifies the number of BFD packets from a peer that can be missed before reporting a failure. Range: 3-100

Default for equipments:

. DM4001, DM4004 and DM4008: Interval: 500 milliseconds. Minrx: 500 milliseconds. Multiplier: 3.

. DM4100: Interval and Minrx: 1000 milliseconds. Multiplier: 3.

Command Modes

Router BGP configuration.

Command History

Release	Modification
14.6	This command was introduced.

Usage Guidelines

Defines the minimum transmit and receive intervals of BFD packets, as well as the number of packets from a peer that can be missed before reporting a failure. Note that the actual transmit interval and failure detection time for a given BFD session is calculated based on the interval parameters of both peers that are part of the session. This configuration causes the BGP session to be reset.

Example

This example shows how to configure BFD interval parameters for a neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 bfd interval 350 minrx 350 mult 3
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 bfd interval 350 minrx 350 mult 3
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
neighbor bfd enable	Configure BFD support for a BGP neighbor.
show ip bfd neighbors	Show the state of all BFD IPv4 sessions.
show ipv6 bfd neighbors	Shows the state of all BFD IPv6 sessions.

neighbor description

neighbor {*ip-address* | *ipv6-address*} **description** *text*

no neighbor {*ip-address* | *ipv6-address*} **description**

Description

Associates a description to the specified BGP neighbor.

The **no** command removes the neighbor description.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>text</i>	Textual description associated with the neighbor router.

Default

No description.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

Use this command to configure a textual description for a BGP neighbor. The neighbor must exist in an already established BGP session.

Example

This example shows how to configure a description for a BGP neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 description Remote_DmSwitch
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 description Remote_DmSwitch_2
```

```
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor enforce first as

neighbor {*ip-address* | *ipv6-address*} **enforce-first-as**

no neighbor {*ip-address* | *ipv6-address*} **enforce-first-as**

Description

This feature is used to configure a Border Gateway Protocol (BGP) routing process to discard updates received from an external BGP (eBGP) peers that do not list their autonomous system (AS) number as the first AS path segment in the AS_PATH attribute of the incoming route. This command allows discards for routes advertised by individual neighbors.

The **no** command removes the **enforce-first-as** feature.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.

Default

No enforce first AS for individual neighbors.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

This command configures the discard of updates messages advertised to the specified neighbor.

Example

This example shows how to configure the discard of routes advertised by neighbor 172.16.88.131 in the case their AS_PATH does not contain its AS as first one.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 enforce-first-as
```

```
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
bgp enforce-first-as	Discards updates when peer's AS number isn't the first in AS_PATH

neighbor ebgp-multihop

neighbor {*ip-address* | *ipv6-address*} **ebgp-multihop** [*hop-count*]

no neighbor {*ip-address* | *ipv6-address*} **ebgp-multihop**

Description

Allows EBGp neighbors not on directly connected networks.

The **no** command disallow EBGp neighbors not on directly connected networks.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>hop-count</i>	Optional. Specify a maximum hop count for EBGp neighbors not on directly connected networks. Range 1-255. If omitted, maximum value 255 is assumed.

Default

Only directly connected EBGp neighbors.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

This feature should be used carefully.

Example

This example shows how to configure non-adjacent EBGp neighbors with maximum 125 hop count.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 ebgp-multihop 125
DmSwitch(config-router-bgp)#
```

```
DmSwitch(config-router-bgp)#neighbor 2001:DB8::1 ebgp-multihop 125
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor local-address

neighbor {*ip-address* | *ipv6-address*} **local-address** {*local-ip-address* | *local-ipv6-address*}

no neighbor {*ip-address* | *ipv6-address*} **local-address**

Description

Specifies a local IP address to communicate with a neighbor.

The **no** command removes the local IP address.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>local-ip-address</i> <i>local-ipv6-address</i>	Local IP address to be used to communicate with a neighbor.

Default

No local IP address.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

This command configures the source IP of messages advertised to the specified neighbor. A loopback address could, for instance, be used as an origin IP address.

Example

This example shows how to configure a local IP address 172.16.88.132 to communicate with neighbor 172.16.88.131 as IP address 172.16.95.131.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 local-address 172.16.95.131
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor local-port

neighbor {*ip-address* | *ipv6-address*} **local-port** *port*

no neighbor {*ip-address* | *ipv6-address*} **local-port**

Description

Specifies a local TCP port to communicate with a neighbor.

The **no** command removes the local TCP port.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>local-port</i>	Local TCP port to be used to communicate with a neighbor.

Default

No specific TCP port.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

Example

This example shows how to configure a local TCP port 1000 to communicate with neighbor 172.16.88.131.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 local-port 1000
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 local-port 1001
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor maximum-prefix

neighbor {*ip-address* | *ipv6-address*} **maximum-prefix** *number* [**warning-only**]

no neighbor {*ip-address* | *ipv6-address*} **maximum-prefix**

Description

Specifies maximum number of prefixes accepted from this neighbor.

The **no** command disable maximum number of prefixes accepted from this neighbor.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>number</i>	Number of prefixes accepted from this neighbor.
warning-only	(Optional) Allows the router to generate a log message when the maximum-prefix limit is exceeded, instead of terminating the peering session.

Default

No limit of prefixes.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

Allows the configuration of a maximum number of prefixes a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer. In the case the number of received prefixes exceeds the maximum number configured, the router terminates the peering. The **warning-only** parameter is not used to terminate the peering but rather to report a warning message into the system log.

Example

This example shows how to configure a maximum number of prefixes for a neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 maximum-prefix 1500 warning-only
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 maximum-prefix 1500 warning-only
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor next-hop-self

neighbor {*ip-address* | *ipv6-address*} **next-hop-self**

no neighbor {*ip-address* | *ipv6-address*} **next-hop-self**

Description

Disables next hop calculation and configures the switch as the next hop for a neighbor.

The **no** command restores next hop calculation.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.

Default

Next hop calculation enabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

This command is useful in non mashed networks where BGP neighbors might have no direct access to all neighbors in the same subnetwork.

Example

This example shows how to disable next hop calculation and configure switch as next hop for a neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 next-hop-self
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 next-hop-self
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor passive

neighbor {*ip-address* | *ipv6-address*} **passive**

no neighbor {*ip-address* | *ipv6-address*} **passive**

Description

This command specifies a passive connection with a neighbor. In this case, BGP speaker only accepts inbound connections from, but does not initiate outbound connections to, the peer or peer group.

The **no** command allows the initiation of outbound connections.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.

Default

Outbound connections enabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

Example

This example shows how to configure a neighbor as passive.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 passive
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 passive
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor password

neighbor {*ip-address* | *ipv6-address*} **password** *passwd*

no neighbor {*ip-address* | *ipv6-address*} **password**

Description

Defines the neighbor's MD5 encrypted password for BGP protocol.

The **no** command resets the password.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the BGP neighbor router.
password <i>passwd</i>	MD5 Password.

Default

No MD5 password is set.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set a MD5 password in order to establish a BGP neighborhood.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 password TEST
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 password TEST2
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

neighbor port

neighbor {*ip-address* | *ipv6-address*} **port** *port*

no neighbor {*ip-address* | *ipv6-address*} **port**

Description

Specifies a remote TCP port to communicate with a neighbor.

The **no** command removes the remote TCP port.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>port</i>	Remote TCP port to be used to communicate with a neighbor.

Default

No specific TCP port.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a remote TCP port 1000 to communicate with neighbor 172.16.88.131.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 port 1000
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor prefix-list

```
neighbor ip address prefix-list prefix-list-name {in|out}
```

```
no neighbor ip address prefix-list prefix-list-name {in|out}
```

Description

Prefix-lists are a way of filtering and controlling the BGP neighbor's advertisements. Prior to being used by a BGP router, they have to be created via **ip prefix-list** command(IPv4 and/or IPv6).

The **no** command undoes the already assigned prefix-list.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of BGP neighbor.
<i>ipv6-address</i>	IPv6 address of BGP neighbor.
<i>prefix-list-name</i>	Name of prefix-list previously created.
in	Prefix-list rule is valid for incoming routes.
out	Prefix-list rule is valid for outgoing routes.

Default

No assigned Prefix-List.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

Use this command to assign a previously created Prefix-List to filter the BGP neighbor's advertisements. Prefix list is one of two ways to filter BGP advertisements. The other way is to use AS-path filters under Route-Maps.

Example

This example shows how to assign a prefix-list for BGP.

```
DmSwitch#config
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 prefix-list list1 in
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 prefix-list list2 out
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 prefix-list list3 in
```

You can verify the configuration by entering the **show ip bgp** or the **show ipv6 bgp** privileged EXEC command.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
ip prefix-list	Configure a prefix list.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

neighbor peer-group

neighbor {*ip-address* | *ipv6-address*} **peer-group** *name*

no neighbor {*ip-address* | *ipv6-address*} **peer-group** *name*

Description

Creates a neighbor based on peer-group *text*. If the neighbor already exists, it imports all configurations from peer-group *name*, except the ones that were previously defined in the neighbor.

The **no** option detaches the neighbor from the peer-group *name*. The neighbor retains all peer-group configurations.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the BGP neighbor router.
peer-group <i>name</i>	Name of the peer-group.

Default

No peer-group is linked to the neighbor.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to define a peer-group and add neighbor routers IP address that share the same policies and configurations from the peer-group.

```
DmSwitch(config-router-bgp)#peer-group EBGp
DmSwitch(config-router-bgp-peergr-EBGP)#remote-as 1000
```

```
DmSwitch(config-router-bgp-peergr-EBGP)#advertisement-interval 10
DmSwitch(config-router-bgp-peergr-EBGP)#next-hop-self
DmSwitch(config-router-bgp-peergr-EBGP)#exit
DmSwitch(config-router-bgp)#
```

With the peer-group "EBGP" configured, it is possible to add a set of neighbors sharing the same set of configurations

```
DmSwitch(config-router-bgp)#neighbor 10.11.12.1 peer-group EBGP
DmSwitch(config-router-bgp)#neighbor 10.12.12.1 peer-group EBGP
DmSwitch(config-router-bgp)#neighbor 10.13.12.1 peer-group EBGP
DmSwitch(config-router-bgp)#show this
router bgp 1
  peer-group EBGP
    remote-as 1000
    advertisement-interval 10
    next-hop-self
  neighbor 10.11.12.1 peer-group EBGP
  neighbor 10.12.12.1 peer-group EBGP
  neighbor 10.13.12.1 peer-group EBGP
!
DmSwitch(config-router-bgp)#show ip bgp peer-group
BGP peer-group is EBGP, remote AS 1000
  BGP Version 4.
  Status is Active
  Peer-group is external, members:
    10.11.12.1
    10.12.12.1
    10.13.12.1
```

You can verify that the neighbor was defined by entering the **show ip bgp neighbors** privileged EXEC command.

Related Commands

Command	Description
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.
peer-group	Defines a peer-group router.
neighbor description	Associates a description to the specified BGP neighbor.
neighbor	Allows soft reconfiguration.
soft-reconfiguration inbound	
neighbor shutdown	Shutdown session with a neighbor.
neighbor advertisement-interval	Configures the advertisement interval of UPDATE message to BGP neighbor.
neighbor route-reflector-client	Configure a neighbor as Route Reflector client.
neighbor remove-private-as	Removes private AS number from outbound updates.
neighbor prefix-list	Configures the filtering of BGP neighbor's advertisements.
neighbor passive	Disables routes advertisement.
neighbor maximum-prefix	Defines the maximum number of prefixes.

Command	Description
neighbor local-address	Defines a local IP address for BGP neighbor.
neighbor ebgp-multihop	Allows non-adjacent EBGp neighbors.
neighbor next-hop-self	Disable the next hop calculation.
neighbor port	Defines a remote TCP port for BGP neighbor.
neighbor remote-as	Creates a BGP neighbor.
neighbor timers	Configure BGP timers per neighbor.

neighbor remote-as

neighbor {*ip-address* | *ipv6-address*} **remote-as** *AS-number*

no neighbor {*ip-address* | *ipv6-address*} **remote-as** *AS-number*

Description

Creates a BGP neighbor.

The **no** command deletes the BGP neighbor.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>AS-number</i>	Autonomous System of the peer-group router (Range: 1-4294967295 in AS_PLAIN format, [1-65535].[1-65535] in AS_DOT format).

Default

No neighbors created.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

A neighbor with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the neighbor as internal to the local autonomous system.

Example

This example shows how to create a neighbor.


```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 remote-as 10
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 remote-as 10
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**, **show ip bgp neighbors**, **show ip bgp summary**, **show ipv6 bgp neighbors** or **show ipv6 bgp summary**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.

neighbor remove-private-as

```
neighbor {ip-address | ipv6-address} remove-private-as
```

```
no neighbor {ip-address | ipv6-address} remove-private-as
```

Description

Removes private AS from outbound updates to a neighbor.

The **no** command keeps private AS from outbound updates to a neighbor.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of the neighbor router.
<i>ipv6-address</i>	IPv6 address of the neighbor router.

Default

Keep private AS.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

This feature is available for EBGp neighbors only. When an update message is advertised to the external neighbor, the software will drop the private autonomous system numbers if the AS-path includes private autonomous system numbers. If the AS-path contains the autonomous system number of the EBGp neighbor, the private autonomous system numbers will not be removed. The private autonomous system values are from 64512 to 65535.

Example

This example shows how to remove private AS from outbound update to a neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 remove-private-as
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:DB8::1 remove-private-as
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
router bgp	Enables and accesses the BGP configuration.

neighbor route-map

```
neighbor {ip-address | ipv6-address} route-map route-map-name {in | out}
```

```
no neighbor {ip-address | ipv6-address} route-map route-map-name {in | out}
```

Description

Route-maps are a way of filtering and modifying the BGP neighbor's advertisements. Such an advertisement control and setting occurs via definition of redistribution conditions. This is done via command **route-map**

The **no** command undoes the already assigned route-map.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of BGP neighbor.
<i>route-map-name</i>	Name of route-map previously created.
in	Prefix-list rule is valid for incoming routes.
out	Prefix-list rule is valid for outgoing routes.

Default

No assigned Route-Map.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.
11.0	Added IPv6 support.

Usage Guidelines

Use this command to assign a previously created Route-Map to filter and modify the BGP neighbor's advertisements.

Example

This example shows how to assign a route-map for BGP.

```

DmSwitch#config
DmSwitch(config)#route-map map1 permit 5
DmSwitch(config-route-map)#match as-path 100
DmSwitch(config-route-map)#set metric 5
DmSwitch(config)#route-map map2 permit 3
DmSwitch(config-route-map)#match as-path 150
DmSwitch(config-route-map)#set metric 10
DmSwitch(config-router-bgp)#router bgp 10
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 route-map map1 in
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 route-map map2 out

```

You can verify the configuration by entering the **show ip bgp** or the **show ipv6 bgp** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
description	Insert descriptive text for the route map rule.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

neighbor route-reflector-client

neighbor {*ip-address* | *ipv6-address*} **route-reflector-client**

no neighbor {*ip-address* | *ipv6-address*} **route-reflector-client**

Description

Configures the router as Route Reflector server and register a neighbor as client.

The **no** command disables Route Reflector server and unregister neighbor as client.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.

Default

Route Reflector server disabled with no clients.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use this command in router configuration mode. If there is not at least one registered client, the local router does not act as route reflector.

Example

This example shows how to enable Route Reflector and register a neighbor as client.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 route-reflector-client
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:DB8::1 route-reflector-client
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config** or **show ip bgp neighbors**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.

neighbor send-label ^[1] ^[3] ^[5]

neighbor *ip address* **send-label**

no neighbor *ip address* **send-label**

Description

Use the **neighbor send-label** command to enable RFC3107 Carrying Label Information in BGP-4.

The **no** command disables RFC3107 Carrying Label Information in BGP-4.

Syntax

Parameter	Description
<i>ip-address</i>	IP address of the neighboring router.

Cross Dependencies

Enabling this command will activate the **mpls bgp forwarding** command on all VLAN whose network contains this neighbor.

Default

There is no default configuration.

Command Modes

address-family ipv4

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

Use this command to advertise label information to a BGP neighbor. Also configure **mpls ldp control-mode independent** in order to support LDP-BGP LSP's. Moreover, the neighbor *ip address* must be contained in some VLAN network with mask /30 or /31.

Example

The following example shows how to enable label exchange for address family IP version4 for the neighbor 1.2.3.4:

```
DmSwitch(config-router-bgp)#address-family ipv4
DmSwitch(config-router-bgp-af-ipv4)#neighbor 1.2.3.4 send-label
```

You can verify that the neighbor is activated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
show running-config	Shows the current operating configuration.
mpls ldp control-mode	Specifies the label distribution mode of LDP.
mpls bgp forwarding	Enable MPLS traffic forwarding in selected VLAN.

neighbor shutdown

neighbor {*ip-address* | *ipv6-address*} **shutdown**

no neighbor {*ip-address* | *ipv6-address*} **shutdown**

Description

Administratively shut down this neighbor BGP session and remove all associated routes.

The **no** command administratively bring up this neighbor BGP session.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.

Default

Neighbors BGP sessions are created administratively up.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

This command terminates any active session for the specified neighbor and removes all associated routing information.

Example

This example shows how to shut down a neighbor BGP session.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 shutdown
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 shutdown
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor soft-reconfiguration inbound

```
neighbor {ip-address | ipv6-address} soft-reconfiguration inbound
```

```
no neighbor {ip-address | ipv6-address} soft-reconfiguration inbound
```

Description

Allows storage of UPDATE messages needed for reconfiguration and policies to be configured and activated without clearing the BGP session.

The **no** command disables soft reconfiguration.

Syntax

Parameter	Description
<i>ip-address ipv6-address</i>	IP address of the neighbor router.

Default

Soft reconfiguration is disabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
5.0	This command was introduced.

Usage Guidelines

This is memory intensive and should be avoided. On the other hand, outbound soft reconfiguration does not have any memory overhead.

Example

This example shows how to enable soft reconfiguration.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 soft-reconfiguration inbound
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 soft-reconfiguration inbound
```

```
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

neighbor timers

```
neighbor {ip-address | ipv6-address} timers keepalive-interval holdtime-interval
```

```
no neighbor {ip-address | ipv6-address} timers
```

Description

Configures keep alive and hold time intervals for a BGP neighbor. Per neighbor timers settings prevail over global BGP timers values for the specified neighbor.

The **no** command set timers to default values.

Syntax

Parameter	Description
<i>ip-address</i> <i>ipv6-address</i>	IP address of the neighbor router.
<i>keepalive-interval</i>	Interval in seconds which keep alive messages are sent to the neighbor. Range: 0-65535.
<i>holdtime-interval</i>	Interval in seconds without receiving keep alive messages before considering a neighbor down. Range: 0 or 3-65535.

Default

Keep alive: 60 seconds.

Hold time: 180 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.2	The configuration sequence of parameters keepalive and holdtime for timers bgp and neighbor timers commands has been changed in order to be the same in both cases.
11.0	Added IPv6 support.
9.4	This command was introduced.

Usage Guidelines

Using this command for a specific neighbor or peer group override the timers configured for all BGP neighbors. If Hold time is set to zero it will not be used, and Keepalive value is ignored. Hold time must be greater than Keepalive (preferably, 3 times).

Example

This example shows how to set BGP timers to a neighbor.

```
DmSwitch(config-router-bgp)#neighbor 172.16.88.131 timers 45 150
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#neighbor 2001:db8::1 timers 45 150
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**, **show ip bgp neighbors** or **show ipv6 bgp neighbors**.

Related Commands

Command	Description
router bgp	Enables and accesses the BGP configuration.
show running-config	Shows the current operating configuration.

network

network {*ip-address/mask* | *ipv6-address/prefix*}

no network {*ip-address/mask* | *ipv6-address/prefix*}

Description

Specify a network to be announced via BGP.

Entering with **no** command, it dissociates the concerned network of the BGP protocol.

Syntax

Parameter	Description
<i>ip-address/mask</i> <i>ipv6-address/prefix</i>	Specifies the network.

Default

No network is announced via BGP.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.0	Added IPv6 support.
10.0	This command was introduced again.
9.4	This command was removed.
7.6	This command was introduced.

Usage Guidelines

The BGP process will act only over associated networks, where they will advertise and listen for BGP updates.

Example

This example shows how to associate a network with the BGP protocol.

```
DmSwitch(config-router-bgp)#network 10.11.12.0/24
DmSwitch(config-router-bgp)#
DmSwitch(config-router-bgp)#network 2001:db8::/32
```



```
DmSwitch(config-router-bgp)#
```

You can verify that the network was associated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
redistribute	Redistributes routes with a metric of BGP protocol.
ip prefix-list	Configure a prefix list.
route-map	Create route-map or enter route-map command mode.
show ip bgp	Shows the BGP routing table entries.
show ipv6 bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

peer-group

peer-group *name*

no peer-group *name*

Description

Defines a peer-group to exchange routing information. You will often find it more convenient to enter your set(s) of configurations and policies so that they apply to a group of neighbors, rather than a single neighbor. Additionally, you may want to apply policy only once for an entire group of neighbors. For these reasons, neighbors can be grouped using the peer-group set of commands.

Entering with **no** command, it deletes a peer-group.

Syntax

Parameter	Description
<i>name</i>	Specify the peer-group name.

Default

No default peer-group is defined.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Add an entry to the BGP peer-group table specifying that the peer-group identified by the *name* has a set of configurations that will be applied to a number of neighbors. Once the group of neighbors is created with the command "**neighbor** *ip-address* **peer-group** *name*", any configurations that are applied to the peer-group, is also applied to all neighbors belonging to the peer-group.

Example

This example shows how to define a peer-group and add neighbor routers IP address that share the same policies and configurations from the peer-group.

```
DmSwitch(config-router-bgp)#peer-group EBGp
DmSwitch(config-router-bgp-peergr-EBGP)#remote-as 1000
DmSwitch(config-router-bgp-peergr-EBGP)#advertisement-interval 10
DmSwitch(config-router-bgp-peergr-EBGP)#next-hop-self
DmSwitch(config-router-bgp-peergr-EBGP)#exit
DmSwitch(config-router-bgp)#
```

The same set of configurations from above can be configured in a different way. The next example show how to configure a peer-group without having to enter the peer-group tree:

```
DmSwitch(config-router-bgp)#peer-group EBGp remote-as 1000
% Warning:
New peer-group created.
DmSwitch(config-router-bgp)#peer-group EBGp advertisement-interval 10
DmSwitch(config-router-bgp)#peer-group EBGp next-hop-self
```

With the peer-group "EBGP" configured, it is possible to add a set of neighbors sharing the same set of configurations

```
DmSwitch(config-router-bgp)#neighbor 10.11.12.1 peer-group EBGp
DmSwitch(config-router-bgp)#neighbor 10.12.12.1 peer-group EBGp
DmSwitch(config-router-bgp)#neighbor 10.13.12.1 peer-group EBGp
DmSwitch(config-router-bgp)#show this
router bgp 1
peer-group EBGp
remote-as 1000
advertisement-interval 10
next-hop-self
neighbor 10.11.12.1 peer-group EBGp
neighbor 10.12.12.1 peer-group EBGp
neighbor 10.13.12.1 peer-group EBGp
!
DmSwitch(config-router-bgp)#show ip bgp peer-group
BGP peer-group is EBGp, remote AS 1000
BGP Version 4.
Status is Active
Peer-group is external, members:
10.11.12.1
10.12.12.1
10.13.12.1
```

You can verify that the neighbor was defined by entering the **show ip bgp neighbors** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
network	Specify a network to announce via BGP.
redistribute	Redistributes routes with a metric of BGP protocol.
show ip bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

peer-group activate

peer-group *name* **activate**

no peer-group *name* **activate**

Description

Use the **peer-group activate** command to enable the exchange of information with a BGP neighbor.

