

DATACOM



DmSwitch

Versão 15.2.18

GUIA DE CONFIGURAÇÃO RÁPIDA

204.0333.06 - 16 de junho de 2021

Contatos

Suporte Técnico

A Datacom disponibiliza um portal de atendimento - DmSupport, para auxílio aos clientes no uso e configuração de nossos equipamentos.

O acesso ao DmSupport pode ser feito através do link: <https://supportcenter.datacom.com.br>

Neste portal estão disponíveis firmwares, descritivos técnicos, guia de configuração, MIBs e manuais para download. Além disto, permite a abertura de chamados para atendimento com a nossa equipe técnica.

Para contato telefônico: **+55 51 3933-3122**

Salientamos que o atendimento de nosso suporte por telefone ocorre de segunda a sexta-feira das 08:00 as 17:30.

Importante: Para atendimento de suporte em regime 24x7, favor solicitar cotação ao nosso setor comercial.

Informações Gerais

Para qualquer outra informação adicional, visite <https://www.datacom.com.br> ou entre em contato:

DATACOM

Rua América, 1000

92990-000 - Eldorado do Sul - RS - Brazil

+55 51 3933-3000

Documentações de Produto

Este documento é parte de um conjunto de documentações preparado para oferecer todas as informações necessárias sobre os produtos DATACOM.

Plataforma de Software

- **Guia de Configuração Rápida** - Fornece orientações sobre como configurar as funcionalidades de forma rápida no equipamento
- **Referência de Comandos** - Fornece todos os comandos pertinentes ao produto (apenas em inglês)
- **Release Notes** - Fornece orientações sobre as novas funcionalidades, defeitos conhecidos e compatibilidades entre Software e Hardware

Plataforma de Hardware

- **Descritivo** - Fornece as características técnicas do Hardware e Software do produto
- **Guia de Instalação** - Fornece orientações sobre os procedimentos para instalação do produto

A disponibilidade de alguns documentos pode variar dependendo do tipo de produto.

Acesse <https://supportcenter.datacom.com.br> para localizar as documentações relacionadas ou entre em contato com o Suporte Técnico para mais informações.



Introdução ao documento

Sobre este documento

Este documento é uma coleção de orientações que proveem uma explanação rápida e objetiva sobre o uso das funcionalidades disponíveis no produto. Também cobre as configurações iniciais que normalmente são necessárias imediatamente após a instalação do produto.

Esse documento foi elaborado para servir como uma fonte eventual para resolução de questões técnicas, por isso sua leitura sequencial não é mandatória. Entretanto, se você está configurando o equipamento e não é familiar com o produto é recomendada a leitura do documento desde o princípio.

É assumido que o indivíduo ou indivíduos que gerenciam qualquer aspecto do produto tenham conhecimentos básicos de Ethernet, protocolos de rede e redes de comunicações em geral.


Público-Alvo






Este guia é voltado para administradores de rede, técnicos ou equipes qualificadas para instalar, configurar, planejar e manter este produto.

Convenções

Para facilitar o entendimento ao longo deste manual foram adotadas as seguintes convenções:

Ícones

Ícone	Tipo	Descrição
	Nota	As notas explicam melhor algum detalhe apresentado no texto.

Ícone	Tipo	Descrição
	Nota	Símbolo da diretiva WEEE (Aplicável para União Europeia e outros países com sistema de coleta seletiva). Este símbolo no produto ou na embalagem indica que o produto não pode ser descartado junto com o lixo doméstico. No entanto, é sua responsabilidade levar os equipamentos a serem descartados a um ponto de coleta designado para a reciclagem de equipamentos eletroeletrônicos. A coleta separada e a reciclagem dos equipamentos no momento do descarte ajudam na conservação dos recursos naturais e garantem que os equipamentos serão reciclados de forma a proteger a saúde das pessoas e o meio ambiente. Para obter mais informações sobre onde descartar equipamentos para reciclagem entre em contato com o revendedor local onde o produto foi adquirido.
	Perigo	Indica que, caso os procedimentos não sejam corretamente seguidos, existe risco de choque elétrico.
	Perigo	Indica presença de radiação laser. Se as instruções não forem seguidas e se não for evitada a exposição direta à pele e olhos, pode causar danos à pele ou danificar a visão.
	Perigo	Indica emissão de radiação não ionizante.
	Advertência	Esta formatação indica que o texto aqui contido tem grande importância e há risco de danos.
	Advertência	Indica equipamento ou parte sensível à eletricidade estática. Não deve ser manuseado sem cuidados como pulseira de aterramento ou equivalente.