Use the **no** for this command to disable the exchange of information with a BGP neighbor.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

The exchange of addresses with BGP neighbors and peer-groups is enabled for the IPv4 address family. Address exchange for all other address families is disabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to allow a peer-group to advertise address information to a BGP neighbor. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

Example

The following example shows how to enable address exchange for address family vpnv4 for the peer-group "IBGP":

```
DmSwitch(config-router-bgp)#address-family vpnv4
DmSwitch(config-router-bgp-af-vpnv4)#peer-group IBGP activate
```

You can verify that the neighbor is activated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
show running-config	Shows the current operating configuration.

peer-group advertisement-interval

```
peer-group name advertisement-interval seconds
```

```
no peer-group name advertisement-interval
```

Description

Configures the advertisement interval of UPDATE message to BGP peer-group.

The **no** command resets the interval value to default value.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
advertisement-interval <i>seconds</i>	Advertisement interval of UPDATE message to BGP peer-group.

Default

30 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to configure the interval of UPDATE messages to be sent to the BGP neighbor by the peer-group.

Example

This example shows how to configure an advertisement interval of 60 seconds for BGP Update messages.

```
DmSwitch(config-router-bgp)#peer-group IBGP advertisement-interval 60
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show ip bgp** privileged EXEC command.

Related Commands

Command	Description
show ip bgp	Shows the BGP routing table entries.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group description

peer-group *name* **description** *text*

no peer-group *name* **description**

Description

Associates a description to the specified BGP peer-group.

The **no** command removes the peer-group description.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>text</i>	Textual description associated with the peer-group.

Default

No description.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to configure a textual description for a BGP peer-group. The peer-group must exist in an already established BGP session.

Example

This example shows how to configure a description for a BGP peer-group.

```
DmSwitch(config-router-bgp) #peer-group IBGP description Internal BGP peer-group
DmSwitch(config-router-bgp) #
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
 peer-group local-address	 Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGP peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group ebgp-multihop

peer-group *name* **ebgp-multihop** [*hop-count*]

no peer-group *name* **ebgp-multihop**

Description

Allows EBGp peer-groups not on directly connected networks.

The **no** command disallow EBGp peer-groups not on directly connected networks.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>hop-count</i>	Optional. Specify a maximum hop count for EBGp peer-groups not on directly connected networks. Range 1-255. If omitted, maximum value 255 is assumed.

Default

Only directly connected EBGp peer-groups.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This feature should be used carefully.

Example

This example shows how to configure non-adjacent EBGp peer-groups with maximum 125 hop count.

```
DmSwitch(config-router-bgp)#peer-group EBGp_PG ebgp-multihop 125
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group local-address

peer-group *name* **local-address** *local-name*

no peer-group *name* **local-address**

Description

Specifies a local IP address to communicate for a peer-group.

The **no** command removes the local IP address.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>local-name</i>	Local IP address to be used to communicate for a peer-group.

Default

No local IP address.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command configures the source IP of messages advertised to the specified peer-group. A loopback address could, for instance, be used as an origin IP address.

Example

This example shows how to configure a local IP address to communicate for a peer-group named IBGP as IP address 172.16.95.131.

```
DmSwitch(config-router-bgp)#peer-group IBGP local-address 172.16.95.131
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group local-port

peer-group *name* **local-port** *port*

no peer-group *name* **local-port**

Description

Specifies a local TCP port to communicate for a peer-group.

The **no** command removes the local TCP port.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>local-port</i>	Local TCP port to be used to communicate for a peer-group.

Default

No specific TCP port.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Example

This example shows how to configure a local TCP port 1000 to communicate for peer-group EBGP.

```
DmSwitch(config-router-bgp) #peer-group EBGP local-port 1000
DmSwitch(config-router-bgp) #
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

peer-group maximum-prefix

peer-group *name* **maximum-prefix** *number* [**warning-only**]

no peer-group *name* **maximum-prefix**

Description

Specifies maximum number of prefixes accepted from this peer-group.

The **no** command disable maximum number of prefixes accepted from this peer-group.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>number</i>	Number of prefixes accepted from this peer-group.
warning-only	(Optional) Allows the router to generate a log message when the maximum-prefix limit is exceeded, instead of terminating the peering session.

Default

No limit of prefixes.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Allows the configuration of a maximum number of prefixes a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer. In the case the number of received prefixes exceeds the maximum number configured, the router terminates the peering. The **warning-only** parameter is not used to terminate the peering but rather to report a warning message into the system log.

Example

This example shows how to configure a maximum number of prefixes for a peer-group named EBGp.

```
DmSwitch(config-router-bgp) #peer-group EBGp maximum-prefix 1500 warning-only
DmSwitch(config-router-bgp) #
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group next-hop-self

peer-group *name* **next-hop-self**

no peer-group *name* **next-hop-self**

Description

Disables next hop calculation and configures the switch as the next hop for a peer-group.

The **no** command restores next hop calculation.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

Next hop calculation enabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command is useful in non mashed networks where BGP peer-groups might have no direct access to all peer-groups in the same subnetwork.

Example

This example shows how to disable next hop calculation and configure switch as next hop for a peer-group.

```
DmSwitch(config-router-bgp)#peer-group GROUP next-hop-self
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

peer-group passive

peer-group *name* **passive**

no peer-group *name* **passive**

Description

Configures the relationship with a peer-group as passive, that is, do not advertise routes to a peer-group.
The **no** command enables routes advertisement.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

Routes advertisement enabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Example

This example shows how to configure a peer-group as passive.

```
DmSwitch(config-router-bgp)#peer-group GROUP passive
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group port

peer-group *name* **port** *port*

no peer-group *name* **port**

Description

Specifies a remote TCP port to communicate with a peer-group.

The **no** command removes the remote TCP port.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>port</i>	Remote TCP port to be used to communicate with a peer-group.

Default

No specific TCP port.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure a remote TCP port 1000 to communicate with peer-group 172.16.88.131.

```
DmSwitch(config-router-bgp)#peer-group GROUP port 1000
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group prefix-list

```
peer-group Name prefix-list prefix-list-name {in|out}
```

```
no peer-group Name prefix-list prefix-list-name {in|out}
```

Description

Prefix-lists are a way of filtering and controlling the BGP peer-group's advertisements. Prior to being used by a BGP router, they have to be created via command **ip prefix-list**

The **no** command undoes the already assigned prefix-list.

Syntax

Parameter	Description
<i>name</i>	Name of BGP peer-group.
<i>prefix-list-name</i>	Name of prefix-list previously created.
in	Prefix-list rule is valid for incoming routes.
out	Prefix-list rule is valid for outgoing routes.

Default

No assigned Prefix-List.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to assign a previously created Prefix-List to filter the BGP peer-group's advertisements. Prefix list is one of two ways to filter BGP advertisements. The other way is to use AS-path filters under Route-Maps.

Example

This example shows how to assign a prexix-list for BGP.


```
DmSwitch#config
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#peer-group EBGp prefix-list list1 in
DmSwitch(config-router-bgp)#peer-group EBGp prefix-list list2 out
```

You can verify the configuration by entering the **show ip bgp** privileged EXEC command.

Related Commands

Command	Description
ip prefix-list	Configure a prefix list.
show ip bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group password

peer-group *name* **password** *passwd*

no peer-group *name* **password**

Description

Defines the peer-group's MD5 encrypted password for BGP protocol.

The **no** command resets the password.

Syntax

Parameter	Description
<i>name</i>	Name of the BGP peer-group.
password <i>passwd</i>	MD5 Password.

Default

No MD5 password is set.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set a MD5 password in order to establish a BGP peer-group neighborhood.

```
DmSwitch(config-router-bgp)#peer-group IBGP password TEST
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.

peer-group remote-as

peer-group *name* **remote-as** *AS-number*

no peer-group *name* **remote-as** *AS-number*

Description

Configures a BGP peer-group remote AS.

The **no** command resets the BGP peer-group remote-as.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.
<i>AS-number</i>	Autonomous System of the peer-group router (Range: 1-4294967295 in AS_PLAIN format, [1-65535].[1-65535] in AS_DOT format).

Default

No peer-groups remote-as set.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

A peer-group with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the peer-group as internal to the local autonomous system. In addition, a peer-group with an autonomous system number that differs the autonomous system number specified in the router bgp global configuration, and matches a remote-AS that was configured as in confederation, identifies the peer-group as In Confederation to the local autonomous system. Any other AS configuration identifies the peer-group as External to the local autonomous system.

Notice that, if the peer-group has no remote-as configuration, and no neighbor members, a peer-group identification area is undefined. It leaves this state until a remote-AS is configured in the peer-group, or the first neighbor

member is configured to be in the peer-group.

Example

This example shows how to set a peer-group remote AS in order to identify it as internal.

```
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#peer-group IBGP remote-as 10
DmSwitch(config-router-bgp)#
```

The next example shows how to set a peer-group named remote AS in order to identify it as external.

```
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#peer-group EBGP remote-as 500
DmSwitch(config-router-bgp)#
```

In this case, all neighbors that will be created as a member of this peer-group will belong to the peer-group remote AS.

```
DmSwitch(config-router-bgp)#neighbor 15.15.15.15 peer-group EBGP
DmSwitch(config-router-bgp)#
```

As a remark, it is also possible for existing neighbors with different remote-AS than the peer-group to be a member of this peer-group, as long as their remote AS are identified to belong to the same area (internal, in confederation or external) as the peer-group. The next example illustrates this situation.

```
DmSwitch(config)#router bgp 10
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 remote-as 30
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 description External AS neighbor
DmSwitch(config-router-bgp)#neighbor 2.2.2.2 remote-as 10
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 description Internal AS neighbor
DmSwitch(config-router-bgp)#peer-group EBGP
DmSwitch(config-router-bgp-peergr-EBGP)#remote-as 600
DmSwitch(config-router-bgp-peergr-EBGP)#exit
DmSwitch(config-router-bgp)#neighbor 1.1.1.1 peer-group
DmSwitch(config-router-bgp)#neighbor 2.2.2.2 peer-group
% 7: Invalid parameter
% External peer-group must not have internal neighbors.
```

You can verify the configuration by entering the **show running-config** or **show ip bgp peer-groups**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show ip bgp	Shows the BGP routing table entries.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.

Command	Description
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group remove-private-as

peer-group *name* **remove-private-as**

no peer-group *name* **remove-private-as**

Description

Removes private AS from outbound updates to a peer-group.

The **no** command keeps private AS from outbound updates to a peer-group.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

Keep private AS.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This feature is available for EBGp peer-groups only. When an update message is advertised to the external peer-group, the software will drop the private autonomous system numbers if the AS-path includes private autonomous system numbers. If the AS-path contains the autonomous system number of the EBGp peer-group, the private autonomous system numbers will not be removed. The private autonomous system values are from 64512 to 65535 for 16bit AS's.

Example

This example shows how to remove private AS from outbound update to a peer-group.

```
DmSwitch(config-router-bgp)#peer-group EBGp remove-private-as
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGP peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group route-map

```
peer-group name route-map route-map-name {in|out}
```

```
no peer-group Name route-map route-map-name {in|out}
```

Description

Route-maps are a way of filtering and modifying the BGP peer-group's advertisements. Such an advertisement control and setting occurs via definition of redistribution conditions. This is done via command **route-map**

The **no** command undoes the already assigned route-map.

Syntax

Parameter	Description
<i>name</i>	Name of BGP peer-group.
<i>route-map-name</i>	Name of route-map previously created.
in	Prefix-list rule is valid for incoming routes.
out	Prefix-list rule is valid for outgoing routes.

Default

No assigned Route-Map.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to assign a previously created Route-Map to filter and modify the BGP peer-group's advertisements.

Example

This example shows how to assign a route-map for BGP.

```

DmSwitch#config
DmSwitch(config)#route-map map1 permit 5
DmSwitch(config-route-map)#match as-path 100
DmSwitch(config-route-map)#set metric 5
DmSwitch(config)#route-map map2 permit 3
DmSwitch(config-route-map)#match as-path 150
DmSwitch(config-route-map)#set metric 10
DmSwitch(config-router-bgp)#router bgp 10
DmSwitch(config-router-bgp)#peer-group GROUP route-map map1 in
DmSwitch(config-router-bgp)#peer-group GROUP route-map map2 out

```

You can verify the configuration by entering the **show ip bgp** privileged EXEC command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show ip bgp	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

peer-group route-reflector-client

peer-group *name* **route-reflector-client**

no peer-group *name* **route-reflector-client**

Description

Configures the router as Route Reflector server and register a peer-group as client.

The **no** command disables Route Reflector server and unregister peer-group as client.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

Route Reflector server disabled with no clients.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

To configure the router as a BGP route reflector and configure the specified peer-group as its client, use this command in router configuration mode. If there is not at least one registered client, the local router does not act as route reflector.

Example

This example shows how to enable Route Reflector and register a peer-group as client.

```
DmSwitch(config-router-bgp)#peer-group GROUP route-reflector-client
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show ip bgp	Shows the BGP routing table entries.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGP peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group shutdown

peer-group *name* **shutdown**

no peer-group *name* **shutdown**

Description

Administratively shut down all neighbors member of the peer-group and remove all associated routes.

The **no** command administratively bring up the neighbor BGP session, members of the peer-group.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

Neighbors BGP sessions and peer-groups are created administratively up.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command terminates any active session for the specified peer-group members and removes all associated routing information.

Example

This example shows how to shut down a peer-group BGP session.

```
DmSwitch(config-router-bgp)#peer-group GROUP shutdown
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group soft-reconfiguration inbound

```
peer-group name soft-reconfiguration inbound
```

```
no peer-group name soft-reconfiguration inbound
```

Description

Allows storage of UPDATE messages needed for reconfiguration and policies to be configured and activated without clearing the BGP session.

The **no** command disables soft reconfiguration.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group.

Default

Soft reconfiguration is disabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This is memory intensive and should be avoided. On the other hand, outbound soft reconfiguration does not have any memory overhead.

Example

This example shows how to enable soft reconfiguration.

```
DmSwitch(config-router-bgp)#peer-group GROUP soft-reconfiguration inbound
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group timers	Configure BGP timers per peer-group.
peer-group password	Configures BGP's peer-group MD5 PW.

peer-group timers

peer-group *name* **timers** *keepalive-interval holdtime-interval*

no peer-group *name* **timers**

Description

Configures keep alive and hold time intervals for a BGP peer-group. Per neighbor timers settings prevail over global BGP timers values for the members of the specified peer-group.

The **no** command set timers to default values.

Syntax

Parameter	Description
<i>name</i>	Name of the peer-group router.
<i>keepalive-interval</i>	Interval in seconds which keep alive messages are sent to the peer-group. Range: 0-65535.
<i>holdtime-interval</i>	Interval in seconds without receiving keep alive messages before considering a peer-group down. Range: 0 or 3-65535.

Default

Keep alive: 60 seconds.

Hold time: 180 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Using this command for a specific peer-group overrides the timers configured for all BGP peer-group members. If Hold time is set to zero it will not be used, and Keepalive value is ignored. Hold time must be greater than Keepalive (preferably, 3 times).

Example

This example shows how to set BGP timers to a peer-group.

```
DmSwitch(config-router-bgp)#peer-group GROUP timers 45 150
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config**.

Related Commands

Command	Description
show running-config	Shows the current operating configuration.
show ip bgp peer-groups	Shows the BGP routing table entries.
peer-group description	Associates a description to the specified BGP peer-group.
peer-group soft-reconfiguration inbound	Allows soft reconfiguration.
peer-group shutdown	Shutdown session with a peer-group.
peer-group advertisement-interval	Configures the advertisement interval of UPDATE message to BGP peer-group.
peer-group route-reflector-client	Configure a peer-group as Route Reflector client.
peer-group remove-private-as	Removes private AS number from outbound updates.
peer-group prefix-list	Configures the filtering of BGP peer-group's advertisements.
peer-group passive	Disables routes advertisement.
peer-group maximum-prefix	Defines the maximum number of prefixes.
peer-group local-address	Defines a local IP address for BGP peer-group.
peer-group ebgp-multihop	Allows non-adjacent EBGp peer-groups.
peer-group next-hop-self	Disable the next hop calculation.
peer-group port	Defines a remote TCP port for BGP peer-group.
peer-group remote-as	Configures BGP peer-group remote-as.
peer-group password	Configures BGP's peer-group MD5 PW.

redistribute

```
redistribute { connected | ospf | rip | static } [ metric metric-value | route-map name ]
```

```
no redistribute { connected | ospf | rip | static } [ metric | route-map ]
```

Description

Redistributes connected, OSPF, RIP or static routes, with a specific or default metric or route-map of BGP protocol.

Entering with **no** command, it stops the redistribution of the specified routes types.

Syntax

Parameter	Description
connected	Redistributes connected routes.
ospf	Redistributes OSPF routes.
rip	Redistributes RIP routes.
static	Redistributes configured static routes.
metric <i>metric-value</i>	(Optional) Specifies a metric. (Range: 0-4294967294)
route-map <i>name</i>	(Optional) Specifies a route-map reference name.

Default

No redistribution routes are defined.

Command Modes

Router BGP configuration.

Command History

Release	Modification
7.6	This command was introduced.
4.0	Redistribution of BGP routes has been included. The minimum value for metric has been changed to 0.

Usage Guidelines

Not available.

Example

This example shows how to redistribute connected routes configured with a specific metric.

```
DmSwitch(config-router-bgp)#redistribute connected metric 5
DmSwitch(config-router-bgp)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
network	Specify a network to announce via BGP.
show ip rip	Shows the RIP process parameters.
show running-config	Shows the current operating configuration.

timers bgp

timers bgp *keepalive-time hold-time*

no timers bgp

Description

Configures the keepalive and hold time interval BGP.

The **no** command resets these BGP timers to default values.

Syntax

Parameter	Description
<i>keepalive-time</i>	Indicates how often a router sends a keepalive message to a neighbor to inform the neighbor that the router is still alive and well (in seconds). (Range: 0-65535)
<i>hold-time</i>	This parameter is used as a deathwatch. If a keepalive message is not received within the holdtime, the neighbor is declared dead and the session is terminated (in seconds). (Range: 0 or 3-65535)

Default

Keepalive: 60 seconds.

Holdtime: 180 seconds.

Command Modes

Router BGP configuration.

Command History

Release	Modification
11.2	The configuration sequence of parameters keepalive and holdtime for timers bgp and neighbor timers commands has been changed in order to be the same in both cases.
9.4	Hold time and Keepalive arguments order has been changed and consistency check is done.
7.6	This command was introduced.

Usage Guidelines

If Hold time is set to zero it will not be used, and Keepalive value is ignored. Hold time must be greater than Keepalive (preferably, 3 times).

Example

This example shows how to change the BGP timers.

```
DmSwitch(config-router-bgp)#timers bgp 20 110
DmSwitch(config-router-bgp)#
```

You can verify this configuration by entering the **show running-config** privileged EXEC commands.

Related Commands

Command	Description
show ip ospf	Shows the BGP routing table entries.
show running-config	Shows the current operating configuration.

Chapter 51. Router ISIS Commands

authentication direction recv-only

```
authentication direction recv-only [ level-1 | level-2 ]
```

```
no authentication direction recv-only [ level-1 | level-2 ]
```

Description

Use this command to configure that authentication is performed only on IS-IS packets being received in an IS-IS instance.

Inserting **no** as a prefix for this command will disable the recv-only authentication direction for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the recv-only authentication direction for IS-IS level-1.
level-2	(Optional) Specifies the recv-only authentication direction for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the isis authentication recv-only direction for an IS-IS instance. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the configuration of recv-only authentication direction.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication direction recv-only
```

The following example shows the configuration of recv-only authentication direction for level-1.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication direction recv-only level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
authentication direction send-only	Configure the send-only authentication direction in an IS-IS instance.
authentication key-chain	Configure the authentication key-chain for an IS-IS instance.
authentication mode clear-text	Configure the clear-text authentication mode for an IS-IS instance.
authentication mode hmac-md5	Configure the hmac-md5 authentication mode for an IS-IS instance.
show isis	Shows the IS-IS routing table entries.

authentication direction send-only

```
authentication direction send-only [ level-1 | level-2 ]
```

```
no authentication direction send-only [ level-1 | level-2 ]
```

Description

Use this command to configure that authentication is performed only on IS-IS packets being sent in an IS-IS instance.

Inserting **no** as a prefix for this command will disable the send-only authentication direction for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the send-only authentication direction for IS-IS level-1.
level-2	(Optional) Specifies the send-only authentication direction for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the isis authentication send-only direction for an IS-IS instance. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the configuration of send-only authentication direction.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication direction send-only
```

The following example shows the configuration of send-only authentication direction for level-1.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication direction send-only level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
authentication direction recv-only	Configure the recv-only authentication direction in an IS-IS instance.
authentication key-chain	Configure the authentication key-chain for an IS-IS instance.
authentication mode clear-text	Configure the clear-text authentication mode for an IS-IS instance.
authentication mode hmac-md5	Configure the hmac-md5 authentication mode for an IS-IS instance.
show isis	Shows the IS-IS routing table entries.

authentication key-chain

authentication key-chain *key-chain name* [**level-1** | **level-2**]

no authentication key-chain *key-chain name* [**level-1** | **level-2**]

Description

Configures authentication for IS-IS packets and specifies the set of keys that can be used on an IS-IS instance.

Inserting **no** as a prefix for this command will disable the authentication key-chain for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
key-chain name	Specifies the key-chain name.
level-1	(Optional) Specifies the authentication key-chain for IS-IS level-1.
level-2	(Optional) Specifies the authentication key-chain for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Configures first the key-chain in the configuration mode and after enables it for the IS-IS router.

Example

The following example shows the key-chain creation in the configuration mode and its association with an IS-IS router level-2.

```
DmSwitch(config)#key chain isis_level_2
DmSwitch(config-keychain)#key 1
```

```

DmSwitch(config-keychain-key)#key-string datacom
DmSwitch(config-keychain-key)#exit
DmSwitch(config-keychain)#exit
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication key-chain isis_level_2 level-2

```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
authentication direction recv-only	Configure the recv-only authentication direction in an IS-IS instance.
authentication direction send-only	Configure the send-only authentication direction in an IS-IS instance.
authentication mode clear-text	Configure the clear-text authentication mode for an IS-IS instance.
authentication mode hmac-md5	Configure the hmac-md5 authentication mode for an IS-IS instance.
show isis	Shows the IS-IS routing table entries.

authentication mode clear-text

```
authentication mode clear-text [ level-1 | level-2 ]
```

```
no authentication mode clear-text [ level-1 | level-2 ]
```

Description

The **authentication mode** command specifies the type of authentication used for an IS-IS instance. The parameter **clear-text** enables the clear text authentication.

Inserting **no** as a prefix for this command will disable the clear-text authentication mode for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the clear-text authentication mode for IS-IS level-1.
level-2	(Optional) Specifies the clear-text authentication mode for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the clear-text authentication mode for an IS-IS instance. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the clear-text authentication mode configuration.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication mode clear-text
```

The following example shows the clear-text authentication mode configuration for level-1.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication mode clear-text level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
authentication direction recv-only	Configure the recv-only authentication direction in an IS-IS instance.
authentication direction send-only	Configure the send-only authentication direction in an IS-IS instance.
authentication key-chain	Configure the authentication key-chain for an IS-IS instance.
authentication mode hmac-md5	Configure the hmac-md5 authentication mode for an IS-IS instance.
show isis	Shows the IS-IS routing table entries.

authentication mode hmac-md5

```
authentication mode hmac-md5 [ level-1 | level-2 ]
```

```
no authentication mode hmac-md5 [ level-1 | level-2 ]
```

Description

The **authentication mode** command specifies the type of authentication used for an IS-IS router. The parameter **hmac-md5** enables the Message Digest 5 (MD5) authentication.

Inserting **no** as a prefix for this command will disable the hmac-md5 authentication mode for the given level, or for both levels if none is specified.

Syntax

Parameter	Description
level-1	(Optional) Specifies the hmac-md5 authentication mode for IS-IS level-1.
level-2	(Optional) Specifies the hmac-md5 authentication mode for IS-IS level-2.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to enable the hmac-md5 authentication mode for an IS-IS instance. If neither the level-1 nor level-2 is configured, the mode applies to both levels.

Example

The following example shows the hmac-md5 authentication mode configuration.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication mode hmac-md5
```

The following example shows the hmac-md5 authentication mode configuration for level-1.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#authentication mode hmac-md5 level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
authentication direction recv-only	Configure the recv-only authentication direction in an IS-IS instance.
authentication direction send-only	Configure the send-only authentication direction in an IS-IS instance.
authentication key-chain	Configure the authentication key-chain for an IS-IS instance.
authentication mode clear-text	Configure the clear-text authentication mode for an IS-IS instance.
show isis	Shows the IS-IS routing table entries.

distance

distance isis *external_distance internal_distance*

no distance isis

Description

Configure the administrative distance in an IS-IS instance.

Inserting **no** as a prefix for this command will disable the administrative distance.

Syntax

Parameter	Description
external_distance	Specifies the administrative distance for external routes (1-255).
internal_distance	Specifies the administrative distance for internal routes (1-255).

Default

level-1: external distance is 115 and the internal distance is 117

level-2: external distance is 116 and the internal distance is 118

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure an administrative distance.

Example

The following example shows the administrative distance configuration.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#distance isis 10 20
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
router isis	Enables and accesses the IS-IS configuration.
show ip route	Shows the IP routing table.

graceful-restart

```
graceful-restart [ { max-adj-restart-time seconds | max-db-sync-time seconds | max-restart-time seconds | helper-disable } ]
```

```
no graceful-restart [ max-adj-restart-time | max-db-sync-time | max-restart-time | helper-disable ]
```

Description

This command enable and configure IS-IS graceful restart capability.

Inserting **no** as a prefix for this command will disable the IS-IS graceful restart. If the parameters **max-adj-restart-time**, **max-db-sync-time**, **max-restart-time** or **helper-disable** are specified, inserting **no** prefix will restore the default value for the parameter.

Syntax

Parameter	Description
max-adj-restart-time <i>seconds</i>	Define the maximum time for adjacencies establishment before completing start/restart phase, with values in the range between 1 and 3600.
max-db-sync-time <i>seconds</i>	Define the maximum time for LSP database synchronization, with values in the range between 1 and 3600. This parameter is equivalent to the T2 timer.
max-restart-time <i>seconds</i>	Define the maximum restart time for the restarting router, with values in the range between 1 and 65535.
helper-disable	Disable the helper capability on the local system.

Default

By default, the helper-mode is enabled and the graceful restart is disabled. The default value for max-adj-restart-time is 10 seconds. For max-restart-time, the default value is 65535 seconds and for max-db-sync-time is 60 seconds.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The IS-IS graceful restart command enable the capability of supporting non-stop-forwarding (NSF) between routers in a network. The parameters values are optimal by default for almost networks.

When the router initiates the switchover procedures, the IS-IS router will announce a new holdtime value, based on max-restart-time in order to preserve the LSP database during restart.

Example

The following example show how to configure the graceful restart features using max-restart-time:

```
DmSwitch(config)#router isis area1
DmSwitch(config-router-isis)#graceful-restart
DmSwitch(config-router-isis)#graceful-restart max-restart-time 240
```

You can verify the configuration here by entering either **show running-config** or **show this** privileged EXEC commands.

Related Commands

Command	Description
isis hello interval	Configure the IS-IS hello interval in a VLAN
router isis	Enables and accesses the IS-IS configuration.
show isis	Shows the IS-IS routing table entries.

is-type

```
is-type { level-1 | level-1-2 | level-2 }
```

```
no is-type
```

Description

Configure the IS-IS Level for the routing process.

Inserting **no** as a prefix for this command will set the IS type for the default level (level-1-2).

Syntax

Parameter	Description
level-1	Specifies the IS-IS level for level-1. In this case the router acts as a station router only.
level-1-2	Specifies the IS-IS level for level-1-2. In this case the router acts as both station router and an area router.
level-2	Specifies the IS-IS level for level-2. In this case the router acts as an area router.

Default

The default configuration is type level-1-2.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the IS-IS level.

Example

The following example shows the configuration of level-1.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#is-type level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis circuit-type	Configure adjacency type in an interface
router isis	Enables and accesses the IS-IS configuration.
show isis	Shows the IS-IS routing table entries.

lsp-gen-interval max-lsp-int

```
lsp-gen-interval max-lsp-int max_interval_value
```

```
no lsp-gen-interval max-lsp-int
```

Description

Maximum interval, in seconds, between successive generation of LSPs with the same LSPID by an instance of the protocol. The range of valid values for this field is 1 - 65235.

Inserting **no** as a prefix for this command will set this value to the default one.

Syntax

Parameter	Description
max_interval_value	Specifies the maximum LSP generation interval value.

Default

The default value is 900 seconds.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the maximum interval of LSP generation for both level-1 and level-2. This field must be greater than min-lsp-int. Additionally, max-lsp-int must be at least 300 seconds less than the max-age.

Example

The following example shows the maximum LSP generation interval configuration in an IS-IS router.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#lsp-gen-interval max-lsp-int 90
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
lsp-gen-interval	Configure the minimum LSP generation interval for an IS-IS instance.
min-lsp-int	
max-age	Configure the LSP lifetime for an IS-IS instance.
router isis	Enables and accesses the IS-IS configuration.
show isis	Shows the IS-IS routing table entries.

lsp-gen-interval min-lsp-int

```
lsp-gen-interval min-lsp-int min_interval_value { level-1 | level-2 }
```

```
no lsp-gen-interval min-lsp-int min_interval_value { level-1 | level-2 }
```

Description

Minimum interval, in seconds, between successive generation of LSPs with the same LSPID by an instance of the protocol. The range of valid values for this field is 1 - 65535.

Inserting **no** as a prefix for this command will set this value to the default one.

Syntax

Parameter	Description
min_interval_value	Specifies the minimum LSP generation interval value.
level-1	(Optional) Specifies the minimum interval of LSP generation for IS-IS level-1.
level-2	(Optional) Specifies the minimum interval of LSP generation for IS-IS level-2.

Default

The default value is 30 seconds.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the minimum interval of LSP generation. If neither the level-1 nor level-2 is configured, the command is applied to both levels. This field must be less than max-lsp-int.

Example

The following example shows the minimum LSP generation interval configuration in an IS-IS router.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#lsp-gen-interval min-lsp-int 40
```

The following example shows the minimum lsp generation interval configuration in an IS-IS router for level-1.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#lsp-gen-interval min-lsp-int 40 level-1
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
lsp-gen-interval	Configure the maximum LSP generation interval for an IS-IS instance.
max-lsp-int	
max-age	Configure the LSP lifetime for an IS-IS instance.
router isis	Enables and accesses the IS-IS configuration.

max-age

max-age *max_age_value*

no max-age

Description

Each LSP contains a Remaining Lifetime field which is initially set to the max-age value on the generating IS-IS. The value stored in this field is decremented to mark the passage of time and the number of times it has been forwarded. So, use this field to configure the maximum remaining lifetime of a LSP. The range of valid values for this field is 350-65535.

Inserting **no** as a prefix for this command will set this value to the default one.

Syntax

Parameter	Description
max_age_value	Specifies the maximum LSP lifetime value.

Default

The default value is 1200 seconds (20 minutes).

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the maximum LSP lifetime value. This value must be at least 300 seconds greater than max-lsp-int. If you misconfigure the max-age value to be too low compared to the max-lsp-int, the software will reduce the max-lsp-int value to prevent the LSPs from timing out.

Example

The following example shows the maximum LSP generation interval configuration in an IS-IS router.

```
DmSwitch(config)#router isis router1
```

```
DmSwitch(config-router-isis)#max-lsp-int 1300
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
lsp-gen-interval max-lsp-int	Configure the maximum LSP generation interval for an IS-IS instance.
lsp-gen-interval min-lsp-int	Configure the minimum LSP generation interval for an IS-IS instance.
router isis	Enables and accesses the IS-IS configuration.
show isis	Shows the IS-IS routing table entries.

metric-style

```
metric-style { both | narrow | wide } [ level-1 | level-2 | level-1-2 ]
```

```
no metric-style { both | narrow | wide } [ level-1 | level-2 | level-1-2 ]
```

Description

This command configures the metric type used for the routing calculations. It specifies the metric style that is advertised in LSPs.

Inserting **no** as a prefix for this command will set the metric style configuration to the default one.

Syntax

Parameter	Description
both	Use both styles of TLVs.
narrow	Use the old-style of TLVs.
wide	Use the new-style of TLVs.
level-1	(Optional) Specifies the metric style for IS-IS level-1.
level-2	(Optional) Specifies the metric style for IS-IS level-2.
level-1-2	(Optional) Specifies the metric style for both IS-IS level-1 and level-2.

Default

The default configuration is metric style narrow for both level-1 and level-2.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the metric style in an IS-IS router. This command is related to the metric commands in the interfaces. The interfaces allow two types of metric to be configured: **metric** and **metric-wide**. If the *narrow* metric style is configured in the IS-IS router, the **metric** command should be used in the interface. Otherwise, if the *wide* metric style is configured, the **metric-wide** command should be used in the interface. The *both* metric style allows the transition between the two metric styles and should be used while not all the routers in the network are changed to use *wide* metric style. If neither the level-1 nor

level-2 parameter is configured, the metric style is applied to both levels.

Example

The following example shows the metric wide style configuration:

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#metric-style wide
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis metric	Configure the IS-IS metric in a VLAN
isis metric-wide	Configure the IS-IS wide metric in a VLAN
router isis	Enables and accesses the IS-IS configuration.
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

net

net *network_entity_title*

no net *network_entity_title*

Description

This command configures the NET (Network Entity Title) that specifies the area address and the system ID for a IS-IS routing process.

Inserting **no** as a prefix for this command will remove the configured NET from the IS-IS router.

Syntax

Parameter	Description
network_entity_title	NSAP (Network Service Access Point) address that defines this NET.

Default

There is no default configuration.

Command Modes

Router ISIS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The NET is a NSAP address where the last byte (NSEL) is always zero. It must contain between 8 and 20 bytes, where the 6 bytes directly in front of the NSEL byte form the system ID, which is mandatory. The system ID must be unique throughout each area (level 1) and throughout the backbone (level 2). The remaining bytes in front of the system ID form the area ID, which must have at least 1 byte. It is possible to configure up to 3 NETs per IS-IS router instance, which must have the same system ID and a different area ID each.

Example

The following example shows the NET configuration:

```
DmSwitch(config)#router isis router1
```

```
DmSwitch(config-router-isis)#net 49.0001.1001.0010.0001.0
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
router isis	Enables and accesses the IS-IS configuration.
show isis	Shows the IS-IS routing table entries.

redistribute

```
redistribute { connected | bgp | ospf | rip | static } [ level-1 | level-2 | level-1-2 ]
```

```
no redistribute { connected | bgp | ospf | rip | static } [ level-1 | level-2 | level-1-2 ]
```

Description

This command configures the router to redistribute information from another routing protocol into IS-IS routing process.

Inserting **no** as a prefix for this command will set the redistribute configuration on IS-IS.

Syntax

Parameter	Description
connected	Configures redistribution of connected routes into IS-IS routing process.
bgp	Configures redistribution of BGP routes into IS-IS routing process.
ospf	Configures redistribution of OSPF routes into IS-IS routing process.
rip	Configures redistribution of RIP routes into IS-IS routing process.
static	Configures redistribution of static routes into IS-IS routing process.
level-1	(Optional) Applies redistribution only for IS-IS level-1.
level-2	(Optional) Applies redistribution only for IS-IS level-2.
level-1-2	(Optional) Applies redistribution for both IS-IS level-1 and level-2.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Execute this command to configure the IS-IS redistribute information.

Example

The following example shows the redistribute connected configuration:

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#redistribute connected
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
isis metric	Configure the IS-IS metric in a VLAN
isis metric-wide	Configure the IS-IS wide metric in a VLAN
lsp-gen-interval max-lsp-int	Configure the maximum LSP generation interval for an IS-IS instance.
lsp-gen-interval min-lsp-int	Configure the minimum LSP generation interval for an IS-IS instance.
metric-style	Configure the IS-IS metric style
router isis	Enables and accesses the IS-IS configuration.
set-attached	Set set-attached configuration for router IS-IS
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

set-attached

```
set-attached { enable | disable | no-overlap | no-overlap-redistributing }
```

```
no set-attached
```

Description

This command configures the behavior of an IS-IS instance in regards to when the attached-bit should be set. Inserting **no** as a prefix for this command will disable the set-attached.

Syntax

Parameter	Description
enable	Always set attached-bit.
disable	Never set attached-bit.
no-overlap	Set attached-bit if at least one other area can be reached.
no-overlap-redistributing	Set attached-bit if at least one other area can be reached or when external routes are being redistributed into the IS-IS routing process.

Default

The default configuration uses the no-overlap behavior.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

In order to allow more control over the attached-bit setting for L1/L2 routers, enter the set-attached-bit command in router configuration mode. If the attached-bit is set, the advertizing router is seen by its neighbors as a default gateway.

Example

The following example shows the set-attached configuration.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)#set-attached enable
```

You can verify the fill here by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
redistribute	Configure the IS-IS redistribute operation
router isis	Enables and accesses the IS-IS configuration.
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

summary-address

summary-address *ip_address/mask* [**metric** *metric_value*]

no summary-address *ip_address/mask* [**metric** *metric_value*]

Description

This command configure IP address summarization.

Inserting **no** as a prefix for this command will disable the summarization for the given network address.

Syntax

Parameter	Description
ip_address/mask	IP address and mask combination specifying the network from which routes will be summarized.
metric_value	(Optional) Metric used for the generated summary route.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

By using this command, multiple groups of addresses in level 1 can be summarized into one summary route, which is then passed to level 2 and redistribute into other IS-IS areas, effectively reducing routing table size.

Example

The following example shows the summary-address configuration.

```
DmSwitch(config)#router isis router1
DmSwitch(config-router-isis)summary-address 172.16.95.0/24 metric 63
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
router isis	Enables and accesses the IS-IS configuration.
show ip route	Shows the IP routing table.
show isis	Shows the IS-IS routing table entries.

vrf

vrf *vrf_name*

no vrf *vrf_name*

Description

This command associates an IS-IS instance with a VRF.

Inserting **no** as a prefix for this command will disable the VRF.

Syntax

Parameter	Description
vrf_name	Specifies the VRF name.

Default

There is no default configuration.

Command Modes

Router IS-IS configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Each IS-IS instance can be associated with an existing VRF, which will result in the routing process taking place in that particular VRF.

Example

The following example shows the VRF creation in the configuration mode and its association with an IS-IS router.

```
DmSwitch(config)#ip vrf v1
DmSwitch(config-ip-vrf)#rd 1:1
DmSwitch(config-ip-vrf)#exit
DmSwitch(config)#exit
DmSwitch(config)#router isis router1
```

```
DmSwitch(config-router-isis)#vrf v1
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
ip router isis	Associate interface to an IS-IS routing process
net	Configure the IS-IS network entity title (NET)
router isis	Enables and accesses the IS-IS configuration.
show ip route vrf	Shows the RIB of the specified VRF.
show isis	Shows the IS-IS routing table entries.

Chapter 52. Router OSPF Commands

abr-type

```
abr-type { cisco | ibm | shortcut | standard }
```

```
no abr-type
```

Description

Configures OSPF ABR type.

The **no** command resets the ABR type to the default value.

Syntax

Parameter	Description
cisco	Alternative ABR, cisco implementation.
ibm	Alternative ABR, ibm implementation.
shortcut	Shortcut ABR.
standard	Standard behavior (RFC2328).

Default

Standard ABR type.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
7.6	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to change the OSPF ABR type.

```
DmSwitch(config-router-ospf) #abr-type shortcut
DmSwitch(config-router-ospf) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* authentication

```
area { id | ip-address_id } authentication [ message-digest ]
```

```
no area { id | ip-address_id } authentication
```

Description

Configures authentication for the specified OSPF area ID.

The **no** command disables authentication for the area.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
message-digest	(Optional) Uses message-digest authentication.

Default

Authentication is disabled.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The area authentication provides a global configuration for enabling or disabling authentication in all OSPF networks that belong to that specific area.

The area authentication requires the key configuration in the VLAN interface that belongs to the OSPF network domain in order to guarantee the correct authentication. In case of the option **message-digest** is added to the area authentication it will require the option **ip ospf message-digest-key** to be used in the VLAN interface for the key definition. Otherwise the option **ip ospf authentication-key** must be used in the VLAN interface for the key definition by using a simple authentication.

Do not specify the **message-digest** option to use simple authentication (plain text).

Example

This example shows how to enable simple authentication for area 0.

```
DmSwitch(config-router-ospf)#area 0 authentication
% Warning:
  This command requires the ip ospf authentication-key configuration in VLAN interface.
  Do you wish to continue? <y/N> y
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* default-cost

```
area { id | ip-address_id } default-cost default-cost-value
```

```
no area { id | ip-address_id } default-cost
```

Description

Configures the default cost of a NSSA or a stub area ID.

The **no** command resets the cost to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
default-cost <i>default-cost-value</i>	Specifies stub's advertised default summary cost. (Range: 0-16777215)

Default

Default cost: 1.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

It is not possible to configure default cost for area ID 0 (IP 0.0.0.0). To configure a default cost, it is necessary to define a NSSA or a stub configuration in the same area (except area ID 0). If a NSSA or a stub configuration is removed in an area, the default cost returns to its default value.

Example

This example shows how to change the default cost for area 1.

```
DmSwitch(config-router-ospf)#area 1 default-cost 200
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id nssa	Configures an area as NSSA.
area id stub	Configures an area as stub.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* nssa

```
area { id | ip-address_id } nssa { translate-always | translate-candidate |  
translate-never } [ no-summary ]
```

```
no area { id | ip-address_id } nssa [ no-summary ]
```

Description

Configures an area as NSSA.

The **no** command removes the NSSA configuration in the area, or removes the **no-summary** option.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
translate-always	Configures NSSA-ABR to always translate.
translate-candidate	Configures NSSA-ABR for translate election.
translate-never	Configures NSSA-ABR to never translate.
no-summary	(Optional) Configures an NSSA totally stub area.

Default

NSSA area is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Configures an OSPF not-so-stubby area (NSSA). Use the **no-summary** option to configure an NSSA totally stub area.

It is not possible to configure the area ID 0 (IP 0.0.0.0) as NSSA. It is not allowed to set an area as NSSA if it

has a virtual link configured in it.

If a NSSA configuration is removed in an area, the default cost returns to its default value.

Example

This example shows how to configure an area as NSSA.

```
DmSwitch(config-router-ospf)#area 1 nssa translate-candidate
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id default-cost	Configures the default cost of a NSSA or stub area.
area id stub	Configures an area as stub.
area id virtual-link ip-address	Configures a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* range

```
area { id | ip-address_id } range ip-address/mask [ advertise | not-advertise ]
```

```
no area { id | ip-address_id } range ip-address/mask
```

Description

Summarizes routes matching IP address/mask at an area boundary.

The **no** command removes the range configuration in the area.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address/mask</i>	Area range IP address to match.
advertise	(Optional) Advertise the range.
not-advertise	(Optional) Does not advertise the range.

Default

Area range is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
9.4	The parameter cost was changed to advertise .

Usage Guidelines

The default action is to advertise the range. Area range configuration is available for border routers only.

Example

This example shows how to summarize a route matching address/mask.

```
DmSwitch(config-router-ospf)#area 0 range 10.10.20.1/24
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* stub

```
area { id | ip-address_id } stub [ no-summary ]
```

```
no area { id | ip-address_id } stub [ no-summary ]
```

Description

Configures an area as stub.

The **no** command removes the stub configuration in the area, or removes the **no-summary** option.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
no-summary	(Optional) Prevents from sending summary LSA into the stub area.

Default

Stub area is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

To further reduce the number of link state advertisements (LSAs) sent into a stub area, you can configure **no-summary** on the DmSwitch to prevent it from sending summary LSA into the stub area.

It is not possible to configure the area ID 0 (IP 0.0.0.0) as stub. It is not allowed to set an area as stub if it has a virtual link configured in it.

If a stub configuration is removed in an area, the default cost returns to its default value.

Example

This example shows how to configure an area as stub.

```
DmSwitch(config-router-ospf)#area 1 stub
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id default-cost	Configures the default cost of a NSSA or stub area.
area id nssa	Configures an area as NSSA.
area id virtual-link ip-address	Configures a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address*

area { *id* | *ip-address_id* } **virtual-link** *ip-address*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address*

Description

Configures a virtual link.

The **no** command removes the virtual link.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

It is not possible to configure the area ID 0 (IP 0.0.0.0) on a virtual link. It is not allowed to set a virtual link in an area that is a NSSA or a stub area.

Example

This example shows how to configure a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 100.10.10.10
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id nssa	Configures an area as NSSA.
area id stub	Configures an area as stub.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* authentication

```
area { id | ip-address_id } virtual-link ip-address authentication [ message-digest | null ]
```

```
no area { id | ip-address_id } virtual-link ip-address authentication
```

Description

Configures authentication on a virtual link.