Um ícone de advertência pede atenção para condições que, se não evitadas, podem causar danos físicos ao equipamento.



Um ícone de perigo pede atenção para condições que, se não evitadas, podem resultar em risco de morte ou lesão grave.

Sumário

Contatos	2
Documentações de Produto	3
Introdução ao documento	4
1 Iniciando	9
1.1 Instalando e energizando o Equipamento	9
1.2 Conectando via porta Console	9
1.3 Conectando via porta de gerência out-of-band	9
1.4 Conectando pela primeira vez no equipamento	10
2 Atualização de Firmware	11
3 Gerenciamento da Configuração	13
3.1 Modo Operacional	13
3.2 Modo de Configuração	14
3.3 Configurações Salvas	14
3.4 Restaurando Configuração	14
3.5 Exportando os Arquivos	15
3.6 Restaurando a Configuração de Fábrica	15
3.7 Reset de senha	15
4 Gerenciamento do Equipamento	17
4.1 Configurando a Gerência Out-Of-Band	17
4.2 Configurando a Gerência In-Band	18
4.3 Configurando o Hostname	18
4.4 Configurando o relógio e data do sistema	19
4.5 Configurando o SNTP	19
4.6 Configurando o Syslog remoto	20
4.7 Configurando o SNMP	21
4.8 Ativando a Licença MPLS	22
5 Ferramentas de Conectividade	23
5.1 Ping e Ping6	23
5.2 Traceroute e Traceroute6	23
5.3 SSH Client e Telnet Client	24
6 Autenticação de Usuários	25
6.1 Níveis de acesso	25
6.2 Configurando Usuários Locais	25

6.3 Configurando o TACACS+	26
6.4 Configurando o RADIUS	26
6.5 Configurando a ordem de autenticação	27
7 Interfaces	28
7.1 Configurando as Interfaces Ethernet	28
7.2 Configurando o Link-aggregation (Port-Channel Estático)	28
7.3 Configurando o Link-aggregation (LACP)	29
7.4 Configurando o Port Mirroring	30
8 OAM	31
8.1 Configuração do RDM	31
8.1.1 Configurando o RDM como mestre	32
8.1.2 Configurando o RDM como escravo	32
8.1.3 Comunicação Mestre/Escravo	32
8.1.4 Configuração do limite global de pacotes repassados para remotos	33
8.1.5 Configuração de serviços disponibilizados no remoto	33
8.1.6 Verificando o RDM	33
9 Switching	34
9.1 Configurando o aging time da tabela MAC	34
9.2 Configurando VLAN com interfaces tagged	35
9.3 Configurando VLAN com interfaces untagged	35
9.4 Configurando o QinQ	36
9.5 Configurando VLAN-translate	36
9.6 Configurando RSTP	37
9.7 Configurando EAPS	38
10 Roteamento	40
10.1 Configurando Roteamento Estático	40
10.2 Configurando Roteamento Entre VLANs	41
10.3 Configurando OSPFv2	41
10.4 Configurando BGP IPv4	43
11 MPLS	45
11.1 Configurando uma L2VPN VPWS Port-Based	45
11.2 Configurando uma L2VPN VPWS VLAN-Based	47
11.3 Configurando uma L2VPN VPLS VLAN-Based	49
11.4 Configurando uma L3VPN	52
12 Segurança	55

12.1 Configurando Rate Limit	55
12.2 Configurando Storm Control	55
12.3 Configurando Port Security	56
12.4 Configurando SSH e Telnet	57
Nota Legal	59
Garantia	59