The **no** command disables authentication on the virtual link.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
message-digest	(Optional) Uses message-digest authentication.
null	(Optional) Does not use authentication.

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area { *id* | *ip-address_id* } virtual-link *ip-address*** configuration.

Example

This example shows how to configure authentication on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 authentication
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address authentication-key	Configures authentication key on a virtual link.
area id virtual-link ip-address message-digest-key	Configures message digest key on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* authentication-key

```
area { id | ip-address_id } virtual-link ip-address authentication-key { key }
```

```
no area { id | ip-address_id } virtual-link ip-address authentication-key
```

Description

Configures authentication key on a virtual link.

The **no** command removes the authentication key configured on the virtual link.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
<i>key</i>	Specifies the authentication key.

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area { *id* | *ip-address_id* } virtual-link *ip-address*** configuration.

Example

This example shows how to configure the authentication key on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 authentication-key key_test
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address authentication	Configures authentication on a virtual link.
area id virtual-link ip-address message-digest-key	Configures message digest key on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* dead-interval

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **dead-interval** *value*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **dead-interval**

Description

Configures dead router detection time on a virtual link.

The **no** command resets the dead interval to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
<i>value</i>	Specifies the dead interval (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area** { *id* | *ip-address_id* } **virtual-link** *ip-address* configuration.

Example

This example shows how to configure the dead router detection time on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 dead-interval 20
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address hello-interval	Configures the hello packet interval on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* hello-interval

```
area { id | ip-address_id } virtual-link ip-address hello-interval { value }
```

```
no area { id | ip-address_id } virtual-link ip-address hello-interval
```

Description

Configures the hello packet interval on a virtual link.

The **no** command resets the hello interval to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
<i>value</i>	Specifies the hello interval (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area { *id* | *ip-address_id* } virtual-link *ip-address*** configuration.

Example

This example shows how to configure the hello packet interval on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 hello-interval 20
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* message-digest-key

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **message-digest-key** *key-id* **md5** *key-text*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **message-digest-key** *key-id*

Description

Configures message digest key on a virtual link.

The **no** command removes the specified message digest key configured on the virtual link.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
<i>key-id</i>	Specifies the key ID. (Range: 1-255)
md5	Uses the MD5 algorithm.
<i>key-text</i>	Specifies the key string.

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area** { *id* | *ip-address_id* } **virtual-link** *ip-address* configuration.

Example

This example shows how to configure a message digest key on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 message-digest-key 1 md5 test_key
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address authentication	Configures authentication on a virtual link.
area id virtual-link ip-address authentication-key	Configures authentication key on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* retransmit-interval

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **retransmit-interval** *value*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **retransmit-interval**

Description

Configures the link state retransmit interval on a virtual link.

The **no** command resets the retransmit interval to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
<i>value</i>	Specifies the retransmit interval (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area** { *id* | *ip-address_id* } **virtual-link** *ip-address* configuration.

Example

This example shows how to configure the link state retransmit interval on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 retransmit-interval 20
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address hello-interval	Configures the hello packet interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* transmit-delay

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **transmit-delay** *value*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **transmit-delay**

Description

Configures the link state transmit delay on a virtual link.

The **no** command resets the transmit delay to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
<i>ip-address</i>	Specifies the IP address associated with virtual link neighbor.
<i>value</i>	Specifies the transmit delay (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This parameter might only be set after **area** { *id* | *ip-address_id* } **virtual-link** *ip-address* configuration.

Example

This example shows how to configure the link state transmit delay on a virtual link.

```
DmSwitch(config-router-ospf)#area 1 virtual-link 2.2.2.2 transmit-delay 20
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address hello-interval	Configures the hello packet interval on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

auto-cost reference-bandwidth

auto-cost reference-bandwidth *bandwidth*

no auto-cost reference-bandwidth

Description

Configures OSPF interface cost according to bandwidth.

The **no** command resets the reference bandwidth to the default value.

Syntax

Parameter	Description
reference-bandwidth <i>bandwidth</i>	Specifies reference bandwidth (in Mbits/second) method to assign OSPF cost. Range (1-4294967)

Default

Bandwidth: 100 Mbits/second.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the reference bandwidth.

```
DmSwitch(config-router-ospf)#auto-cost reference-bandwidth 50
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip ospf</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.

compatible rfc1583

`compatible rfc1583`

`no compatible rfc1583`

Description

Defines the RFC1583 compatibility.

The **no** command disables the RFC1583 compatibility.

Syntax

No parameter accepted.

Default

RFC1583 compatibility is disabled.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The RFC2328, the successor to RFC1583, suggests a change to the path preference algorithm that prevents possible routing loops that were possible in the old version of OSPFv2. More specifically, it demands that inter-area paths and intra-area path are now of equal preference but still both preferred to external paths.

Example

This example shows how to define the RFC1583 compatibility.

```
DmSwitch(config-router-ospf)#compatible rfc1583
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** or the **show ip ospf** privileged EXEC commands.

Related Commands

Command	Description
<code>show ip ospf</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.

default-information-originate

```
default-information-originate [ metric metric-value | metric-type metric-type-value
| tag external-tag-value ]
```

```
no default-information-originate
```

Description

Enables redistribution of a default route (with the exception of black-hole routes), if one is present in the routing table.

The **no** command disables the redistribution of a default route.

Syntax

Parameter	Description
metric <i>metric-value</i>	Specifies the metric for the redistributed default route. (Range: 0-16777214)
metric-type <i>metric-type-value</i>	Specifies the External Type metric for the redistributed default routes. (Range: 1-2)
tag <i>external-tag-value</i>	Specifies the External Tag for the redistributed default route. (Range: 1-4294967295)

Default

Distribution of default route is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
7.6	The option route-map was introduced.
8.0	This command was deprecated.
12.4.12	This command was reintroduced containing the metric, metric-type and tag optional parameters.

Usage Guidelines

Force the autonomous system boundary router to redistribute a default route into the OSPF routing domain.

Example

This example shows how to redistribute a default route.

```
DmSwitch(config-router-ospf) #default-information-originate metric-type 2
DmSwitch(config-router-ospf) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

default-metric

default-metric *metric-value*

no default-metric

Description

Defines a OSPF metric of redistribute routes.

The **no** command resets the metric to the default value.

Syntax

Parameter	Description
<i>metric-value</i>	Specifies the default metric. (Range: 0-16777214)

Default

Default metric is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to define the default metric for redistribute.

```
DmSwitch(config-router-ospf)#default-metric 100
DmSwitch(config-router-ospf)#
```

You can verify that the default metric was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip ospf</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.

distance

```
distance ospf { external external-distance | internal internal-distance }
```

```
no distance [ ospf { external | internal } ]
```

Description

Defines an administrative distance for the OSPF protocol.

The no **no** command removes the global administrative distance or only for the specified routes area type.

Syntax

Parameter	Description
ospf	Administrative distance for external and internal routes.
external	Administrative distance for external routes.
<i>external-distance</i>	Specifies the administrative distance for routes from another routing domain learned via redistribution. (Range: 1-255)
internal	Administrative distance for internal routes.
<i>internal-distance</i>	Specifies the administrative distance for internal routes. (Range: 1-255)

Default

By default, the external distance is 110 and the internal distance is 30.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
9.4	The parameters <i>inter-area</i> and <i>intra-area</i> were changed to <i>internal</i> .
14.2	The command distance administrative-distance was deprecated.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Example

This example shows how to define the global administrative distance.

```
DmSwitch(config-router-ospf)#distance ospf internal 100
DmSwitch(config-router-ospf)#
```

You can verify that the administrative distance was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

log-adjacency-changes

log-adjacency-changes

no log-adjacency-changes

Description

To configure the router to send a syslog message when an OSPF neighbor status changes, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command. Through this command you can see all neighbor status transitions.

Syntax

No parameter accepted.

Default

OSPF logging adjacency changes disabled.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
9.4.4	This command was introduced.

Usage Guidelines

This command allows you to know about OSPF neighbors status transitions (DOWN, INIT, 2WAY, EXSTART, EXCHANGE, FULL).

Example

This example shows how to enable OSPF logging adjacency changes.

```
DmSwitch(config-router-ospf) #log-adjacency-changes
DmSwitch(config-router-ospf) #
```

You can verify whether OSPF logging adjacency changes is enabled by entering the **show running-config**

Once enabled you also can see OSPF logging through command **show log ram**

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show log ram</code>	Shows log messages.

max-metric router-lsa

```
max-metric router-lsa { administrative | on-startup announce-time | on-shutdown  
announce-time }
```

```
no max-metric router-lsa
```

Description

This enables *RFC3137, OSPF Stub Router Advertisement support*, where the OSPF process describes its transit links in its router-LSA as having infinite distance so that other routers will avoid calculating transit paths through the router while still being able to reach its locally announced networks.

The **no** command disables **max-metric router-lsa**.

Syntax

Parameter	Description
administrative	Administrative enabling allows for administrative intervention for what-ever reason, for an indefinite period of time. Note that if the configuration is written to file, this administrative form of the stub-router command will also be written to file. If ospfd is restarted later, the command will then take effect until manually deconfigured.
on-startup <i>announce-time</i>	Enabling this for a period after startup allows OSPF to converge fully first without affecting any existing routes used by other routers, while still allowing any connected stub links and/or redistributed routes to be reachable (in seconds). (Range: 5-86400)
on-shutdown <i>announce-time</i>	(Deprecated) Enabling this for a period of time in advance of shutdown allows the router to gracefully excuse itself from the OSPF domain (in seconds). (Range: 5-86400)

Default

Not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
9.0	This command was introduced.
9.4	The parameter on-shutdown was deprecated.

Usage Guidelines

Not available.

Example

In this example, this support is enabled administratively (and indefinitely).

```
DmSwitch(config-router-ospf) #max-metric router-lsa administrative
DmSwitch(config-router-ospf) #
```

You can verify this configuration by entering the **show running-config**.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

mpls ldp sync ^[1] ^[3] ^[6]

mpls ldp sync

no mpls ldp sync

Description

Configures MPLS LDP Synchronization with OSPF.

Inserting **no** as a prefix for this command will disable the MPLS LDP Synchronization with OSPF.

Syntax

No parameters accepted.

Default

MPLS LDP Synchronization with OSPF is disabled.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The LDP-IGP Synchronization is supported with OSPF only. Other IGPs are not supported.

This feature provides a means to synchronize LDP and IGP to minimize MPLS packet loss.

To enable LDP-IGP Synchronization on each interface that belongs to an OSPF process, use the **mpls ldp sync** command. If you do not want some of the interfaces to have LDP-IGP Synchronization enabled, issue the **no mpls ldp igp sync** command on those interfaces.

If the LDP peer is reachable, the IGP will wait indefinitely (by default) for synchronization to be achieved. To limit the amount of time the IGP session will wait, use the **mpls ldp igp sync holddown** command. If the LDP peer is not reachable, the IGP establishes the adjacency to enable the LDP session to be established.

When an IGP adjacency is established on a link but LDP-IGP Synchronization is not yet achieved or is lost, the IGP advertises the max-metric on that link.

Example

This example shows how to enable the MPLS LDP Synchronization with OSPF.

```
DmSwitch(config-router-ospf) #mpls ldp sync
DmSwitch(config-router-ospf) #
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Shows the LDP-IGP Synchronization

mpls traffic-eng ^[1] ^[3] ^[6]

mpls traffic-eng

no mpls traffic-eng

Description

Enable support for OSPF Traffic Engineering Extension (internet-draft) this requires support for Opaque LSAs. CSPF (Constrained Shortest Path First) is also enabled.

The **no** command disables Traffic-Engineering Constraints Calculation (CSPF) for OSPF.

Syntax

No parameter accepted.

Default

MPLS Traffic Engineering disabled.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
9.0	This command was introduced.

Usage Guidelines

Traffic engineering enables ISPs to route network traffic in such a way that they can offer the best service to their users in terms of throughput and delay.

Example

This example shows how to enable MPLS Traffic Engineering.

```
DmSwitch(config-router-ospf) #mpls traffic-eng
DmSwitch(config-router-ospf) #
```

You can verify whether MPLS Traffic Engineering is enabled by entering the **show running-config**

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.

neighbor

neighbor *ip-address* [**priority** *priority-value*]

no neighbor *ip-address*

Description

Defines a static neighbor router.

Entering with **no** command, it removes a configured neighbor router.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the neighbor IP address.
priority <i>priority-value</i>	(Optional) Specifies the priority of non-broadcast neighbor. (Range: 0-255)

Default

No neighbor is configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command configures static neighbors routers attached to the network.

A neighbor with priority 0 is considered ineligible for DR (Designated Router) election.

Example

This example shows how to define a neighbor router IP address.

```
DmSwitch(config-router-ospf)#neighbor 10.11.12.1
DmSwitch(config-router-ospf)#
```

You can verify that the neighbor was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
passive-interface	Suppresses OSPF routing updates on specified VLAN interfaces.
network	Associates a network with a OSPF routing process.
show ip ospf	Shows the OSPF process parameters.

network

```
network ip-address/mask area { area-id | ip-address_id }
```

```
no network ip-address/mask area { area-id | ip-address_id }
```

Description

Enables OSPF routing on an IP network.

The **no** command disables OSPF routing on the specified network.

Syntax

Parameter	Description
<i>ip-address/mask</i>	Specifies the network.
area	OSPF area ID.
<i>area-id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.

Default

No network is configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The OSPF process will act only over associated networks.

Example

This example shows how to associate a network with the OSPF routing.

```
DmSwitch(config-router-ospf)#network 10.11.12.0/24  
DmSwitch(config-router-ospf)#
```

You can verify that the network was associated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

nsf

```
nsf { planned | unplanned | max-restart-interval interval }[5]
```

```
nsf helper { disabled | max-restart-interval interval }
```

```
no nsf { planned | unplanned | max-restart-interval interval }[5]
```

```
no nsf helper { disabled | max-restart-interval interval }
```

Description

This enables *RFC3623, OSPF Graceful Restart, a.k.a. Non-stop Forwarding (NSF) support*, where the OSPF process enhances itself so that the router can stay on the forwarding path even as the OSPF process is restarted. This accomplished by exchanging OSPF grace-LSA messages.

The **no** command disables the **nsf** options.

Syntax

Parameter	Description
helper	Configures NSF helper mode.
disabled	Disables helper mode in restart configuration.
planned ^[5]	Enables planned mode in restart configuration.
unplanned ^[5]	Enables unplanned mode in restart configuration.
max-restart-interval interval	Sets the restart interval announced in grace-LSAs (in seconds). (Range: 1-1800)

Default

NSF planned and unplanned modes are disabled. NSF helper mode is enabled. NSF maximum restart interval: 120 seconds. NSF helper maximum restart interval: 140 seconds.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
9.4	This command was introduced.

Usage Guidelines

The equipment that should support OSPF graceful restart, usually a redundant chassis, should enable this feature and, if needed, set **max-restart-interval**. Also make sure all OSPF neighbors have helper mode on.

Example

In this example, the NSF support is enabled administratively.

```
DmSwitch(config-router-ospf)#nsf planned
DmSwitch(config-router-ospf)#
```

You can verify this configuration by entering the **show running-config**.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

passive-interface

```
passive-interface { all | index | range first-index last-index }
```

```
no passive-interface { all | index | range first-index last-index }
```

Description

Disables routing updates on specified VLAN interfaces.

Entering with **no** command, it re-enable the sending of routing updates on the specified VLAN interfaces.

Syntax

Parameter	Description
all	Suppresses for all VLANs.
<i>index</i>	Suppresses for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Suppresses for a range of VLANs. (Range: 1-4094)

Default

Routing updates are sent on the VLANs.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you disable the sending of routing updates on a VLAN, the particular subnet will continue to be advertised to other VLANs (if these are created), and updates from other routers on that VLAN continue to be received and processed.

OSPF routing information is neither sent nor received through the specified VLAN. The specified VLAN address appears as a stub network in the OSPF domain.

Example

This example shows how to suppress routing updates on a specific VLAN interface.

```
DmSwitch(config-router-ospf) #passive-interface 1
DmSwitch(config-router-ospf) #
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
neighbor	Defines a neighbor router.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

redistribute

```
redistribute { ip-address/mask | bgp | connected | isis | rip | static } [ metric metric-value | metric-type metric-type-value | tag tag-value ]
```

```
no redistribute { bgp | connected | isis | rip | static }
```

Description

Redistributes bgp, connected, RIP or static routes, with a specific metric and metric type.

Entering with **no** command, it stops the redistribution of the specified routes types.

Syntax

Parameter	Description
bgp	Redistributes Border Gateway Protocol (BGP) routes.
connected	Redistributes connected routes.
isis	Redistributes IS-IS routes.
rip	Redistributes RIP routes.
static	Redistributes configured static routes.
metric <i>metric-value</i>	(Optional) Defines a metric for a specified redistribute route. (Range: 0-16777214)
metric-type <i>metric-type-value</i>	(Optional) Defines OSPF exterior metric type for a specified redistribute route. (Range: 1-2)
tag <i>tag-value</i>	(Optional) Defines the external route tag value. (Range: 1-4294967295)

Default

No redistribution routes are defined.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
7.6	The option route-map was introduced.
9.0	The option route-map was removed.
11.0.2	The parameter <i>ip-address/mask</i> was introduced.
13.0	The option tag was introduced.

Usage Guidelines

Not available.

Example

This example shows how to redistribute connected routes configured with a specific metric.

```
DmSwitch(config-router-ospf)#redistribute connected metric 5
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

refresh timer

refresh timer *refresh-value*

no refresh timer

Description

Configures OSPF refresh timer.

Entering with the **no** command, it returns to the default refresh timer value.

Syntax

Parameter	Description
<i>refresh-value</i>	Specifies the refresh timer value (in seconds). Must be multiple of 10. (Range: 10-1800)

Default

Refresh value: 10 seconds.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the refresh timer.

```
DmSwitch(config-router-ospf)#refresh timer 30
DmSwitch(config-router-ospf)#
```

You can verify this configuration by entering the **show running-config** or the **show ip ospf** privileged EXEC commands.

Related Commands

Command	Description
<code>show ip ospf</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.
<code>timers spf</code>	Configures the SPF timers.

router-id

router-id *A.B.C.D*

no router-id

Description

Defines a router ID for the OSPF process.

The **no** command removes the router ID configured.

Syntax

Parameter	Description
<i>A.B.C.D</i>	Specifies the OSPF router ID in IP address format.

Default

No router ID is configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The router ID is the highest IP address on the box, calculated at boot time or whenever the OSPF process is restarted. This command defines a static router ID.

Example

This example shows how to configure a static router ID.

```
DmSwitch(config-router-ospf)#router-id 10.10.20.30
DmSwitch(config-router-ospf)#
```

You can verify the router ID configured by entering the **show running-config** or the **show ip ospf** privileged EXEC command.

Related Commands

Command	Description
<code>show ip ospf</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.

timers spf

timers spf *delay-time hold-time*

no timers spf

Description

Configures the delay and hold down SPF timers.

The **no** command resets the SPF timers to its default values.

Syntax

Parameter	Description
<i>delay-time</i>	Specifies the amount of time to wait before running an SPF after receiving a database change (in seconds). (Range: 1-600000)
<i>hold-time</i>	Specifies the amount of time to wait between consecutive SPF runs (in seconds). (Range: 1-600000)

Default

Delay time: 1 second.

Hold time: 1 second.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
9.4	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to change the SPF timers.

```
DmSwitch(config-router-ospf)#timers spf 2 10
DmSwitch(config-router-ospf)#
```

You can verify this configuration by entering the **show running-config** or the **show ip ospf** privileged EXEC commands.

Related Commands

Command	Description
refresh timer	Configures OSPF refresh timer.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

timers throttle spf

timers throttle spf *delay-time initial-hold-time maximum-hold-time*

no timers throttle spf

Description

This command sets the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation.

The **no** command resets the Throttle SPF timers to its default values.

Syntax

Parameter	Description
<i>delay-time</i>	Specifies the minimum amount of time to delay SPF calculation (in milliseconds). (Range: 1-600000)
<i>initial-hold-time</i>	Consecutive SPF calculations will always be separated by at least <i>hold-time</i> milliseconds. The <i>hold-time</i> is adaptive and initially is set to the <i>initial-holdtime</i> configured with the above command (in milliseconds). (Range: 1-600000)
<i>maximum-hold-time</i>	Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the <i>maximum-holdtime</i> configured with this command (in milliseconds). (Range: 1-600000)

Default

Delay time: 200 milliseconds.

Initial Hold time: 1 second.

Maximum Hold time: 10 seconds.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
9.0	This command was introduced.

Usage Guidelines

Not available.

Example

In this example, the delay is set to 200ms, the initial holdtime is set to 400ms and the maximum holdtime to 10s. Hence there will always be at least 200ms between an event which requires SPF calculation and the actual SPF calculation. Further consecutive SPF calculations will always be separated by between 400ms to 10s, the hold-time increasing by 400ms each time an SPF-triggering event occurs within the hold-time of the previous SPF calculation. This command supercedes the **timers spf** command. .

```
DmSwitch(config-router-ospf)#timers throttle spf 200 400 10000
DmSwitch(config-router-ospf)#
```

You can verify this configuration by entering the **show running-config** or the **show ip ospf** privileged EXEC commands.

Related Commands

Command	Description
refresh timer	Configures OSPF refresh timer.
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

Chapter 53. Router OSPFv3 Commands

area id/ipv4-address_id default-cost

area { *id* | *ipv4-address_id* } **default-cost** *default-cost-value*

no area { *id* | *ipv4-address_id* } **default-cost**

Description

Configures the default cost of a NSSA or a stub area ID.

The **no** command resets the cost to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ipv4-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
default-cost <i>default-cost-value</i>	Specifies stub's advertised default summary cost. (Range: 0-16777215)

Default

Default cost: 1.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

It is not possible to configure default cost for area ID 0 (IPv4 0.0.0.0). To configure a default cost, it is necessary to define a NSSA or a stub configuration in the same area (except area ID 0). If a NSSA or a stub configuration is removed in an area, the default cost returns to its default value.

Example

This example shows how to change the default cost for area 1.

```
DmSwitch(config-router-ospfv3)#area 1 default-cost 200
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id nssa	Configures an area as NSSA.
area id stub	Configures an area as stub.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ipv4-address_id* nssa

```
area { id | ipv4-address_id } nssa { translate-always | translate-candidate [ no-summary ]
```

```
no area { id | ipv4-address_id } nssa [ no-summary ]
```

Description

Configures an area as NSSA.

The **no** command removes the NSSA configuration in the area, or removes the **no-summary** option.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ipv4-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
translate-always	Configures NSSA-ABR to always translate.
translate-candidate	Configures NSSA-ABR for translate election.
no-summary	(Optional) Configures an NSSA totally stub area.

Default

NSSA area is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Configures an OSPFv3 not-so-stubby area (NSSA). Use the **no-summary** option to configure an NSSA totally stub area.

It is not possible to configure the area ID 0 (IP 0.0.0.0) as NSSA. It is not allowed to set an area as NSSA if it has a virtual link configured in it.