1 Iniciando

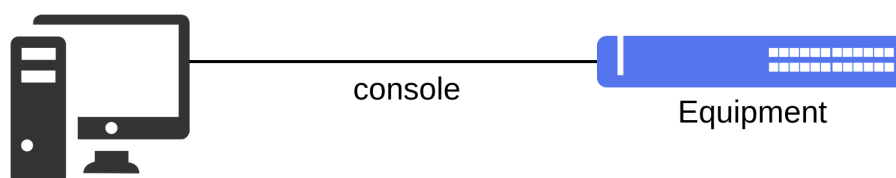
Este capítulo contém as seguintes seções:

- Instalando e energizando o equipamento
- Conectando via porta console
- Conectando via porta de gerência out-of-band
- Conectando pela primeira vez no equipamento

1.1 Instalando e energizando o Equipamento

Por favor, verificar as instruções detalhadas no **Guia de Instalação** do equipamento.

1.2 Conectando via porta Console



Conectando via porta console

O acesso a CLI do equipamento pode ser realizado pela porta Console do equipamento. É necessário conectar um cabo serial e executar um emulador de terminal como, por exemplo, o Hyper Terminal ou outro similar. O programa deve ser configurado com **9600 8N1**.

1.3 Conectando via porta de gerência out-of-band



Conectando via porta Out-of-Band

Outra forma de acessar a CLI do equipamento é através do uso da porta de gerenciamento MGMT. A porta MGMT é uma porta Ethernet dedicada para o gerenciamento do equipamento e não está habilitada a ser utilizada em protocolos de switching (L2) ou roteamento (L3).

Para acessar a CLI é necessário conectar um cabo LAN na porta MGMT e configurar um endereço IP na placa de rede do PC auxiliar. O endereço IP de fábrica do equipamento é o **192.168.0.25/24**. É necessário executar uma aplicação SSH no PC auxiliar para abrir uma sessão com o equipamento.

1.4 Conectando pela primeira vez no equipamento

Para acessar o equipamento via CLI é necessário utilizar o usuário de fábrica **admin** e a senha de fábrica **admin**.

```
login as: admin  
Password: admin
```



Por razões de segurança é altamente recomendado modificar a senha padrão do equipamento.

Consulte o capítulo referente à **Autenticação de Usuários** para verificar como proceder com a alteração das senhas.

Usando a CLI

A maneira mais simples de se utilizar a linha de comando é simplesmente escrevendo o comando e pressionando [Enter].

```
# comando [Enter]
```

Se o comando incluir um parâmetro também devem ser inseridas a palavra-chave e seus argumentos. O argumento especifica como o parâmetro é alterado. Valores incluem números, strings ou endereços, dependendo da palavra-chave. Depois de inserir o comando deve ser pressionado [Enter].

```
# comando palavra-chave argumento [Enter]
```

2 Atualização de Firmware

Os equipamentos da linha DmSwitch possuem duas posições de memória flash para armazenamento de firmware e salva automaticamente a nova versão de firmware na posição não utilizada.



Entre em contato com o Suporte Técnico DATACOM para verificar as imagens de firmware disponíveis para download e instalação de acordo com seu produto e seus requisitos.

Para atualização via CLI será necessário utilizar um PC com um servidor TFTP, SCP ou HTTP instalado a fim de encaminhar o arquivo de firmware para o equipamento.

Para enviar o arquivo de firmware através do **TFTP**, usar o seguinte comando:

```
copy tftp 192.168.0.1 firmware-name.im firmware
```



Caso o arquivo de firmware não esteja na pasta padrão do servidor TFTP, adicione o path no comando.

```
copy tftp 192.168.0.1 /PATH/firmware-name.im firmware
```

Para os equipamentos DM4100 em stacking, DM4004 e DM4008 é necessário enviar o firmware para cada unit de acordo com o modelo da placa/unit.

```
copy tftp 192.168.0.1 firmware-name.im firmware unit <1-9>  
copy tftp 192.168.0.1 firmware-name.im firmware unit range <1-9> <1-9>
```

No caso do DM4004 e DM4008 que possuem **standby MPU**, é necessário atualiza-la utilizando o comando abaixo. Neste caso, o novo firmware já deve ter sido enviado para a MPU ativa. Verifique o FIRMWARE ID antes de executar o comando.

```
show firmware all  
copy firmware <FIRMWARE ID> standby-mpu
```

O firmware será encaminhado para a posição **Startup**. É possível verificar o novo firmware copiado através do seguinte comando:

```
show firmware all
```

Para ativar o firmware que está na posição Startup, é necessário reiniciar o equipamento.