If a NSSA configuration is removed in an area, the default cost returns to its default value.

Example

This example shows how to configure an area as NSSA.

```
DmSwitch(config-router-ospfv3)#area 1 nssa translate-candidate
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id default-cost	Configures the default cost of a NSSA or stub area.
area id stub	Configures an area as stub.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ipv4-address_id* stub

```
area { id | ipv4-address_id } stub [ no-summary ]
```

```
no area { id | ipv4-address_id } stub [ no-summary ]
```

Description

Configures an area as stub.

The **no** command removes the stub configuration in the area, or removes the **no-summary** option.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ipv4-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
no-summary	(Optional) Prevents from sending summary LSA into the stub area.

Default

Stub area is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

To further reduce the number of link state advertisements (LSAs) sent into a stub area, you can configure **no-summary** on the DmSwitch to prevent it from sending summary LSA into the stub area.

It is not possible to configure the area ID 0 (IP 0.0.0.0) as stub. It is not allowed to set an area as stub if it has a virtual link configured in it.

If a stub configuration is removed in an area, the default cost returns to its default value.

Example

This example shows how to configure an area as stub.

```
DmSwitch(config-router-ospfv3)#area 1 stub
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id default-cost	Configures the default cost of a NSSA or stub area.
area id nssa	Configures an area as NSSA.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address*

area { *id* | *ip-address_id* } **virtual-link** *ip-address*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address*

Description

Configures a virtual link.

The **no** command removes the virtual link.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
<i>ip-address</i>	Specifies the IPv4 address associated with virtual link neighbor.

Default

Virtual Link is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

It is not possible to configure the area ID 0 (IP 0.0.0.0) on a virtual link. It is not allowed to set a virtual link in an area that is a NSSA or a stub area.

Example

This example shows how to configure a virtual link.

```
DmSwitch(config-router-ospfv3)#area 1 virtual-link 100.10.10.10
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id nssa	Configures an area as NSSA.
area id stub	Configures an area as stub.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* dead-interval

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **dead-interval** *value*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **dead-interval**

Description

Configures dead router detection time on a virtual link.

The **no** command resets the dead interval to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
<i>ip-address</i>	Specifies the IPv4 address associated with virtual link neighbor.
<i>value</i>	Specifies the dead interval (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the dead router detection time on a virtual link.

```
DmSwitch(config-router-ospfv3)#area 1 virtual-link 2.2.2.2 dead-interval 20
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address hello-interval	Configures the hello packet interval on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* hello-interval

```
area { id | ip-address_id } virtual-link ip-address hello-interval { value }
```

```
no area { id | ip-address_id } virtual-link ip-address hello-interval
```

Description

Configures the hello packet interval on a virtual link.

The **no** command resets the hello interval to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
<i>ip-address</i>	Specifies the IPv4 address associated with virtual link neighbor.
<i>value</i>	Specifies the hello interval (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the hello packet interval on a virtual link.

```
DmSwitch(config-router-ospfv3)#area 1 virtual-link 2.2.2.2 hello-interval 20
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* instance-id

```
area { id | ip-address_id } virtual-link ip-address instance-id { value }
```

```
no area { id | ip-address_id } virtual-link ip-address instance-id
```

Description

Configures the instance-id on a virtual link.

The **no** command resets the instance-id to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
<i>ip-address</i>	Specifies the IPv4 address associated with virtual link neighbor.
<i>value</i>	Specifies the instance-id. (Range: 0-255)

Default

Virtual Link is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the instance-id on a virtual link.

```
DmSwitch(config-router-ospfv3)#area 1 virtual-link 2.2.2.2 instance-id 2
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* retransmit-interval

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **retransmit-interval** *value*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **retransmit-interval**

Description

Configures the link state retransmit interval on a virtual link.

The **no** command resets the retransmit interval to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPFv3 area ID in IPv6 address format.
<i>ip-address</i>	Specifies the IPv6 address associated with virtual link neighbor.
<i>value</i>	Specifies the retransmit interval (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the link state retransmit interval on a virtual link.

```
DmSwitch(config-router-ospfv3)#area 1 virtual-link 2.2.2.2 retransmit-interval 20
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address hello-interval	Configures the hello packet interval on a virtual link.
area id virtual-link ip-address transmit-delay	Configures the link state transmit delay on a virtual link.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

area *id*/*ip-address_id* virtual-link *ip-address* transmit-delay

area { *id* | *ip-address_id* } **virtual-link** *ip-address* **transmit-delay** *value*

no area { *id* | *ip-address_id* } **virtual-link** *ip-address* **transmit-delay**

Description

Configures the link state transmit delay on a virtual link.

The **no** command resets the transmit delay to its default value.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPFv3 area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPFv3 area ID in IPv4 address format.
<i>ip-address</i>	Specifies the IPv4 address associated with virtual link neighbor.
<i>value</i>	Specifies the transmit delay (in seconds). (Range: 1-65535)

Default

Virtual Link is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the link state transmit delay on a virtual link.

```
DmSwitch(config-router-ospfv3)#area 1 virtual-link 2.2.2.2 transmit-delay 20
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
area id virtual-link ip-address dead-interval	Configures dead router detection time on a virtual link.
area id virtual-link ip-address hello-interval	Configures the hello packet interval on a virtual link.
area id virtual-link ip-address retransmit-interval	Configures the link state retransmit interval on a virtual link.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

auto-cost reference-bandwidth

auto-cost reference-bandwidth *bandwidth*

no auto-cost reference-bandwidth

Description

Configures OSPFv3 interface cost according to bandwidth.

The **no** command resets the reference bandwidth to the default value.

Syntax

Parameter	Description
reference-bandwidth <i>bandwidth</i>	Specifies reference bandwidth (in Mbits/second) method to assign OSPFv3 cost. Range (1-4294967)

Default

Bandwidth: 100 Mbits/second.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to configure the reference bandwidth.

```
DmSwitch(config-router-ospfv3)#auto-cost reference-bandwidth 50
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ipv6 ospfv3</code>	Shows the OSPF process parameters.
<code>show running-config</code>	Shows the current operating configuration.

default-information-originate

default-information-originate [**metric** *metric-value* | **metric-type** *metric-type-value*]

no default-information-originate

Description

Enables redistribution of a default route (with the exception of black-hole routes), if one is present in the routing table.

The **no** command disables the redistribution of a default route.

Syntax

Parameter	Description
metric <i>metric-value</i>	Specifies the metric for the redistributed default route. (Range: 0-16777214)
metric-type <i>metric-type-value</i>	Specifies the External Type metric for the redistributed default routes. (Range: 1-2)

Default

Distribution of default route is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
14.4	This command was introduced.

Usage Guidelines

Force the autonomous system boundary router to redistribute a default route into the OSPFv3 routing domain.

Example

This example shows how to redistribute a default route.

```
DmSwitch(config-router-ospfv3)#default-information-originate metric-type 2
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

default-metric

default-metric *metric-value*

no default-metric

Description

Defines a OSPFv3 metric of redistribute routes.

The **no** command resets the metric to the default value.

Syntax

Parameter	Description
<i>metric-value</i>	Specifies the default metric. (Range: 0-16777214)

Default

Default metric is not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to define the default metric for redistribute.

```
DmSwitch(config-router-ospfv3)#default-metric 100
DmSwitch(config-router-ospfv3)#
```

You can verify that the default metric was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ipv6 ospfv3</code>	Shows the OSPFv3 process parameters.
<code>show running-config</code>	Shows the current operating configuration.

distance

```
distance ospfv3 { external external-distance | internal internal-distance }
```

```
no distance [ ospfv3 { external | internal } ]
```

Description

Defines an administrative distance for the OSPFv3 protocol.

The no **no** command removes the global administrative distance or only for the specified router area type.

Syntax

Parameter	Description
ospfv3	Administrative distance for external and internal routes.
external	Administrative distance for external routes.
<i>external-distance</i>	Specifies the administrative distance for routes from another routing domain learned via redistribution. (Range: 1-255)
internal	Administrative distance for internal routes.
<i>internal-distance</i>	Specifies the administrative distance for internal routes. (Range: 1-255)

Default

Administrative distance is 30 for internal and 110 for external by default.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.
14.2	The command distance <i>administrative-distance</i> was deprecated.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Example

This example shows how to define the global administrative distance.

```
DmSwitch(config-router-ospfv3)#distance ospfv3 internal 100
DmSwitch(config-router-ospfv3)#
```

You can verify that the administrative distance was configured by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

log-adjacency-changes

log-adjacency-changes

no log-adjacency-changes

Description

Use the **log-adjacency-changes** command in router configuration mode to log all OSPFV3 neighbor status changes. When enabled, the router will send a syslog message when an OSPFV3 neighbor status change occurs. To turn off this function, use the **no** form of this command.

Syntax

No parameter accepted.

Default

OSPFV3 logging adjacency changes disabled.

Command Modes

Router OSPFV3 configuration.

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

This command allows you to know about OSPFV3 neighbors status transitions (DOWN, INIT, 2WAY, EXSTART, EXCHANGE, FULL).

Example

This example shows how to enable OSPFV3 logging adjacency changes.

```
DmSwitch(config-router-ospfv3) #log-adjacency-changes
DmSwitch(config-router-ospfv3) #
```

You can verify whether OSPF logging adjacency changes is enabled by entering the **show running-config**

Once enabled you also can see OSPFV3 logging through command **show log ram**

Related Commands

Command	Description
<code>show running-config</code>	Shows the current operating configuration.
<code>show log ram</code>	Shows log messages.

max-metric router-lsa

```
max-metric router-lsa { administrative | on-startup announce-time }
```

```
no max-metric router-lsa { administrative | on-startup }
```

Description

This enables *RFC3137, OSPFv3 Stub Router Advertisement support*, where the OSPFv3 process describes its transit links in its router-LSA as having infinite distance so that other routers will avoid calculating transit paths through the router while still being able to reach interfaces through the router.

The **no** command disables **max-metric router-lsa**.

Syntax

Parameter	Description
administrative	Administrative enabling allows for administrative intervention for what-ever reason, for an indefinite period of time. Note that if the configuration is written to file, this administrative form of the stub-router command will also be written to file. If ospfd is restarted later, the command will then take effect until manually deconfigured.
on-startup <i>announce-time</i>	Enabling this for a period after startup allows OSPFv3 to converge fully first without affecting any existing routes used by other routers, while still allowing any connected stub links and/or redistributed routes to be reachable (in seconds). (Range: 5-86400)

Default

Not configured.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

In this example, this support is enabled administratively (and indefinitely).

```
DmSwitch(config-router-ospfv3) #max-metric router-lsa administrative
DmSwitch(config-router-ospfv3) #
```

You can verify this configuration by entering the **show running-config**.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

nsf

```
nsf { planned | unplanned | max-restart-interval interval }[5]
```

```
nsf helper { disabled | max-restart-interval interval }
```

```
no nsf { planned | unplanned | max-restart-interval interval }[5]
```

```
no nsf helper { disabled | max-restart-interval interval }
```

Description

This enables *RFC3623, OSPFv3 Graceful Restart, a.k.a. Non-stop Forwarding (NSF) support*, where the OSPFv3 process enhances itself so that the router can stay on the forwarding path even as the OSPFv3 process is restarted. This accomplished by exchanging OSPFv3 grace-LSA messages.

The **no** command disables the **nsf** options.

Syntax

Parameter	Description
helper	Configures NSF helper mode.
disabled	Disables helper mode in restart configuration.
planned ^[5]	Enables planned mode in restart configuration.
unplanned ^[5]	Enables unplanned mode in restart configuration.
max-restart-interval interval	Sets the restart interval announced in grace-LSAs (in seconds). (Range: 1-1800)

Default

NSF planned and unplanned modes are disabled. NSF helper mode is enabled. NSF maximum restart interval: 120 seconds. NSF helper maximum restart interval: 140 seconds.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The equipment that should support OSPFv3 graceful restart, usually a redundant chassis, should enable this feature and, if needed, set **max-restart-interval**. Also make sure all OSPFv3 neighbors have helper mode on.

Example

In this example, the NSF support is enabled administratively.

```
DmSwitch(config-router-ospfv3)#nsf planned
DmSwitch(config-router-ospfv3)#
```

You can verify this configuration by entering the **show running-config**.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

passive-interface

passive-interface { **all** | *index* | **range** *first-index last-index* }

no passive-interface { **all** | *index* | **range** *first-index last-index* }

Description

Disables routing updates on specified VLAN interfaces.

Entering with **no** command, it re-enable the sending of routing updates on the specified VLAN interfaces.

Syntax

Parameter	Description
all	Suppresses for all VLANs.
<i>index</i>	Suppresses for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Suppresses for a range of VLANs. (Range: 1-4094)

Default

Routing updates are sent on the VLANs.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The particular subnet will continue to be advertised to other VLANs (if these are created), and updates from other routers on that VLAN continue to be received and processed.

OSPFv3 routing information is neither sent nor received through the specified VLAN. The specified VLAN address appears as a stub network in the OSPFv3 domain.

Example

This example shows how to suppress routing updates on a specific VLAN interface.

```
DmSwitch(config-router-ospfv3) #passive-interface 1
DmSwitch(config-router-ospfv3) #
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

redistribute

```
redistribute { bgp | connected | rip | static } [ metric metric-value | metric-type  
metric-type-value ]
```

```
no redistribute { bgp | connected | rip | static }
```

Description

Redistributes bgp, connected, RIP or static routes, with a specific metric and metric type.

Entering with **no** command, it stops the redistribution of the specified routes types.

Syntax

Parameter	Description
bgp	Redistributes Border Gateway Protocol (BGP) routes.
connected	Redistributes connected routes.
rip	Redistributes RIP routes.
static	Redistributes configured static routes.
metric <i>metric-value</i>	(Optional) Defines a metric for a specified redistribute route. (Range: 0-16777214)
metric-type <i>metric-type-value</i>	(Optional) Defines OSPFv3 exterior metric type for a specified redistribute route. (Range: 1-2)

Default

No redistribution routes are defined.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to redistribute connected routes configured with a specific metric.

```
DmSwitch(config-router-ospfv3)#redistribute connected metric 5
DmSwitch(config-router-ospfv3)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

refresh timer

refresh timer *refresh-value*

no refresh timer

Description

Configures OSPFv3 refresh timer.

Entering with the **no** command, it returns to the default refresh timer value.

Syntax

Parameter	Description
<i>refresh-value</i>	Specifies the refresh timer value (in seconds). Must be multiple of 10. (Range: 10-1800)

Default

Refresh value: 10 seconds.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the refresh timer.

```
DmSwitch(config-router-ospfv3)#refresh timer 30
DmSwitch(config-router-ospfv3)#
```

You can verify this configuration by entering the **show running-config** or the **show ipv6 ospfv3** privileged EXEC commands.

Related Commands

Command	Description
<code>show ipv6 ospfv3</code>	Shows the OSPFv3 process parameters.
<code>show running-config</code>	Shows the current operating configuration.
<code>timers throttle spf</code>	Configures the Throttle SPF timers.

router-id

router-id *A.B.C.D*

no router-id

Description

Defines a router ID for the OSPFv3 process.

The **no** command removes the router ID configured.

Syntax

Parameter	Description
<i>A.B.C.D</i>	Specifies the OSPF router ID in IPv4 address format.

Default

No router ID is configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The router ID is the highest IPv4 address on the box, calculated at boot time or whenever the OSPFv3 process is restarted. This command defines a static router ID.

Example

This example shows how to configure a static router ID.

```
DmSwitch(config-router-ospfv3)#router-id 10.10.20.30
DmSwitch(config-router-ospfv3)#
```

You can verify the router ID configured by entering the **show running-config** or the **show ipv6 ospfv3** privileged EXEC command.

Related Commands

Command	Description
<code>show ipv6 ospfv3</code>	Shows the OSPFv3 process parameters.
<code>show running-config</code>	Shows the current operating configuration.

timers throttle spf

timers throttle spf *delay-time initial-hold-time maximum-hold-time*

no timers throttle spf

Description

This command sets the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation.

The **no** command resets the Throttle SPF timers to its default values.

Syntax

Parameter	Description
<i>delay-time</i>	Specifies the minimum amount of time to delay SPF calculation (in milliseconds). (Range: 1-600000)
<i>initial-hold-time</i>	Consecutive SPF calculations will always be separated by at least <i>hold-time</i> milliseconds. The <i>hold-time</i> is adaptive and initially is set to the <i>initial-holdtime</i> configured with the above command (in milliseconds). (Range: 1-600000)
<i>maximum-hold-time</i>	Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the <i>maximum-holdtime</i> configured with this command (in milliseconds). (Range: 1-600000)

Default

Delay time: 200 milliseconds.

Initial Hold time: 1 second.

Maximum Hold time: 10 seconds.

Command Modes

Router OSPFv3 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

In this example, the delay is set to 200ms, the initial holdtime is set to 400ms and the maximum holdtime to 10s. Hence there will always be at least 200ms between an event which requires SPF calculation and the actual SPF calculation. Further consecutive SPF calculations will always be separated by between 400ms to 10s, the hold-time increasing by 400ms each time an SPF-triggering event occurs within the hold-time of the previous SPF calculation. This command supercedes the **timers spf** command. .

```
DmSwitch(config-router-ospfv3)#timers throttle spf 200 400 10000
DmSwitch(config-router-ospfv3)#
```

You can verify this configuration by entering the **show running-config** or the **show ipv6 ospfv3** privileged EXEC commands.

Related Commands

Command	Description
refresh timer	Configures OSPFv3 refresh timer.
show ipv6 ospfv3	Shows the OSPFv3 process parameters.
show running-config	Shows the current operating configuration.

Chapter 54. Router RIP Commands

default-metric

default-metric *metric-value*

no default-metric

Description

Defines the default metric of RIP protocol.

Entering with **no** command, it resets the default metric to default value.

Syntax

Parameter	Description
<i>metric-value</i>	Specifies the default metric. (Range: 1-16)

Default

Default metric: 1.

Command Modes

Router RIP configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The default-metric command is used to modify the metric of redistributing routes of RIP. Notice that it will only affect the outgoing routes. The RIP router will always add 1 to metric values of incoming routes.

Example

This example shows how to define the default metric.

```
DmSwitch(config-router-rip)#default-metric 10
DmSwitch(config-router-rip)#
```

You can verify that the default metric was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ip rip process	Clear RIP routing data.
distance	Defines the administrative distance of RIP protocol.
network	Associates a network with a RIP routing process.
passive-interface	Suppresses RIP routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIP protocol.
router rip	Enables and accesses the RIP configuration.
show ip rip	Shows the RIP process parameters.
show ip rip neighbor	Shows RIP neighbors
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIP protocol.

distance

distance *administrative-distance*

no distance

Description

Defines the administrative distance to reach a network whose route was discovered by RIP protocol.

Entering with **no** command, it resets the administrative distance to default value.

Syntax

Parameter	Description
<i>administrative-distance</i>	Specifies the administrative distance. (Range: 1-255)

Default

Administrative distance: 120.

Command Modes

Router RIP configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

If the router have two routes to reach the same network, given by two different routing protocols, the packets to this network will be sent by the lowest administrative distance route. Administrative distance is necessary because there aren't how to compare different metrics of two routing protocols to define the best route.

Example

This example shows how to define the administrative distance to all networks whose route was discovered by RIP protocol.

```
DmSwitch(config-router-rip)#distance 100
DmSwitch(config-router-rip)#
```

You can verify that the administrative distance was defined by entering the **show running-config** or the **show ip rip** privileged EXEC commands.

Related Commands

Command	Description
clear ip rip process	Clear RIP routing data.
default-metric	Defines the default metric of RIP protocol.
network	Associates a network with a RIP routing process.
passive-interface	Suppresses RIP routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIP protocol.
router rip	Enables and accesses the RIP configuration.
show ip rip	Shows the RIP process parameters.
show ip rip neighbor	Shows RIP neighbors
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIP protocol.

network

network *ip-address/mask*

no network *ip-address/mask*

Description

Associates a network with a RIP routing process.

Entering with **no** command, it dissociates a network of a RIP routing process.

Syntax

Parameter	Description
<i>ip-address/mask</i>	Specifies the network.

Default

No default is defined.

Command Modes

Router RIP configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The RIP process will act only over associated networks, where they will advertise and listen for RIP updates.

Example

This example shows how to associate a network with the RIP protocol.

```
DmSwitch(config-router-rip)#network 10.11.12.0/24
DmSwitch(config-router-rip)#
```

You can verify that the network was associated by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>clear ip rip process</code>	Clear RIP routing data.
<code>default-metric</code>	Defines the default metric of RIP protocol.
<code>distance</code>	Defines the administrative distance of RIP protocol.
<code>passive-interface</code>	Suppresses RIP routing updates on specified VLAN interfaces.
<code>redistribute</code>	Redistributes routes with a metric of RIP protocol.
<code>router rip</code>	Enables and accesses the RIP configuration.
<code>show ip rip</code>	Shows the RIP process parameters.
<code>show ip rip neighbor</code>	Shows RIP neighbors
<code>show running-config</code>	Shows the current operating configuration.
<code>timers basic</code>	Defines the basic timers of RIP protocol.

passive-interface

passive-interface { **all** | *index* | **range** *first-index last-index* }

no passive-interface { **all** | *index* | **range** *first-index last-index* }

Description

Suppresses routing updates on specified VLAN interfaces.

Entering with **no** command, it enables routing updates on the specified VLAN interfaces.

Syntax

Parameter	Description
all	Suppresses for all VLANs.
<i>index</i>	Suppresses for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Suppresses for a range of specific VLANs index. (Range: 1-4094)

Default

Routing updates are sent on the VLANs.

Command Modes

Router RIP configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

This command suppresses the sending of RIP messages by broadcast (RIP version 1) and multicast (RIP version 2) packets. However, it is possible to exchange RIP messages by unicast packets with the neighbor routes, specified by the **neighbor** router RIP command.

Example

This example shows how to suppress routing updates on a specific VLAN interface.

```
DmSwitch(config-router-rip)#passive-interface 1
DmSwitch(config-router-rip)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ip rip process	Clear RIP routing data.
default-metric	Defines the default metric of RIP protocol.
distance	Defines the administrative distance of RIP protocol.
network	Associates a network with a RIP routing process.
redistribute	Redistributes routes with a metric of RIP protocol.
router rip	Enables and accesses the RIP configuration.
show ip rip	Shows the RIP process parameters.
show ip rip neighbor	Shows RIP neighbors
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIP protocol.

redistribute

```
redistribute { bgp | connected | ospf [ area-id ] | static } [ metric metric-value ]
```

```
no redistribute { bgp | connected | ospf | static }
```

Description

Redistributes connected, OSPF or static routes, with a specific or default metric into RIP protocol.

Entering with **no** command, it stops the redistribution of the specified routes types.

Syntax

Parameter	Description
bgp	Redistributes Border Gateway Protocol (BGP) routes.
connected	Redistributes connected routes.
ospf [<i>area-id</i>]	Redistributes OSPF routes. <i>area-id</i> is an optional parameter that accepts decimal or IP address format.
static	Redistributes configured static routes.
metric <i>metric-value</i>	(Optional) Specifies a metric. (Range: 1-16)

Default

No redistribution routes are defined.

Command Modes

Router RIP configuration.

Command History

Release	Modification
9.4.2	This command was introduced.

Usage Guidelines

This command allows the RIP protocol to advertise routes that are learned by some other means, such as by another routing protocol, static routes, or directly connected routes.

The redistribution of an specific OSPF area will advertise only internal routes, that means LSA type 1 and 2.

Example

This example shows how to redistribute connected routes configured with a specific metric.

```
DmSwitch(config-router-rip)#redistribute connected metric 5
DmSwitch(config-router-rip)#
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ip rip process	Clear RIP routing data.
default-metric	Defines the default metric of RIP protocol.
distance	Defines the administrative distance of RIP protocol.
network	Associates a network with a RIP routing process.
passive-interface	Suppresses RIP routing updates on specified VLAN interfaces.
router rip	Enables and accesses the RIP configuration.
show ip rip	Shows the RIP process parameters.
show ip rip neighbor	Shows RIP neighbors
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIP protocol.

timers basic

timers basic *update-time timeout-time garbage-time*

no timers basic

Description

Defines the basic timers of RIP protocol.

Entering with **no** command, it resets the basic timers to default value.

Syntax

Parameter	Description
<i>update-time</i>	Specifies the time that de RIP router send your complete routing table to all neighbor RIP router. (Range: 5-2000000000)
<i>timeout-time</i>	Specifies the timeout of entries in the routing table. After this time, the entries without a update are marked as invalid. (Range: 5-2000000000)
<i>garbage-time</i>	Specifies the time where the entries are removed from the routing table after its timeout. (Range: 5-2000000000)

Default

Update time: 30.

Timeout time: 180.

Garbage time: 120.

Command Modes

Router RIP configuration.

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

If the basic timers are configured as default value, they are not shown with the **show running-config** privileged EXEC command.

Example

This example shows how to define the basic timers.

```
DmSwitch(config-router-rip)#timers basic 40 190 130
DmSwitch(config-router-rip)#
```

You can verify that the basic timers was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ip rip process	Clear RIP routing data.
default-metric	Defines the default metric of RIP protocol.
distance	Defines the administrative distance of RIP protocol.
network	Associates a network with a RIP routing process.
passive-interface	Suppresses RIP routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIP protocol.
router rip	Enables and accesses the RIP configuration.
show ip rip	Shows the RIP process parameters.
show ip rip neighbor	Shows RIP neighbors
show running-config	Shows the current operating configuration.

Chapter 55. Router RIPng Commands

default-metric

default-metric *metric-value*

no default-metric

Description

Defines the default metric of RIPng protocol.

Entering with **no** command, it resets the default metric to default value.

Syntax

Parameter	Description
<i>metric-value</i>	Specifies the default metric. (Range: 1-16)

Default

Default metric: 1.

Command Modes

Router RIPng configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The default-metric command is used to modify the metric of redistributing routes of RIPng. Notice that it will only affect the outgoing routes. The RIPng router will always add 1 to metric values of incoming routes.

Example

This example shows how to define the default metric.

```
DmSwitch(config-router-ripng)#default-metric 10
DmSwitch(config-router-ripng)#
```

You can verify that the default metric was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

distance

distance *administrative-distance*

no distance

Description

Defines the administrative distance to reach a network whose route was discovered by RIPv2 protocol.

Entering with **no** command, it resets the administrative distance to default value.

Syntax

Parameter	Description
<i>administrative-distance</i>	Specifies the administrative distance. (Range: 1-255)

Default

Administrative distance: 120.

Command Modes

Router RIPv2 configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

If the router have two routes to reach the same network, given by two different routing protocols, the packets to this network will be sent by the lowest administrative distance route. Administrative distance is necessary because metrics used by different routing protocols cannot be compared when choosing the best route.

Example

This example shows how to define the administrative distance to all interfaces route was discovered by RIPv2 protocol.

```
DmSwitch(config-router-rp2) #distance 100
DmSwitch(config-router-rp2) #
```

You can verify that the administrative distance was defined by entering the **show running-config** or the **show ipv6 ripng** privileged EXEC commands.

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
default-metric	Defines the default metric of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

passive-interface

passive-interface { **all** | *index* | **range** *first-index last-index* }

no passive-interface { **all** | *index* | **range** *first-index last-index* }

Description

Suppresses routing updates on specified VLAN interfaces.

Entering with **no** command, it enables routing updates on the specified VLAN interfaces.

Syntax

Parameter	Description
all	Suppresses for all VLANs.
<i>index</i>	Suppresses for a specific VLAN index. (Range: 1-4094)
range <i>first-index last-index</i>	Suppresses for a range of specific VLANs index. (Range: 1-4094)

Default

Routing updates are sent on the VLANs.

Command Modes

Router RIPng configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command suppresses the sending of RIPng messages by multicast packets on the specified interface.

Example

This example shows how to suppress routing updates on a specific VLAN interface.

```
DmSwitch(config-router-ripng) #passive-interface 1
DmSwitch(config-router-ripng) #
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

redistribute

```
redistribute { bgp | connected | ospfv3 | static } [ metric metric-value ]
```

```
no redistribute { bgp | connected | ospfv3 | static }
```

Description

Redistributes connected, OSPv3 or static routes, with a specific or default metric of RIPng protocol.

Entering with **no** command, it stops the redistribution of the specified routes types.

Syntax

Parameter	Description
bgp	Redistributes Border Gateway Protocol (BGP) routes.
connected	Redistributes connected routes.
ospfv3	Redistributes OSPFv3 routes.
static	Redistributes configured static routes.
metric <i>metric-value</i>	(Optional) Specifies a metric. (Range: 1-16)

Default

No redistribution routes are defined.

Command Modes

Router RIPng configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to redistribute connected routes configured with a specific metric.

```
DmSwitch(config-router-ripng)#redistribute connected metric 5
```

```
DmSwitch(config-router-ripng) #
```

You can verify that the configuration was made by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.
timers basic	Defines the basic timers of RIPng protocol.

timers basic

timers basic *update-time timeout-time garbage-time*

no timers basic

Description

Defines the basic timers of RIPng protocol.

Entering with **no** command, it resets the basic timers to default value.

Syntax

Parameter	Description
<i>update-time</i>	Specifies the time that de RIPng router send your complete routing table to all neighbor RIPng router. (Range: 5-2000000000)
<i>timeout-time</i>	Specifies the timeout of entries in the routing table. After this time, the entries without a update are marked as invalid. (Range: 5-2000000000)
<i>garbage-time</i>	Specifies the time where the entries are removed from the routing table after its timeout. (Range: 5-2000000000)

Default

Update time: 30.

Timeout time: 180.

Garbage time: 120.

Command Modes

Router RIPng configuration.

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

If the basic timers are configured as default value, they are not shown with the **show running-config** privileged EXEC command.

Example

This example shows how to define the basic timers.

```
DmSwitch(config-router-ripng)#timers basic 40 190 130
DmSwitch(config-router-ripng)#
```

You can verify that the basic timers was defined by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
clear ipv6 ripng process	Clear RIPng routing data.
default-metric	Defines the default metric of RIPng protocol.
distance	Defines the administrative distance of RIPng protocol.
ipv6 ripng	Enable the RIPng routing process on the specified interface.
passive-interface	Suppresses RIPng routing updates on specified VLAN interfaces.
redistribute	Redistributes routes with a metric of RIPng protocol.
router ripng	Enables and accesses the RIPng configuration.
show ipv6 ripng	Shows the RIPng process parameters.
show ipv6 ripng database	Shows the RIPng database parameters.
show ipv6 ripng neighbors	Shows the RIPng neighbors parameters.
show running-config	Shows the current operating configuration.

Chapter 56. SFLOW Commands

sflow agent-ip

```
sflow agent-ip {ipaddress | ipv6address}
```

Description

The IP address associated with this agent.

Inserting **no** as a prefix for this command will sets the agent address to default value.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies an IPv4 or IPv6 address to the SFLOW agent.

Default

0.0.0.0

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

A manager should be able to use the SFLOW agent address as a unique key that will identify this agent over extended periods of time so that a history can be maintained.

Example

These examples shows how to configure an IPv4/IPv6 address on SFLOW agent.

```
DmSwitch(config)#sflow ip-address 192.168.1.2
```

```
DmSwitch(config)#sflow ip-address 200A::9C
```

To verify the SFLOW configuration enter the **show sflow config** command.

Related Commands

Command	Description
sflow enable	Enables SFLOW agent.
sflow receiver	Configurations for a SFLOW receiver.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

sflow enable

sflow enable

Description

Enables SFLOW agent.

Inserting **no** as a prefix for this command will disable SFLOW agent.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

If not enabled none SFLOW packet will be sent to receiver.

Example

This example shows how to enable SFLOW agent.

```
DmSwitch(config)#sflow enable
```

To verify the SFLOW configuration enter the **show sflow config** command.

Related Commands

Command	Description
sflow agent-ip	Configures an IP address for SFLOW agent.
sflow receiver	Configurations for a SFLOW receiver.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.

Command	Description
<code>show sflow interfaces</code>	Shows sFlow interfaces configuration.

receiver enable

enable

Description

Enables the SFLOW receiver.

Inserting **no** as a prefix for this command will disable the SFLOW receiver.

Syntax

No parameter accepted.

Default

Disabled.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

If the receiver is not enabled none SFLOW packet will be sent to it.

Example

This example shows how to enable the SFLOW receiver.

```
DmSwitch(config-sflow-recv-1)#enable
```

To verify the SFLOW configuration enter the **show sflow config** command.

Related Commands

Command	Description
sflow receiver	Configurations for a SFLOW receiver.
receiver ip-address	Receiver IP address.
receiver max-datagram-size	Maximum datagram size sent to receiver.
receiver port	Configures the receiver UDP port.

Command	Description
<code>show sflow config</code>	Shows sFlow global configuration.
<code>show sflow counters</code>	Shows sFlow global counters.
<code>show sflow interfaces</code>	Shows sFlow interfaces configuration.

sflow receiver

sflow receiver {1-3}

Description

Accesses the SFLOW receiver configuration menu.

Inserting **no** as a prefix for this command will sets all receiver configuratons for its default values.

Syntax

Parameter	Description
<i>value</i>	Receiver index. (Range: 1-3)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

It is possible to configure up to three receivers, they will be associated to one or more interfaces, and the agent will send SFLOW samples from these interfaces to them.

Example

This example shows how to go to the SFLOW receiver configure menu.

```
DmSwitch(config)#sflow receiver 2
DmSwitch(config-sflow-recv-2)#
```

Related Commands

Command	Description
<code>receiver enable</code>	Enables the SFLOW receiver.
<code>receiver ip-address</code>	Receiver IP address.
<code>receiver max-datagram-size</code>	Maximum datagram size sent to receiver.
<code>receiver port</code>	Configures the receiver UDP port.
<code>show sflow config</code>	Shows sFlow global configuration.
<code>show sflow counters</code>	Shows sFlow global counters.
<code>show sflow interfaces</code>	Shows sFlow interfaces configuration.

receiver ip-address

ip-address {ipaddress | ipv6address}

Description

Configures an IPv4 or IPv6 address on a receiver.

Inserting **no** as a prefix for this command will set to the default value.

Syntax

Parameter	Description
<i>ip-address</i>	Specifies the IPv4 or IPv6 address to the SFLOW receiver.

Default

0.0.0.0

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

The IP address of the sFlow collector, if set to 0.0.0.0 none sFlow datagrams will be sent.

Example

These examples shows how to configure an IPv4/IPv6 address for a SFLOW receiver.

```
DmSwitch(config-sflow-recv-1)#ip-address 192.168.55.44
```

```
DmSwitch(config-sflow-recv-3)#ip-address 2000::5
```

To verify the SFLOW configuration enter the **show sflow config** command.

Related Commands

Command	Description
<code>sflow receiver</code>	Configurations for a SFLOW receiver.
<code>receiver enable</code>	Enables the SFLOW receiver.
<code>receiver max-datagram-size</code>	Maximum datagram size sent to receiver.
<code>receiver port</code>	Configures the receiver UDP port.
<code>show sflow config</code>	Shows sFlow global configuration.
<code>show sflow counters</code>	Shows sFlow global counters.
<code>show sflow interfaces</code>	Shows sFlow interfaces configuration.

receiver max-datagram-size

max-datagram-size {200-9116}

Description

Maximum datagram size that will be sent to receiver.

Inserting **no** as a prefix for this command will set to default value.

Syntax

Parameter	Description
<i>value</i>	Max datagram size. (Range: 200-9116)

Default

1400.

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

The maximum number of data bytes that can be sent in a single sample datagram. The manager should set this value to avoid fragmentation of the sFlow datagrams.

Example

This example shows how configure the receiver max datagram size.

```
DmSwitch(config-sflow-recv-3) #max-datagram-size 512
```

To verify the SFLOW configuration enter the **show sflow config** command.

Related Commands

Command	Description
sflow receiver	Configurations for a SFLOW receiver.
receiver enable	Enables the SFLOW receiver.
receiver ip-address	Receiver IP address.
receiver port	Configures the receiver UDP port.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

receiver port

`port {1-65535}`

Description

Configures the receiver UDP port.

Inserting **no** as a prefix for this command will set the default value.

Syntax

Parameter	Description
<i>value</i>	Port. (Range: 1-65535)

Default

6343

Command Modes

Privileged EXEC.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

The destination port for sFlow datagrams.

Example

This example shows how to configure a receiver port.

```
DmSwitch(config-sflow-recv-1)#port 12356
```

To verify the SFLOW configuration enter the **show sflow config** command.

Related Commands

Command	Description
---------	-------------

Command	Description
sflow receiver	Configurations for a SFLOW receiver.
receiver enable	Enables the SFLOW receiver.
receiver ip-address	Receiver IP address.
receiver max-datagram-size	Maximum datagram size sent to receiver.
show sflow config	Shows sFlow global configuration.
show sflow counters	Shows sFlow global counters.
show sflow interfaces	Shows sFlow interfaces configuration.

Chapter 57. Sniffer Commands

accepted

accepted {ACCEPTED | BOTH | DISCARDED}

no accepted

Description

Sets the type of packet (accepted/discarded) being filtered by sniffer.

Inserting **no** as a prefix for this command will reset the filter packet type.

Syntax

Parameter	Description
ACCEPTED	Filter only packets accepted.
BOTH	Filter packets accepted and discarded.
DISCARDED	Filter only packets discarded.

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the filter packet type.

```
DmSwitch(config-sniffer-1)#accepted DISCARDED
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture files	Shows a list of files containing packet captures.
show capture realtime	Show packets captured in realtime.
sniffer	Accesses the sniffer instance.
direction	Sets the direction of the packet to be filtered by sniffer.
enable	Enables the sniffer.
interface-ethernet	Setse an ethernet interface over which packets are filtered by sniffer.
max-packets	Sets the limit of packets to be captured by the sniffer.
protocol	Sets the protocol of the packets to be filtered by sniffer.
show-config	Shows the settings of sniffer.
vlan	Sets a vlan for the sniffer filter.

direction

```
direction {BOTH | RX | TX}
```

```
no direction
```

Description

Sets the direction of the packet to be filtered by sniffer.

Inserting **no** as a prefix for this command will reset the packet direction filter.

Syntax

Parameter	Description
BOTH	Filter Tx and Rx packets.
RX	Filter only Rx packets.
TX	Filter only Tx packets.

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the packet direction filter.

```
DmSwitch(config-sniffer-1)#direction RX
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
<code>clear capture</code>	Clear packet capture files.
<code>show capture file</code>	Show packets captured contained in a file.
<code>show capture files</code>	Shows a list of files containing packet captures.
<code>show capture realtime</code>	Show packets captured in realtime.
<code>sniffer</code>	Accesses the sniffer instance.
<code>accepted</code>	Sets the type of packet (accepted/discarded) being filtered by sniffer.
<code>enable</code>	Enables the sniffer.
<code>interface-ethernet</code>	Setse an ethernet interface over which packets are filtered by sniffer.
<code>max-packets</code>	Sets the limit of packets to be captured by the sniffer.
<code>protocol</code>	Sets the protocol of the packets to be filtered by sniffer.
<code>show-config</code>	Shows the settings of sniffer.
<code>vlan</code>	Sets a vlan for the sniffer filter.

enable

enable

no enable

Description

Enables the sniffer.

Inserting **no** as a prefix for this command will deactivate the sniffer.

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to activate the sniffer.

```
DmSwitch(config-sniffer-1)#enable
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture files	Shows a list of files containing packet captures.
show capture realtime	Show packets captured in realtime.

Command	Description
sniffer	Accesses the sniffer instance.
accepted	Sets the type of packet (accepted/discarded) being filtered by sniffer.
direction	Sets the direction of the packet to be filtered by sniffer.
interface-ethernet	Setse an ethernet interface over which packets are filtered by sniffer.
max-packets	Sets the limit of packets to be captured by the sniffer.
protocol	Sets the protocol of the packets to be filtered by sniffer.
show-config	Shows the settings of sniffer.
vlan	Sets a vlan for the sniffer filter.

interface-ethernet

interface-ethernet *number*

no interface-ethernet

Description

Setse an ethernet interface over which packets are filtered by sniffer.

Inserting **no** as a prefix for this command will reset the interface-ethernet filter.

Syntax

Parameter	Description
<i>number</i>	Interface Ethernet for capture. (Range: 1-52)

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the filter for ethernet interface.

```
DmSwitch(config-sniffer-1)#interface-ethernet 1
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
<code>clear capture</code>	Clear packet capture files.
<code>show capture file</code>	Show packets captured contained in a file.
<code>show capture files</code>	Shows a list of files containing packet captures.
<code>show capture realtime</code>	Show packets captured in realtime.
<code>sniffer</code>	Accesses the sniffer instance.
<code>accepted</code>	Sets the type of packet (accepted/discarded) being filtered by sniffer.
<code>direction</code>	Sets the direction of the packet to be filtered by sniffer.
<code>enable</code>	Enables the sniffer.
<code>max-packets</code>	Sets the limit of packets to be captured by the sniffer.
<code>protocol</code>	Sets the protocol of the packets to be filtered by sniffer.
<code>show-config</code>	Shows the settings of sniffer.
<code>vlan</code>	Sets a vlan for the sniffer filter.

max-packets

max-packets *number*

no max-packets

Description

Sets the limit of packets to be captured by the sniffer.

Inserting **no** as a prefix for this command will reset the limit of packets to be captured.

Syntax

Parameter	Description
<i>number</i>	Max packets in capture. (Range: 1-1500000)

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the limit of packets to be captured.

```
DmSwitch(config-sniffer-1)#max-packets 500
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
<code>clear capture</code>	Clear packet capture files.
<code>show capture file</code>	Show packets captured contained in a file.
<code>show capture files</code>	Shows a list of files containing packet captures.
<code>show capture realtime</code>	Show packets captured in realtime.
<code>sniffer</code>	Accesses the sniffer instance.
<code>accepted</code>	Sets the type of packet (accepted/discarded) being filtered by sniffer.
<code>direction</code>	Sets the direction of the packet to be filtered by sniffer.
<code>enable</code>	Enables the sniffer.
<code>interface-ethernet</code>	Setse an ethernet interface over which packets are filtered by sniffer.
<code>protocol</code>	Sets the protocol of the packets to be filtered by sniffer.
<code>show-config</code>	Shows the settings of sniffer.
<code>vlan</code>	Sets a vlan for the sniffer filter.

protocol

```
protocol {6OVER4 | 802.1x | ARP | ARP-Reply | ARP-Request | BGP | CDP  
| CFM | DHCP | DNS | Dst-Unreach | EAPS | Echo-request | Echo-reply  
| ELMI | ERPS | GVRP | HTTP | HTTP-STD | HTTPS | HTTPS-STD | ICMP |  
IGMP | IP | IPv6 | IPv6-PIM | IPv6-TCP | IPv6-UDP | IS-IS | L2TP |  
L2_SRCMISS | L2_MOVE | L3-Protocol | LACP | LLDP | LDP-UDP | LDP-TCP  
| Loopback-Detection | Marker | MLD | MPLS | MPLS-OAM | MPLS-UC |  
Neigh-Adv | Neigh-Solic | OAM | OSPF | PIM | PVST | QinQ | RIP | RSVP  
| Slow | SNMP | SNTP | SSH | STP | Telnet | VRRP | Whois}
```

```
no protocol {6OVER4 | 802.1x | ARP | ARP-Reply | ARP-Request | BGP  
| CDP | CFM | DHCP | DNS | Dst-Unreach | EAPS | Echo-request |  
Echo-reply | ELMI | ERPS | GVRP | HTTP | HTTP-STD | HTTPS | HTTPS-STD  
| ICMP | IGMP | IP | IPv6 | IPv6-PIM | IPv6-TCP | IPv6-UDP | IS-IS  
| L2TP | L2_SRCMISS | L2_MOVE | L3-Protocol | LACP | LLDP | LDP-UDP  
| LDP-TCP | Loopback-Detection | Marker | MLD | MPLS | MPLS-OAM |  
MPLS-UC | Neigh-Adv | Neigh-Solic | OAM | OSPF | PIM | PVST | QinQ |  
RIP | RSVP | Slow | SNMP | SNTP | SSH | STP | Telnet | VRRP | Whois}
```

Description

Sets the protocol of the packets to be filtered by sniffer.

Inserting **no** as a prefix for this command will delete delete the protocol to be filtered.

Syntax

Parameter	Description
6OVER4	IP Tunnel 6OVER4.
802.1x	802.1x.
ARP	ARP Protocol.
ARP-Reply	ARP Protocol.
ARP-Request	ARP Protocol.
BGP	BGP Protocol.
CDP	CDP.
CFM	CFM.
DHCP	DHCP Protocol.
DNS	DNS Protocol.
Dst-Unreach	Dst-Unreach.
EAPS	EAPS Protocol.
Echo-request	Echo-request.
Echo-reply	Echo-reply.
ELMI	ELMI Protocol.
ERPS	ERPS.

Parameter	Description
GVRP	GVRP.
HTTP	HTTP Protocol.
HTTP-STD	HTTP STD Protocol.
HTTPS	HTTPS Protocol.
HTTPS-STD	HTTPS STD Protocol.
ICMP	ICMP Protocol.
IGMP	IGMP Protocol.
IP	IP Protocol.
IPv6	IPv6 Protocol.
IPv6-PIM	PIM Protocol.
IPv6-TCP	TCP Protocol.
IPv6-UDP	UDP Protocol.
IS-IS	IS-IS Protocol.
L2TP	L2TP.
L2_SRCMISS	L2 SRC MISS Event.
L2_MOVE	L2 MOVE Event.
L3-Protocol	L3 Protocol.
LACP	Link Aggregation Control Protocol.
LLDP	LLDP.
LDP-UDP	LDP UDP Protocol.
LDP-TCP	LDP TCP Protocol.
Loopback-Detection	Loopback Detection.
Marker	Marker Protocol.
MLD	MLD Protocol.
MPLS	MPLS.
MPLS-OAM	MPLS OAM.
MPLS-UC	MPLS UC.
Neigh-Adv	ICMP6.
Neigh-Solic	ICMP6.
OAM	OAM.
OSPF	OSPF Protocol.
PIM	PIM Protocol.
PVST	PVST.
QinQ	QinQ.
RIP	RIP Protocol.
RSVP	RSVP Protocol.
Slow	Slow Protocol.
SNMP	SNMP Protocol.
SNTP	SNTP Protocol.
SSH	SSH Protocol.
STP	STP.
Telnet	Telnet Protocol.
VRRP	VRRP Protocol.