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



Um reboot automático irá ocorrer após o usuário confirmar a ativação.

Após o equipamento reinicializar, verificar que o novo firmware agora está no estado **RS – Running/Startup** usando novamente o comando:

```
show firmware all
```

3 Gerenciamento da Configuração

O equipamento pode ser gerenciado através da CLI com o uso da porta console do equipamento ou por sessões TELNET e SSH.

A CLI suporta os modos de **configuração** e **operacional** que proveem comandos de configuração, monitoramento, hardware e conectividade.

Este capítulo contém as seguintes seções:

- Modo Operacional
- Modo de Configuração
- Configurações Salvas
- Restaurando Configuração
- Exportando os Arquivos
- Restaurando a configuração de fábrica
- Reset de senha

3.1 Modo Operacional

Ao realizar o login no equipamento o usuário automaticamente entrará no modo operacional. Neste modo é possível verificar as informações do equipamento, executar teste de conectividade da rede e outros. Neste modo, porém, não é possível realizar modificações na configuração do equipamento.



Para visualizar a lista dos comandos disponíveis neste modo, digite o comando ?

É possível verificar algumas informações do equipamento no modo operacional através dos seguintes comandos:

Comando	Descrição
show system	Apresenta o modelo do equipamento, número de série, MAC, licenças e outros.
show unit	Apresenta o modelo do equipamento, número de série, firmware e versão de stacking.
show firmware	Apresenta a versão de firmware
show running-config	Apresenta a configuração atual do equipamento
show cpu usage	Apresenta os valores da CPU em uso do equipamento
show cpu memory	Apresenta os valores de memória do equipamento
show uptime	Apresenta o tempo de atividade do equipamento

Comando	Descrição
<code>show users</code>	Apresenta os usuários configurados no equipamento e o nível de acesso.

3.2 Modo de Configuração

Para modificar a configuração é necessário entrar no modo de configuração através do seguinte comando:

```
configure
```

Se o usuário desejar sair do modo de configuração, poderá usar o comando abaixo em qualquer nível hierárquico de configuração ou também apenas digitar **[Ctrl]+[Z]**.

```
end
```

Se o usuário desejar retornar para o nível anterior de configuração, é possível usar o comando abaixo.

```
exit
```

3.3 Configurações Salvas

Para verificar as posições de memórias disponíveis é necessário executar o seguinte comando:

```
show flash
```

É possível selecionar outra posição para ser a *startup* dentre as 10 possíveis. Para isto, é necessário executar o seguinte comando:

```
select startup-config <id>
```

Enquanto o usuário configura o equipamento, esta configuração é diretamente aplicada na *running-config*. Porém, se o equipamento resetar, as modificações serão perdidas. Para salvar a running na memória flash é necessário executar o seguinte comando:

```
copy running-config startup-config
```

3.4 Restaurando Configuração

Se o usuário deseja carregar alguma configuração salva em alguma das 10 posições da memória flash deve usar o seguinte procedimento:

```
copy flash-config <id> running-config
```

3.5 Exportando os Arquivos

O usuário pode exportar uma configuração salva em alguma das posições da memória flash para um servidor SCP ou TFTP. O comando a seguir encaminhará a configuração salva na posição 10 via protocolo TFTP para o servidor 172.1.1.1.

```
copy flash-config 10 tftp 172.1.1.1
```

3.6 Restaurando a Configuração de Fábrica



O procedimento a seguir apagará a configuração e carregará a configuração de fábrica na sua posição. Configurações de rotas e endereços IP serão perdidas.

Para carregar a configuração de fábrica na configuração candidata o usuário deverá executar o comando:

```
copy default-config running-config
```

É possível carregar a configuração de fábrica para outras posições de memória como:

- flash-config <id>
- running-config
- startup-config

3.7 Reset de senha

Os equipamentos Datacom possuem métodos diferentes para reset de senha, abaixo o passo a passo de acordo com cada modelo de equipamento:

DM2104 / DM2106

- Conecte o switch ao computador via serial;
- Ligue/reinicialize o switch;
- Quando solicitado, pressione CTRL+C;
- Será exibido endereço MAC e número serial. Abra um chamado com o Suporte Técnico com estas estas informações. Será gerado o **password**;
- Após receber o password, cole no prompt e pressione [Enter];
- Digite **unsetenv CATL** e pressione [Enter];
- Digite **reset -sysreset -yes** e pressione [Enter]. O equipamento irá reinicializar;
- Quando solicitado, utilize usuário e senha **admin** para fazer login.

DmSwitch3000

- Conecte o switch ao computador via serial;
- Ligue/reinicialize o switch;
- Quando solicitado, pressione CTRL+C;
- A inicialização será interrompida, digite **setenv CATL[Enter]**;
- Salve a configuração, digite **saveenv[Enter]**;
- Para carregar o firmware, digite **boot[Enter]**;
- Quando solicitado, utilize usuário e senha **admin** para fazer login.

DM4000 / DM4100

- Conecte o switch ao computador via serial;
- Ligue/reinicialize o switch;
- Quando solicitado, pressione CTRL+C;
- Digite **printenv[Enter]**, abra um chamado com o Suporte Técnico com estas estas informações. Será gerado o **password**;
- Digite **enable[Enter]**, cole o password e pressione [Enter];
- A inicialização será interrompida, digite **setenv CATL[Enter]**;
- Salve a configuração, digite **saveenv[Enter]**;
- Para carregar o firmware, digite **boot[Enter]**;
- Quando solicitado, utilize usuário e senha **admin** para fazer login.

Após realizar login no equipamento é possível carregar uma configuração salva no equipamento ou carregar a **startup-config** na **running-config** e alterar a senha do usuário local. Após alterar a senha é necessário salvar a **running-config** na **startup-config**.

- `show flash`
- `show flash-config <ID>`
- `copy startup-config running-config`

```
copy flash config <FLASH-ID> running-config
configure
username <USER> password 0 <NEW PASSWORD>
copy running-config startup-config
end
```


4 Gerenciamento do Equipamento

Este capítulo irá guiar o usuário em como proceder com a configuração de gerenciamento equipamento.

- Configurando a Gerência Out-Of-Band
- Configurando a Gerência In-Band
- Configurando o Hostname
- Configurando o Relógio do Sistema
- Configurando o SNTP
- Configurando o Syslog Remoto
- Configurando o SNMP
- Ativando a Licença MPLS

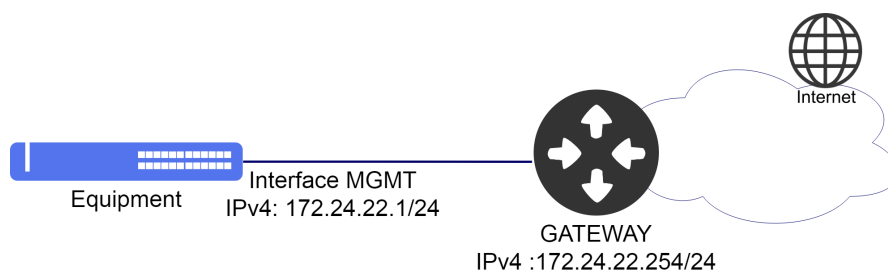
4.1 Configurando a Gerência Out-Of-Band

É possível configurar a gerência out-of-band para manter o acesso ao equipamento mesmo quando a rede de dados está desativada. Se o usuário estiver conectado pela **interface MGMT**, a sessão será desconectada após a confirmação. Para continuar configurando o equipamento pela **interface MGMT**, o usuário deve configurar um endereço IP no seu PC dentro da mesma rede ou conectar pela console.