Parameter	Description
Whois	Whois Protocol.

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the protocol of the packets to be filtered.

```
DmSwitch(config-sniffer-1)#protocol HTTP
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture files	Shows a list of files containing packet captures.
show capture realtime	Show packets captured in realtime.
sniffer	Accesses the sniffer instance.
accepted	Sets the type of packet (accepted/discarded) being filtered by sniffer.
direction	Sets the direction of the packet to be filtered by sniffer.
enable	Enables the sniffer.
interface-ethernet	Setse an ethernet interface over which packets are filtered by sniffer.
max-packets	Sets the limit of packets to be captured by the sniffer.
show-config	Shows the settings of sniffer.
vlan	Sets a vlan for the sniffer filter.

show-config

show-config

Description

Shows the settings of sniffer.

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to display the settings of sniffer.

```
DmSwitch(config-sniffer-1)#show-config
Sniffer 1 Configurations:
  status      : Disabled
  accepted    : ACCEPTED_DISCARDED
  direction   : TX_RX
  interface-ethernet: Not Configured.
  max-packets: 1500000
  vlan        : Not Configured.
  protocols   : all
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
clear capture	Clear packet capture files.
show capture file	Show packets captured contained in a file.
show capture files	Shows a list of files containing packet captures.
show capture realtime	Show packets captured in realtime.

Command	Description
sniffer	Accesses the sniffer instance.
accepted	Sets the type of packet (accepted/discarded) being filtered by sniffer.
direction	Sets the direction of the packet to be filtered by sniffer.
enable	Enables the sniffer.
interface-ethernet	Setse an ethernet interface over which packets are filtered by sniffer.
max-packets	Sets the limit of packets to be captured by the sniffer.
protocol	Sets the protocol of the packets to be filtered by sniffer.
vlan	Sets a vlan for the sniffer filter.

vlan

vlan *number*

no vlan

Description

Sets a vlan for the sniffer filter.

Inserting **no** as a prefix for this command will reset the vlan sniffer filter.

Syntax

Parameter	Description
<i>number</i>	VLAN interface number for capture. (Range: 1-4094)

Default

No default is defined.

Command Modes

Sniffer configuration.

Command History

Release	Modification
13.4	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to set the vlan filter.

```
DmSwitch(config-sniffer-1)#vlan 1
DmSwitch(config-sniffer-1)#
```

Related Commands

Command	Description
<code>clear capture</code>	Clear packet capture files.
<code>show capture file</code>	Show packets captured contained in a file.
<code>show capture files</code>	Shows a list of files containing packet captures.
<code>show capture realtime</code>	Show packets captured in realtime.
<code>sniffer</code>	Accesses the sniffer instance.
<code>accepted</code>	Sets the type of packet (accepted/discarded) being filtered by sniffer.
<code>direction</code>	Sets the direction of the packet to be filtered by sniffer.
<code>enable</code>	Enables the sniffer.
<code>interface-ethernet</code>	Setse an ethernet interface over which packets are filtered by sniffer.
<code>max-packets</code>	Sets the limit of packets to be captured by the sniffer.
<code>protocol</code>	Sets the protocol of the packets to be filtered by sniffer.
<code>show-config</code>	Shows the settings of sniffer.

Chapter 58. Obsolete Commands

Root Commands

clear arp-table

`clear arp-table [ip-address]`

Description

Deletes entries from the ARP table.

Syntax

Parameter	Description
<i>ip-address</i>	(Optional) Clears only the entry that contains the specified IP address.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to <code>clear cpu arp-table</code> .

Usage Guidelines

Not available.

Example

This example shows how to delete the entry that contains the specified IP address.

```
DmSwitch#clear arp-table 192.168.0.1
DmSwitch#
```

You can verify that the information was deleted by entering the **show arp-table** privileged EXEC command.

Related Commands

Command	Description
show cpu	Shows CPU information.

clear counters

clear counters [**ethernet** [*unit-number/*] *port-number* | **port-channel** *channel-group-number*]

Description

Deletes transmit and receive statistics from all ports, or from an specific port or port-channel.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Clears the entries from the specified unit and port.
port-channel <i>channel-group-number</i>	(Optional) Clears the entries from the specified port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
5.0	The command was replaced by the clear statistics command.

Usage Guidelines

Not available.

Example

This example shows how to delete transmit and receive statistics from a specific port.

```
DmSwitch#clear counters ethernet 1
DmSwitch#
```

You can verify that the information was deleted by entering the **show interface counters** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces counters</code>	Shows the interface counters information.

clear cpu-arp-table

clear cpu-arp-table [*ip-address*]

Description

Deletes entries from the CPU ARP table.

Syntax

Parameter	Description
<i>ip-address</i>	(Optional) Clears only the entry that contains the specified IP address.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
4.0	This command was introduced. Before this was called clear arp-table .
4.1	This command was renamed to clear cpu arp-table .

Usage Guidelines

Entering this command without parameters, all hosts address will be removed.

Example

This example shows how to delete the entry that contains the specified IP address.

```
DmSwitch#clear cpu-arp-table 192.168.0.1
DmSwitch#
```

You can verify that the information was deleted by entering the **show arp-table** privileged EXEC command.

Related Commands

Command	Description
show cpu	Shows CPU information.

clear ffpcounters

clear ffpcounters [*filter-counter-id*]

Description

Clears filter counters.

Syntax

Parameter	Description
<i>filter-counter-id</i>	(Optional) Clears only the counter with the specified ID. (Range: 1-32)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
5.0	The command was replaced by the clear counter command.

Usage Guidelines

Not available.

Example

This example shows how to clear all filter counters.

```
DmSwitch#clear ffpcounters
DmSwitch#
```

You can verify that the information was deleted by entering the **show counter** privileged EXEC command.

Related Commands

No related command.

clear meters

clear meters [*meter-number*]

Description

Clears the packet counters of the meters.

Syntax

Parameter	Description
<i>meter-number</i>	(Optional) Clears the packet counters of a specified meter. (Range: 1-63)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to clear meter .

Usage Guidelines

Not available.

Example

This example shows how to clear the counters of meter 3.

```
DmSwitch#clear meters 3
DmSwitch#
```

Related Commands

No related command.

clear statistics

clear statistics [**ethernet** [*unit-number/*] *port-number* | **port-channel** *channel-group-number*]

Description

Deletes transmit and receive statistics from all ports, or from an specific port or port-channel.

Syntax

Parameter	Description
ethernet [<i>unit-number/</i>] <i>port-number</i>	(Optional) Clears the entries from the specified unit and port.
port-channel <i>channel-group-number</i>	(Optional) Clears the entries from the specified port channel. The port channel must be specified in accordance with the port channel configured in the switch. (Range: 1-128)

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
5.0	This command was introduced. It replaces the command clear counters .

Usage Guidelines

Not available.

Example

This example shows how to delete transmit and receive statistics from a specific port.

```
DmSwitch#clear statistics ethernet 1
DmSwitch#
```

You can verify that the information was deleted by entering the **show interface counters** privileged EXEC command.

Related Commands

Command	Description
<code>show interfaces counters</code>	Shows the interface counters information.

show arp-table

show arp-table

Description

Shows the ARP table from CPU.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.1	This command was renamed to show cpu arp-table .

Usage Guidelines

Not available.

Example

This example illustrates how to show the ARP table.

```
DmSwitch#show arp-table
IP Address          MAC address          VLAN
-----
10.11.12.13         00:15:F2:59:B1:07    1
DmSwitch#
```

Related Commands

Command	Description
clear arp-table	Deletes entries from the ARP table.

show cpu-usage

show cpu-usage

Description

Shows CPU utilization.

Output modifiers are available for this command.

Default

No default is defined.

Command Modes

User EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to show cpu usage .

Usage Guidelines

This command shows the main CPU processes and their status, sorting by the highest execution percentage in the last 5 seconds.

Example

This example illustrates how to show the CPU utilization.

```
DmSwitch#show cpu-usage
```

```
(STATUS: S=sleeping R=running W=waiting)
```

			%CPU		
			5Sec	1Min	5Min
CPU	TOTAL	USAGE:	12.52	11.02	10.86
PID	PROCESS	STATUS			
75	traps	S	3.13	0.54	0.53
90	l2_shadow	S	2.94	4.13	4.19
91	counter	S	2.35	1.97	1.98
109	cpu_monitor	R	1.96	2.07	2.04
101	dotlxd	S	0.98	0.99	1.01
102	rmon	S	0.98	0.73	0.74
99	xstp	S	0.20	0.10	0.07
98	RX	S	0.00	0.21	0.14
88	interrupt	S	0.00	0.11	0.06
111	rx_pkt	S	0.00	0.05	0.03

```
97      TX      S      0.00      0.02      0.02
...
DmSwitch#
```

Related Commands

Command	Description
output modifiers	Options to filter text output: after, begin, exclude and include
cpu-dos-protect	CPU Protection configuration.
show memory	Shows the processor memory utilization.
show uptime	Shows the system clock, system uptime and load average.

show ip hardware vrf-table

show ip hardware vrf-table *vrf-name*

Description

Shows the Forwarding Information Base (FIB) associated to the specified VRF instance.

Syntax

Parameter	Description
<i>vrf-name</i>	Name assigned to a VRF.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
10.0	This command was renamed to show ip hardware lpm-table vrf <i>vrf-name</i>

Usage Guidelines

This command shows the FIB associated to the VRF instance, including routes that are temporarily not installed. A VPNv4 route can't be installed without an LSP to reach the remote Provider Edge (PE).

Both IPv4 and VPNv4 routes are displayed together.

Example

This example illustrates how to show the FIB of a VRF instance.

```
DmSwitch#show ip hardware vrf-table vrf1
Network subnet      Gateway            VPN Label  Type    Installed
-----
10.1.73.192/27      10.1.72.42        --         IPv4    Yes
10.1.73.0/25        10.1.72.42        --         IPv4    Yes
10.1.72.16/29       10.1.72.42        --         IPv4    Yes
10.1.72.192/27      200.200.200.5     16         VPNv4   No
10.1.72.8/29        200.200.200.3     16         VPNv4   Yes
```

Related Commands

Command	Description
<code>show ip vrf</code>	Shows VRF general information.
<code>show ip route vrf</code>	Shows the RIB of the specified VRF.

show memory

show memory

Description

Shows the processor memory utilization.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to show cpu memory .

Usage Guidelines

Not available.

Example

This example illustrates how to show the CPU memory utilization.

```
DmSwitch#show memory
Processor Memory Information:

Total: 62848 kB
Free : 26588 kB

DmSwitch#
```

Related Commands

Command	Description
cpu-dos-protect	CPU Protection configuration.

Command	Description
<code>show cpu-usage</code>	Shows CPU utilization.
<code>show uptime</code>	Shows the system clock, system uptime and load average.

show mpls binding ^[1] ^[3] ^[6]

show mpls binding ipv4 all

Description

Shows FECs bound to LSPs (FTN mapping table).

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
9.4	This command has been made obsolete.

Usage Guidelines

This command shows the Forwarding Equivalence Class (FEC) to Next Hop Label Forwarding Entry (NHLFE) Mapping table (or FEC-to-NHLFE, or simply FTN).

Each register shows a FEC that is bound to an LSP which is represented by the label(s) to be pushed to the packet.

Example

This example illustrates how to show the FTN mapping table.

```
DmSwitch#show mpls binding ipv4 all
100.100.100.3/32: Incoming Label: none;
  Outgoing Labels:
    10.1.14.42    2002
100.100.100.2/32: Incoming Label: none;
  Outgoing Labels:
    10.1.14.42    implicit-null
100.100.100.202/32: Incoming Label: none;
  Outgoing Labels:
    10.1.14.42    2003
DmSwitch#
```

Related Commands

Command	Description
<code>show ip route</code>	Shows the IP routing table.
<code>show mpls ldp database</code>	List LSP database

show mpls crossconnect ^[1] ^[3] ^[6]

show mpls crossconnect

Description

Shows current crossconnects on MPLS Label Forwarding Information Base (LFIB).

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
8.0	This command was introduced.
9.4	This command has been made obsolete.

Usage Guidelines

The **show mpls crossconnect** command shows the crossconnected labels effectively installed on MPLS LFIB.

It's also possible to verify the LDP database via **show mpls ldp database**, which shows all labels known by LDP but not necessarily installed on LFIB.

Example

This example illustrates how to show the crossconnected labels on LFIB.

```
DmSwitch#show mpls crossconnect
Local label          Outgoing label          Outgoing Next Hop
-----
2002                 implicit-null            vlan 3   10.1.14.84
3004                 implicit-null            vlan 746 10.1.14.41
2003                 4006                    vlan 3   10.1.14.84
DmSwitch#
```

Related Commands

Command	Description
<code>show ip route</code>	Shows the IP routing table.
<code>show mpls binding</code>	Shows FECs bound to LSPs (FTN mapping table).
<code>show mpls ldp database</code>	List LSP database

show qos config

show qos config [**ethernet** { **range** { [*first-unit-number/*] *first-port-number* [*last-unit-number/*] *last-port-number* } | [*unit-number/*] *port-number* }]

Description

Use to show the qos configuration.

Syntax

Parameter	Description
[<i>unit-number/</i>] <i>port-number</i>	Shows a specific unit and port queue configuration
range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Shows a range of specific units and ports queue configuration

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to show queue config .

Usage Guidelines

Not available.

Example

This example illustrates how to show the queue configuration.

```
DmSwitch#show qos config ethernet 2
-----
Port  Queue  Mode   Max-Bw   Min-Bw   Weight  SP-Queue
-----
1/ 2   0       WRR     unlimit  -----   1       NO
1/ 2   1       WRR     unlimit  -----   2       NO
1/ 2   2       WRR     unlimit  -----   4       NO
```

```
1/ 2    3    WRR  unlimit  -----    6    NO
1/ 2    4    WRR  unlimit  -----    8    NO
1/ 2    5    WRR  unlimit  -----   10    NO
1/ 2    6    WRR  unlimit  -----   12    NO
1/ 2    7    WRR  unlimit  -----   14    NO
-----
DmSwitch#
```

Related Commands

Command	Description
<code>qos max-bw</code>	Configures the maximum bandwidth allocation per queue
<code>qos sched-mode sp</code>	Configures Ethernet interface queues in Strict Priority schedule mode.
<code>qos sched-mode wfq</code>	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
<code>qos sched-mode wrr</code>	Configures Ethernet interface queues in Weighted Round Robin schedule mode
<code>qos cos-map</code>	Maps CoS priorities to queues

show qos cos-map

show qos cos-map

Description

Use to show map of CoS priorities to queues.

Syntax

No parameter accepted.

Default

No default is defined.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to show queue cos-map .

Usage Guidelines

Not available.

Example

This example illustrates how to show the CoS mappings.

```
DmSwitch#show qos cos-map
-----+-----+
Queue | 802.1P Priority |
-----+-----+
  0   | 0               |
  1   | 1               |
  2   | 2               |
  3   | 3               |
  4   | 4               |
  5   | 5               |
  6   | 6               |
  7   | 7               |
-----+-----+
DmSwitch#
```


Related Commands

Command	Description
<code>qos cos-map</code>	Maps CoS priorities to queues
<code>qos max-bw</code>	Configures the maximum bandwidth allocation per queue
<code>qos sched-mode sp</code>	Configures Ethernet interface queues in Strict Priority schedule mode.
<code>qos sched-mode wfq</code>	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
<code>qos sched-mode wrr</code>	Configures Ethernet interface queues in Weighted Round Robin schedule mode

Configure Commands

eaps

eaps

no eaps

Description

Enables the EAPS operation in the DmSwitch.

Inserting **no** as a prefix for this command will disable the EAPS operation.

Syntax

No parameter accepted.

Default

EAPS is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	This command has been made obsolete, since EAPS domain is always globally enabled.

Usage Guidelines

You must disable the spanning-tree protocol in order to use EAPS.

Example

This example shows how to enable eaps operation.

```
DmSwitch(config)#eaps
DmSwitch(config)#
```

You can verify that EAPS operation was enabled by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps domain	Creates a new EAPS domain.
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain disable	Disables the EAPS domain operation.
eaps domain enable	Enables the EAPS domain operation.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.

eaps domain disable

eaps domain disable

Description

Disables the EAPS domain operation.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain name.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	This command was obsoleted, since every existent EAPS domain is always enabled.

Usage Guidelines

Not available.

Example

This example shows how to disable a EAPS domain.

```
DmSwitch(config)#eaps test disable
DmSwitch(config)#
```

You can verify that the EAPS domain was disabled by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps	Enables the EAPS operation in the DmSwitch.
eaps domain	Creates a new EAPS domain.

Command	Description
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain enable	Enables the EAPS domain operation.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.

eaps *domain* enable

eaps *domain* **enable**

Description

Enables the EAPS domain operation.

Syntax

Parameter	Description
<i>domain</i>	Specifies a domain name.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
5.0	This command has been made obsolete since EAPS domain is always enabled.

Usage Guidelines

Not available.

Example

This example shows how to enable a EAPS domain.

```
DmSwitch(config)#eaps test enable
DmSwitch(config)#
```

You can verify that the EAPS domain was enabled by entering the **show eaps** privileged EXEC command.

Related Commands

Command	Description
eaps	Enables the EAPS operation in the DmSwitch.
eaps domain	Creates a new EAPS domain.

Command	Description
eaps domain control-vlan	Configures the control VLAN for the EAPS domain.
eaps domain disable	Disables the EAPS domain operation.
eaps domain failtime	Defines the interval time that the secondary port of DmSwitch master in a EAPS ring waits without receiving the two hello packets before changing the status of EAPS ring to fail.
eaps domain hellotime	Defines the interval between the sending of two hello packets.
eaps domain mode	Configures the mode of DmSwitch in EAPS domain.
eaps domain packet-mode	Configures the encapsulation of EAPS PDUs in the domain.
eaps domain name	Renames the domain.
eaps domain port	Defines both primary and secondary ports of DmSwitch in EAPS ring.
eaps domain protected-vlans	Defines the VLAN groups that will be protected by EAPS ring.
show eaps	Shows EAPS settings.
show running-config	Shows the current operating configuration.

qos cos-map

```
qos cos-map { queue-id priority 1st_queue_prio } [ 2nd_queue_prio ... 8th_queue_prio ]
```

```
no qos cos-map
```

Description

Configure the map of CoS priorities to queues.

Syntax

Parameter	Description
<i>queue-id</i>	Selects a meter to edit by ID
priority	Select CoS priorities mapped to this queue.
<i>1st_queue_prio</i>	1st CoS Priority of 8 possible.
<i>2nd_queue_prio</i>	(Optional) 2nd CoS Priority of 8 possible.
...	...
<i>8th_queue_prio</i>	(Optional) 8th CoS Priority of 8 possible.

Default

Queue	802.1P Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to queue cos-map .

Usage Guidelines

Not available.

Example

This example shows how to map CoS priorities 0, 3 and 6 to queue 5.

```
DmSwitch(config)#qos cos-map 5 priority 0 3 6
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show qos cos-map** privileged EXEC command.

Related Commands

Command	Description
show qos cos-map	Shows priority mappings
qos max-bw	Configures the maximum bandwidth allocation per queue
qos sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
qos sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
qos sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
show running-config	Shows the current operating configuration.

qos max-bw

```
qos max-bw { unlim-all | { { unlimited | bandwidth } { unlimited | bandwidth } {  
unlimited | bandwidth } { unlimited | bandwidth } { unlimited | bandwidth } { unlimited |  
bandwidth } { unlimited | bandwidth } { unlimited | bandwidth } } } { ethernet { all | [  
unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [ last-unit-number/ ]  
last-port-number } } }
```

no qos max-bw

Description

Configure the maximum bandwidth allocation per queue.

Syntax

Parameter	Description
unlim-all	Selects unlimited bandwidth for all queues
unlimited	Selects unlimited bandwidth for queue 1
<i>bandwidth</i>	Max bw for queue 1 in kbit/s (64 kbit/s granularity)
...	...
unlimited	Selects unlimited bandwidth for queue 8
<i>bandwidth</i>	Max bw for queue 8 in kbit/s (64 kbit/s granularity)
all	Adds all ports
[<i>unit-number/</i>] <i>port-number</i>	Adds a specific unit and port
range [<i>first-unit-number/</i>] <i>first-port-number</i> [<i>last-unit-number/</i>] <i>last-port-number</i>	Adds a range of specific units and ports

Default

The default is unlimited bandwidth for all queues of all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to queue max-bw .

Usage Guidelines

Not available.

Example

This example shows how to configure maximum queue bandwidths to Ethernet interface 5.

```
DmSwitch(config)#qos max-bw 10048 unlimited 30016 unlimited 50048 60032 70016 8000 ethernet 5
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show qos max-bw** privileged EXEC command.

Related Commands

Command	Description
show qos config	Shows queue configuration per port
qos sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
qos sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
qos sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
qos cos-map	Maps CoS priorities to queues
show running-config	Shows the current operating configuration.

qos sched-mode sp

```
qos sched-mode sp { unit unit-number ethernet { all | [ 1to8 9to16 17to24 25 26 27 28 ] } }
```

```
no qos sched-mode
```

Description

Configure Ethernet interface queues in the Strict Priority schedule mode.

Syntax

Parameter	Description
unit <i>unit-number</i>	Stack unit
all	Adds all Ethernet interfaces
1to8	Adds ports 1 to 8
9to16	Adds ports 9 to 16
17to24	Adds ports 17 to 24
25	Adds port 25
26	Adds port 26
27	Adds port 27
28	Adds port 28

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Queue	Weight
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to queue sched-mode sp .

Usage Guidelines

Not available.