É possível configurar o gerenciamento do equipamento com endereçamento IPv4 ou IPv6.

A topologia abaixo ilustra um exemplo de como gerenciar o equipamento pela **interface MGMT**.



Exemplo de Gerenciamento Out-of-Band

O procedimento abaixo mostra como configurar a **interface MGMT** com o endereço IPv4 **172.24.22.1/24** e gateway padrão **172.24.22.254/24**.

```
configure
interface mgmt-eth
ip address 172.24.22.1/24
exit
!
ip default-gateway 172.24.22.254
```

4.2 Configurando a Gerência In-Band

É possível configurar a gerência In-band para gerenciar o equipamento através de uma interface também utilizada para tráfego de dados na rede.

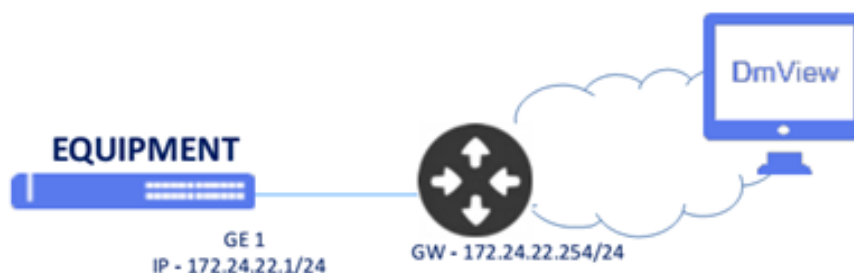


É possível configurar o gerenciamento do equipamento com endereçamento IPv4 ou IPv6.



É possível configurar o gerenciamento do equipamento utilizando endereço IPv4 secundário.

O diagrama abaixo ilustra um exemplo de como gerenciar o equipamento por uma interface In-Band.



Exemplo de Gerenciamento In-Band

O procedimento abaixo demonstra como configurar a **VLAN 10** para gerenciamento In-Band através da interface **ethernet 1/1** com endereço IPv4 **172.24.22.1/24** e gateway padrão **172.24.22.254**.

```
configure
interface vlan 10
name In_Band
ip address 172.24.22.1/24
set-member untagged ethernet 1/1
exit
!
interface ethernet 1/1
description In_Band
switchport native vlan 10
exit
!
ip default-gateway 172.24.22.254
```

4.3 Configurando o Hostname

Para utilizar o nome **DATAKOM-SWITCH-01** para identificar o equipamento, realizar a configuração como abaixo.

```
configure
hostname DATAKOM-SWITCH-01
```

4.4 Configurando o relógio e data do sistema

A configuração abaixo ajusta o relógio do sistema de forma forçada, ou seja, sem nenhuma sincronização. A configuração do relógio e data é importante para visualização de logs e eventos no equipamento.



Recomenda-se fazer uso de uma sincronização centralizada através do protocolo SNTP.

Para configurar a data para **20 de Janeiro de 2017** e o horário para **10 horas, 5 minutos e 30 segundos**, utilizar o procedimento abaixo.

```
clock set 10:05:30 20 01 2019
```

Para alterar o **timezone** para -3, realizar a configuração abaixo.

```
configure
clock timezone BRA -3
```

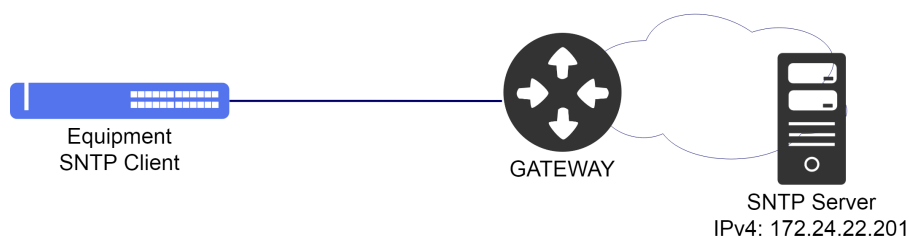
Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show clock
```

4.5 Configurando o SNTP

O SNTP (Simple Network Time Protocol) é uma versão simplificada do NTP (Network Time Protocol) que é utilizado para sincronizar o relógio do sistema com um servidor. Esta configuração é importante para visualização de logs e eventos no equipamento.

O cenário abaixo será usado para demonstrar a configuração do SNTP.



Exemplo de configuração SNTP

Para configurar o equipamento como cliente SNTP e utilizar um servidor SNTP com endereço IPv4 **172.24.22.201** com timezone -3, seguir o procedimento abaixo.

```
configure
ntp client
ntp server 172.24.22.201
clock timezone BRA -3
```

É possível também configurar a autenticação MD5 com o servidor SNTP. O procedimento a seguir apresentará como proceder com esta configuração.

```
configure
sntp client
sntp authenticate
sntp authentication-key 1 md5 SERVER-KEY
sntp server 172.24.22.201 key 1
clock timezone BRA -3
```

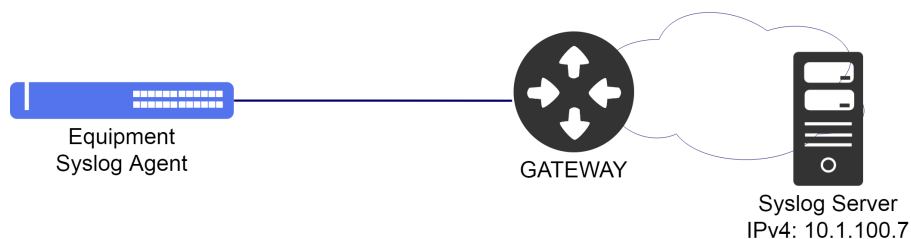
Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade. Caso o usuário esteja no nível de configuração, é necessário utilizar a palavra-chave **do** antes do comando.

```
show sntp
```

4.6 Configurando o Syslog remoto

De acordo com a RFC5424, o protocolo Syslog é usado para transportar mensagens de notificação de eventos. O syslog é usado por dispositivos de rede para enviar mensagens de eventos para um servidor externo, geralmente chamado de Syslog Server. Por exemplo, se uma interface Ethernet for desativada, uma mensagem será enviada para o servidor externo configurado para alertar esta mudança. Esta configuração é importante para visualização de logs e eventos dos equipamentos da rede de forma centralizada.

O cenário abaixo será usado para demonstrar a configuração do Servidor de Syslog Remoto.



Exemplo de configuração do Syslog Remoto

Para utilizar um servidor **syslog remoto** com endereço IPv4 **172.22.1.252**, realizar a configuração abaixo.

```
configure
logging host 172.22.1.252
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade. Caso o usuário esteja no nível de configuração, é necessário utilizar a palavra-chave **do** antes do comando.

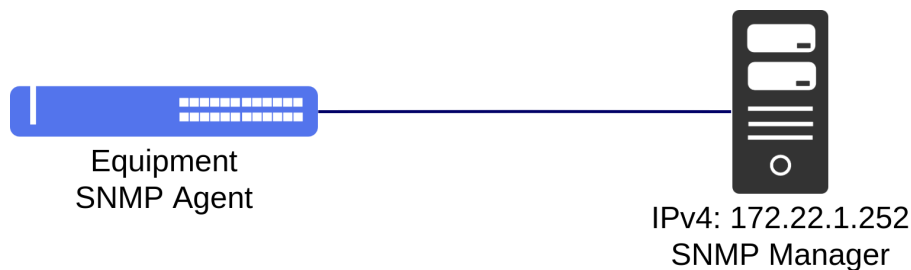
```
show log ram
show log flash
```

4.7 Configurando o SNMP

O SNMP é um protocolo que ajuda os administradores de rede a gerenciar dispositivos de rede e solucionar problemas de rede. O sistema de gerenciamento de rede é baseado em dois elementos principais: gerente e agente. O protocolo SNMP possui três versões:

Versão	Descrição
SNMPv1	Versão original do SNMP, strings das comunidades enviadas em texto simples com segurança fraca.
SNMPv2c	Versão desenvolvida para corrigir alguns dos problemas da v1. No entanto, várias versões foram desenvolvidas, nenhuma abordando verdadeiramente os problemas com v1. A versão v2c é a versão mais usada e melhorou o tratamento de protocolos em relação a versão v1, resultando em operações levemente aprimoradas. No entanto, a segurança ainda é um problema porque utiliza strings de comunidade em texto simples.
SNMPv3	Versão mais recente do SNMP, suportando segurança e autenticação SHA e MD5 completas. Deve ser usado, se possível, especialmente em redes não confiáveis.