Example

This example shows how to configure sp schedule mode to Ethernet interfaces 9 to 16.

```
DmSwitch(config)#qos sched-mode sp unit 1 ethernet 9to16
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show qos config** privileged EXEC command.

Related Commands

Command	Description
show qos config	Shows queue configuration per port
qos sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
qos sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
qos cos-map	Maps CoS priorities to queues
qos max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

qos sched-mode wfq

```
qos sched-mode wfq { unit unit-number ethernet { all | [ 1to8 9to16 17to24 25 26  
27 28 ] } [ min-bw { bandwidth | sp } { bandwidth | sp } { bandwidth | sp } { bandwidth | sp } {  
bandwidth | sp } { bandwidth | sp } { bandwidth | sp } { bandwidth | sp } ] }
```

no qos sched-mode

Description

Configure Ethernet interface queues in the Weighted Fair Queueing schedule mode.

Syntax

Parameter	Description
<i>unit-number</i>	Stack unit
all	Adds all Ethernet interfaces
1to8	Adds ports 1 to 8
9to16	Adds ports 9 to 16
17to24	Adds ports 17 to 24
25	Adds port 25
26	Adds port 26
27	Adds port 27
28	Adds port 28
<i>bandwidth</i>	Minimum bandwidth for queue in kbit/s (64 kbit/s granularity)
sp	Configures queue in strict priority

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to queue sched-mode wfq .

Usage Guidelines

Not available.

Example

This example shows how to configure wfq schedule mode to Ethernet interfaces 25 with different minimum bandwidth.

```
DmSwitch(config)#qos sched-mode wfq unit 1 ethernet 25 min-bw 1024 2048 sp sp sp sp 7040 sp
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show qos config** privileged EXEC command.

Related Commands

Command	Description
show qos config	Shows queue configuration per port
qos sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
qos sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
qos cos-map	Maps CoS priorities to queues
qos max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

qos sched-mode wrr

```
qos sched-mode wrr { unit unit-number ethernet { all | [ 1to8 9to16 17to24 25 26 27 28 ] } [ queue-weights { weight | sp } { weight | sp } { weight | sp } { weight | sp } { weight | sp } { weight | sp } { weight | sp } { weight | sp } ] }
```

no qos sched-mode

Description

Configure Ethernet interface queues in the Weighted Round Robin schedule mode.

Syntax

Parameter	Description
<i>unit-number</i>	Stack unit
all	Adds all Ethernet interfaces
1to8	Adds ports 1 to 8
9to16	Adds ports 9 to 16
17to24	Adds ports 17 to 24
25	Adds port 25
26	Adds port 26
27	Adds port 27
28	Adds port 28
<i>weight</i>	Weight for queue
sp	Queue in Strict Priority

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Queue	Weight
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	This command was renamed to queue sched-mode wrr .

Usage Guidelines

Not available.

Example

This example shows how to configure wrr schedule mode to Ethernet interfaces 25 with different weights.

```
DmSwitch(config)#qos sched-mode wrr unit 1 ethernet 25 queue-weights 2 3 5 sp sp sp 8 15
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show qos config** privileged EXEC command.

Related Commands

Command	Description
show qos config	Shows queue configuration per port
qos sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
qos sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
qos cos-map	Maps CoS priorities to queues
qos max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

queue max-bw

```
queue max-bw { unlim-all | { { unlimited | bandwidth1 } { unlimited | bandwidth2 }  
{ unlimited | bandwidth3 } { unlimited | bandwidth4 } { unlimited | bandwidth5 } {  
unlimited | bandwidth6 } { unlimited | bandwidth7 } { unlimited | bandwidth8 } } } {  
ethernet { all | [ unit-number/ ] port-number | range { [ first-unit-number/ ] first-port-number [  
last-unit-number/ ] last-port-number } } }
```

no queue max-bw

Description

Configure the maximum bandwidth allocation per queue.

Syntax

Parameter	Description
unlim-all	Selects unlimited bandwidth for all queues.
unlimited	Selects unlimited bandwidth for a queue.
<i>bandwidth1 ... bandwidth8</i>	Maximum bandwidth for each queue in kbit/s (64 kbit/s granularity).
all	Adds all ports.
<i>[unit-number/] port-number</i>	Adds a specific unit and port.
range <i>[first-unit-number/] first-port-number [last-unit-number/] last-last-port-number</i>	Adds a range of specific units and ports.

Default

The default is unlimited bandwidth for all queues of all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced. Before this was called qos max-bw .
5.0	This command was moved to Interface Ethernet menu.

Usage Guidelines

Not available.

Example

This example shows how to configure maximum queue bandwidths to Ethernet interface 5.

```
DmSwitch(config)#queue max-bw 10048 unlimited 30016 unlimited 50048 60032 70016 8000 ethernet 5
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue max-bw** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
show running-config	Shows the current operating configuration.

queue sched-mode sp

```
queue sched-mode sp { unit unit-number ethernet { all | [ 1to8 | 9to16 | 17to24 | 25 | 26 | 27 | 28 ] } }
```

no queue sched-mode

Description

Configure Ethernet interface queues in the Strict Priority schedule mode.

Syntax

Parameter	Description
unit <i>unit-number</i>	Stack unit.
all	Adds all Ethernet interfaces.
1to8, 9to16, 17to24, 25, 26, 27, 28	Adds ports 1 to 8, 9 to 16, 17 to 24, 25, 26, 27 and 28 respectively. This command accepts any combination among all these parameters (1to8 , 9to16 , 17to24 , 25 , 26 , 27 and 28).

Default

The default queue schedule mode is wrp for all Ethernet interfaces.

Queue	Weight
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Command Modes

Global configuration.

Command History

Release	Modification
---------	--------------

Release	Modification
4.0	This command was introduced. Before this was called qos sched-mode sp .
5.0	This command was moved to Interface Ethernet menu.

Usage Guidelines

Not available.

Example

This example shows how to configure sp schedule mode to Ethernet interfaces 9 to 16.

```
DmSwitch(config)#queue sched-mode sp unit 1 ethernet 9to16
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

queue sched-mode wfq

```
queue sched-mode wfq { unit unit-number ethernet { all | [ 1to8 | 9to16 | 17to24 | 25  
| 26 | 27 | 28 ] } [ min-bw { bandwidth1 | sp } { bandwidth2 | sp } { bandwidth3 | sp } { bandwidth4  
| sp } { bandwidth5 | sp } { bandwidth6 | sp } { bandwidth7 | sp } { bandwidth8 | sp } ] }
```

no queue sched-mode

Description

Configure Ethernet interface queues in the Weighted Fair Queueing schedule mode.

Syntax

Parameter	Description
<i>unit-number</i>	Stack unit.
all	Adds all Ethernet interfaces.
1to8, 9to16, 17to24, 25, 26, 27, 28	Adds ports 1 to 8, 9 to 16, 17 to 24, 25, 26, 27 and 28 respectively. This command accepts any combination among all these parameters (1to8, 9to16, 17to24, 25, 26, 27 and 28).
<i>bandwidth1 ... bandwidth8</i>	Minimum bandwidth for each queue in kbit/s (64 kbit/s granularity).
sp	Configures queue in strict priority.

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Command Modes

Global configuration.

Command History

Release	Modification
4.0	This command was introduced. Before this was called qos sched-mode wfq .
5.0	This command was moved to Interface Ethernet menu.

Usage Guidelines

Not available.

Example

This example shows how to configure wfq schedule mode to Ethernet interfaces 25 with different minimum bandwidth.

```
DmSwitch(config)#queue sched-mode wfq unit 1 ethernet 25 min-bw 1024 2048 sp sp sp sp 7040 sp
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wrr	Configures Ethernet interface queues in Weighted Round Robin schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

queue sched-mode wrr

```
queue sched-mode wrr { unit unit-number ethernet { all | [ 1to8 | 9to16 | 17to24 | 25  
| 26 | 27 | 28 ] } [ queue-weights { weight1 | sp } { weight2 | sp } { weight3 | sp } { weight4 | sp  
} { weight5 | sp } { weight6 | sp } { weight7 | sp } { weight8 | sp } ] }
```

no queue sched-mode

Description

Configure Ethernet interface queues in the Weighted Round Robin schedule mode.

Syntax

Parameter	Description
<i>unit-number</i>	Stack unit
all	Adds all Ethernet interfaces.
1to8, 9to16, 17to24, 25, 26, 27, 28	Adds ports 1 to 8, 9 to 16, 17 to 24, 25, 26, 27 and 28 respectively. This command accepts any combination among all these parameters (1to8, 9to16, 17to24, 25, 26, 27 and 28).
<i>weight1 ... weight8</i>	Weight for each queue.
sp	Configures queue in strict priority.

Default

The default queue schedule mode is wrr for all Ethernet interfaces.

Queue	Weight
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Command Modes

Global configuration.

Command History

Release Modification

- | | |
|-----|---|
| 4.0 | This command was introduced. Before this was called qos sched-mode wrr . |
| 5.0 | This command was moved to Interface Ethernet menu. |

Usage Guidelines

Not available.

Example

This example shows how to configure wrr schedule mode to Ethernet interfaces 25 with different weights.

```
DmSwitch(config)#queue sched-mode wrr unit 1 ethernet 25 queue-weights 2 3 5 sp sp sp 8 15
DmSwitch(config)#
```

You can verify that the configuration was set by entering the **show queue config** privileged EXEC command.

Related Commands

Command	Description
show queue config	Shows queue configuration per port
queue sched-mode sp	Configures Ethernet interface queues in Strict Priority schedule mode.
queue sched-mode wfq	Configures Ethernet interface queues in Weighted Fair Queueing schedule mode
queue cos-map	Maps CoS priorities to queues
queue max-bw	Configures the maximum bandwidth allocation per queue
show running-config	Shows the current operating configuration.

radius-server port

radius-server port { *port-number* }

no radius-server port

Description

Configures the default RADIUS server port.

Inserting **no** as a prefix for this command will return to the default port number.

Syntax

Parameter	Description
<i>port-number</i>	Specifies the port number. (Range: 1-65535)

Default

Port number: 1812.

Command Modes

Global Configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.1	This command was renamed to radius-server auth-port .

Usage Guidelines

The authentication login by a RADIUS server uses this default server port if no port is configured to a specific RADIUS host.

Example

This example shows how to change the default RADIUS port number.

```
DmSwitch(config)#radius-server port 6500
DmSwitch(config)#
```

The configuration can be verified by entering the **show radius-server** privileged EXEC command.

Related Commands

Command	Description
<code>authentication login</code>	Defines the login authentication method and its precedence.
<code>radius-server host</code>	Configures a specific RADIUS server.
<code>radius-server key</code>	Configures the default RADIUS server key string.
<code>radius-server retries</code>	Configures the RADIUS server retries.
<code>radius-server timeout</code>	Configures the RADIUS server timeout.
<code>show running-config</code>	Shows the current operating configuration.
<code>show radius-server</code>	Shows RADIUS server information.

spanning-tree *instance* vlan

spanning-tree *instance* **vlan** { *index* | **all** | **range** *first-index last-index* }

no spanning-tree *instance* **vlan** { *index* | **all** | **range** *first-index last-index* }

Description

Adds VLANs to a spanning-tree instance.

Inserting **no** as a prefix for this command will remove the specified VLANs from spanning-tree instance.

Syntax

Parameter	Description
<i>instance</i>	Specifies the spanning-tree instance. (Range: 0-15)
<i>index</i>	Specifies a VLAN ID. (Range: 1-4094)
all	Specifies all VLANs.
range <i>first-index last-index</i>	Specifies a range of VLAN IDs.

Default

No default is defined.

Command Modes

Global configuration.

Command History

Release	Modification
3.1	This command was introduced.
4.0	The instance range was changed from 1-15 to 0-15.
5.0	The command was replaced by spanning-tree instance vlan-group command.

Usage Guidelines

Not available.

Example

This example shows how to add a range of VLANs to a spanning-tree instance.

```
DmSwitch(config)#spanning-tree 1 vlan range 1 10
DmSwitch(config)#
```

You can verify that the VLANs was added by entering the **show spanning-tree instance** privileged EXEC command.

Related Commands

Command	Description
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree	Configure Spanning-Tree parameters.
spanning-tree instance	Enables a Spanning-tree instance.
spanning-tree (Interface configuration)	Adds an Ethernet interface in a Spanning-Tree instance.
spanning-tree bpduguard	Enables the Bridge Protocol Data Unit (BPDU) guard.
spanning-tree edge-port (Interface configuration)	Defines the Ethernet interface as the spanning-tree edge port.
spanning-tree instance	Configures an Ethernet interface in a Spanning-Tree instance.
spanning-tree instance forward-delay	Configures the Spanning-Tree Algorithm forward delay time.
spanning-tree instance hello-time	Configures the Spanning-Tree Algorithm hello time.
spanning-tree instance max-age	Configures the Spanning-Tree Algorithm maximum age.
spanning-tree instance priority	Specifies the spanning-tree priority in the DmSwitch.
spanning-tree link-type	Specifies the type of link used with spanning-tree.
spanning-tree mode	Configures the spanning-tree mode.
spanning-tree mst	Defines parameters of Multiple Spanning-Tree configuration.
show running-config	Shows the current operating configuration.
show spanning-tree	Shows spanning-tree configuration and status.
vlan group	Create a VLAN group and manage its members.

MPLS RSVP Commands

rsvp enable [1] [3] [6]

rsvp enable

no rsvp enable

Description

Enables RSVP Protocol. The equipment is not able to handle (send/receive) RSVP messages when RSVP is disabled.

Inserting **no** as a prefix for this command will disable RSVP protocol.

Syntax

No parameter accepted.

Default

By default the RSVP Protocol is enabled.

Command Modes

MPLS RSVP Global configuration.

Command History

Release	Modification
10.0	First release. Command introduced.
14.4	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to enable and disable the RSVP Protocol.

```
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#rsvp enable
DmSwitch(config-mpls-rsvp)#

DmSwitch(config)#mpls rsvp
```

```
DmSwitch(config-mpls-rsvp)#no rsvp enable
DmSwitch(config-mpls-rsvp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls traffic-eng fast-reroute revertive global	Globally enables fast-reroute revertive behavior
signalling hello graceful-restart	Enables RSVP hello graceful restart indication
signalling refresh interval	Configures the interval at which RSVP messages (PATH/RESV) are sent to each neighbor
signalling refresh misses	Configures the number of missed RSVP messages (PATH/RESV) before making neighbor down
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

signalling hello graceful-restart ^[1] ^[3] ^[6]

signalling hello graceful-restart

no signalling hello graceful-restart

Description

Enables RSVP hello graceful restart indication as described in RFC3473.

Inserting **no** as a prefix for this command will disable RSVP hello graceful restart indication.

Syntax

No parameter accepted.

Default

By default the RSVP hello graceful restart indication is enabled

Command Modes

MPLS RSVP Global configuration.

Command History

Release	Modification
10.0	First release. Command introduced.
12.0	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to enable and disable the RSVP hello graceful restart indication.

```
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#signalling hello graceful-restart
DmSwitch(config-mpls-rsvp)#
```

```
DmSwitch(config)#mpls rsvp
DmSwitch(config-mpls-rsvp)#no signalling hello graceful-restart
DmSwitch(config-mpls-rsvp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>mpls traffic-eng fast-reroute revertive global</code>	Globally enables fast-reroute revertive behavior
<code>rsvp enable</code>	Enables RSVP protocol
<code>signalling refresh interval</code>	Configures the interval at which RSVP messages (PATH/RESV) are sent to each neighbor
<code>signalling refresh misses</code>	Configures the number of missed RSVP messages (PATH/RESV) before making neighbor down
<code>show mpls rsvp</code>	Show counters of RSVP messages
<code>show mpls te traffic-eng tunnels</code>	Shows Traffic Engineering Tunnel Information

MPLS TE Commands

tunnel mpls traffic-eng bypass ^[1] ^[3] ^[6]

`tunnel mpls traffic-eng bypass protect vlan vlan`

`no tunnel mpls traffic-eng bypass`

Description

Configures the RSVP Tunnel as a bypass tunnel in order to protect a specific interface for Facility fast-reroute.

Inserting **no** as a prefix for this command will revert bypass configuration.

Syntax

Parameter	Description
<i>vlan</i>	VLAN ID

Default

No default is defined.

Command Modes

MPLS TE configuration mode.

Command History

Release	Modification
10.0	First release. Command introduced.
10.0	This command was deprecated.

Usage Guidelines

Tunnel must be disabled to perform any change. Use: **shutdown** and afterwards **no shutdown**.

Example

This example shows how to configure the RSVP tunnel as a bypass tunnel in order to protect VLAN 400.

```
DmSwitch(config)#mpls te
```

```

DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#tunnel mpls traffic-eng bypass protect vlan 400
DmSwitch(config-mpls-te-if-10)#

DmSwitch(config)#mpls te
DmSwitch(config-mpls-te)#interface te-tunnel 10
DmSwitch(config-mpls-te-if-10)#no tunnel mpls traffic-eng bypass
DmSwitch(config-mpls-te-if-10)#

```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
mpls te	Enters on Traffic Engineering Configuration Mode
interface te-tunnel	Enters on Tunnel Configuration Mode
tunnel mpls destination	Configures the RSVP tunnel egress
tunnel mpls traffic-eng affinity	Configures RSVP Tunnel affinity
tunnel mpls traffic-eng autoroute announce	Configures RSVP tunnel to be announced into IGP
tunnel mpls traffic-eng autoroute metric	Configures the autoroute metric
tunnel mpls traffic-eng bandwidth bw_value	Configures the bandwidth associated to the RSVP tunnel
tunnel mpls traffic-eng fast-reroute	Enables the creation of alternative paths for Fast-Reroute
tunnel mpls traffic-eng igp ospf area	Sets the OSPF area associated with the RSVP tunnel
tunnel mpls traffic-eng path-option po_number explicit identifier ei_number	Configures the path-option index and the explicit path identifier
tunnel mpls traffic-eng record-route	Enables the Record-Route Object
tunnel name	Configures the RSVP tunnel name
shutdown	Disables administratively an RSVP tunnel
show mpls rsvp	Show counters of RSVP messages
show mpls te traffic-eng tunnels	Shows Traffic Engineering Tunnel Information

Router BGP Commands

bgp bestpath

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Description

Change the default BGP bestpath selection.

The **no** command restores the BGP bestpath selection to the default value.

Syntax

No parameter accepted.

Default

Does not ignore as-path length in selecting a route.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was removed.
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to change the the default bestpath selection to ignore as-path length in selecting a route.

```
DmSwitch(config-router-bgp)#bgp bestpath as-path ignore
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
<code>show ip bgp</code>	Shows the BGP routing table entries.
<code>show running-config</code>	Shows the current operating configuration.

bgp fast-external-failover

bgp fast-external-failover

no bgp fast-external-failover

Description

Configures to immediate reset the BGP session if a link to a directly connected external peer goes down.
The **no** command cancel the configuration.

Syntax

No parameter accepted.

Default

The command is enabled.

Command Modes

Router BGP configuration.

Command History

Release	Modification
9.4	This command was removed.
5.0	This command was introduced.

Usage Guidelines

Not available.

Example

This example shows how to disable the automatic resetting of BGP sessions.

```
DmSwitch(config-router-bgp)#no bgp fast-external-failover
DmSwitch(config-router-bgp)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
---------	-------------

Command	Description
<code>show ip bgp</code>	Shows the BGP routing table entries.
<code>show running-config</code>	Shows the current operating configuration.

maximum routes

maximum routes *limit*

no maximum routes

Description

Configures the maximum number of routes allowed in a VRF table inside BGP.

Inserting **no** as a prefix for this command will remove the limit on the maximum number of routes allowed.

Syntax

Parameter	Description
<i>limit</i>	Specifies the maximum number of routes allowed in a VRF.

Default

The default value is the maximum of 8 routes allowed in a VRF.

Command Modes

BGP IP Version 4 address family configuration mode associated with a VRF instance.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Use the **maximum routes** command to limit the number of routes allowed in a VRF inside BGP. This command prevents the router from importing too many routes into a VRF through BGP.

Example

This example shows how to configure the maximum number of VRF routes allowed to 100.

```
DmSwitch(config-router-bgp)#address-family ipv4 vrf vpn1
DmSwitch(config-router-bgp-af-vrf)#maximum routes 100
DmSwitch(config-router-bgp-af-vrf)#
```


You can verify the configuration by entering the **show ip running-config** privileged EXEC command.

Related Commands

Command	Description
address-family	Enters the specified BGP address family configuration mode.
show running-config	Shows the current operating configuration.

Route-Map Commands

description

description *text*

no description

Description

Use the description command to insert some descriptive text for the route map rule.

Inserting **no** as a prefix for this command will remove the description.

Syntax

Parameter	Description
<i>text</i>	Comment describing the route map rule.

Default

No default is defined.

Command Modes

Route-map configuration.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Not available.

Example

The following example set the description "Import routes from peer A" for the route map.

```
DmSwitch(config-route-map)#description Import routes from peer A
```

You can verify the configurations by entering the **show route-map** command.

Related Commands

Command	Description
route-map	Create route-map or enter route-map command mode.
match as-path	Matches as-path values from routing table.
match community	Matches community values from routing table.
match extcommunity	Matches extcommunity values from routing table.
match ip address prefix-list	Matches ip address by prefix-list values from routing table.
match ip next-hop prefix-list	Matches next-hop ip values from routing table.
match ip route-source prefix-list	Matches route-source ip values from routing table.
match metric	Matches metric values from routing table.
set as-path	Sets as-path values in destination routing protocol.
set as-path-limit	Sets as-path-limit values in destination routing protocol.
set community	Sets community values in destination routing protocol.
set extcommunity	Sets extcommunity values in destination routing protocol.
set local-preference	Sets local-preference value in destination routing protocol.
set metric	Sets metric value in destination routing protocol.
set next-hop	Sets next_hop value in destination routing protocol.
set origin	Sets origin value in destination routing protocol.
set weight	Sets weight value in destination routing protocol.
continue	Executes additional entries in a route map.
show running-config	Shows the current operating configuration.

Router OSPF Commands

area id/ip-address_id shortcut

area { *id* | *ip-address_id* } **shortcut** { **default** | **disable** | **enable** }

no area { *id* | *ip-address_id* } **shortcut**

Description

Configures the area's shortcutting mode.

The **no** command removes the shortcut configuration.

Syntax

Parameter	Description
<i>id</i>	Specifies the OSPF area ID as a decimal value. (Range: 0-4294967295)
<i>ip-address_id</i>	Specifies the OSPF area ID in IP address format.
default	Configures the default shortcutting behavior.
disable	Disables shortcutting through the area.
enable	Enables shortcutting through the area.

Default

Area's shortcutting mode is not configured.

Command Modes

Router OSPF configuration.

Command History

Release	Modification
4.0	This command was introduced.
9.4	This command was deprecated.

Usage Guidelines

Not available.

Example

This example shows how to enable shortcutting through an area.

```
DmSwitch(config-router-ospf)#area 0 shortcut enable
DmSwitch(config-router-ospf)#
```

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show ip ospf	Shows the OSPF process parameters.
show running-config	Shows the current operating configuration.

Chapter 59. Notes

Command not available to

1. DmSwitch 3000
2. DM4000
3. ETH12GX, ETH24GX, ETH2x10GX, ETH12GX+1x10GX, ETH24GT and ETH48GT
4. DM4000 H Series
5. DM4100
6. Modules from DM4100 family without MPLS support.
7. DM4000 L Series
8. DM4100 Enduro

Command only available for

9. PWE3 ETH20GX+32E1 H Series, PWE3 ETH20GX+2x10GX+32E1 H Series and PWE3 ETH16GX+4STM1 H Series