O cenário abaixo será usado para demonstrar a configuração do SNMP.



Exemplo de configuração SNMP

Para conectar o equipamento a um servidor SNMPv2 com community **public** com endereço IPv4 **172.22.1.152**, proceda da seguinte forma:

```
configure
ip snmp-server
ip snmp-server community public ro
ip snmp-server user admin rw md5 MD5-KEY des DES-KEY
ip snmp-server host 172.22.1.252 version 2c public
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show ip snmp
show ip snmp traps
```

4.8 Ativando a Licença MPLS

A licença MPLS é necessária para habilitar as configurações de MPLS. Para verificar se a licença está habilitada no seu equipamento utilize o comando **show system**. Para obter a licença entre em contato com o Suporte da DATACOM informando o número de série e o endereço MAC do equipamento. Estas informações podem ser obtidas no comando **show system** conforme abaixo:

```
DmSwitch# show system
Unit 1
Product          DM4001 - ETH24GX L Series
Model:           1.3.6.1.4.1.3709.1.2.83
OID:
Factory
Mainboard ID:    1271882
MAC Address:     00:04:DF:16:9F:EE
System Capabilities HW Available      License Enabled
Bridge:          yes                  yes
Router:          yes                  yes
MPLS:            yes                  no
User configurable
Name:            DM4001
Location:
Contact:
```

Para habilitar a licença, utilize o comando **setf**.

DM4001 / DM4100

```
setf [Enter]
00:04 :DF:00:00:01 0000001 : <KEY MPLS> [Enter]
```

DM4100 em Stacking / DM4004 / DM4008

```
setf [Enter]
Unit: <Unit ID>
00:04 :DF:00:00:02 0000002: <KEY MPLS> [Enter]
```

Standby MPU

```
telnet standby mpu
setf [Enter]
Unit: 1
00:04:DF:00:00:03 0000003: <KEY MPLS> [Enter]
```



Após visualizar a mensagem **Feature will be enabled after reboot**, reinicie o equipamento. Utilize o comando **reboot**.

5 Ferramentas de Conectividade

A linha DmSwitch fornece algumas ferramentas para executar a verificação da conectividade de rede.

Este capítulo contém as seguintes seções:

- Ping e Ping6
- Traceroute e Traceroute6
- SSH Client e Telnet Client

5.1 Ping e Ping6

O comando ping é um método comum para verificar a conectividade do equipamento com os demais ou para testar algum protocolo específico.

Para executar um ping com **endereçamento IPv4**, seguir o procedimento abaixo:

```
ping 5.178.41.1
PING 5.178.41.1 (5.178.41.1) 56(84) bytes of data.
64 bytes from 5.178.41.1: icmp_req=1 ttl=61 time=14.9 ms
64 bytes from 5.178.41.1: icmp_req=2 ttl=61 time=23.8 ms
64 bytes from 5.178.41.1: icmp_req=3 ttl=61 time=10.5 ms
64 bytes from 5.178.41.1: icmp_req=4 ttl=61 time=4.05 ms
64 bytes from 5.178.41.1: icmp_req=5 ttl=61 time=8.19 ms
--- 5.178.41.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 4.057/12.325/23.876/6.769 ms
```

Para executar um ping com **endereçamento IPv6**, seguir o procedimento abaixo:

```
ping6 2400:caca:bebe::2
PING 2400:caca:bebe::2 (2400:caca:bebe::2) 56 data bytes
64 bytes from 2400:caca:bebe::2: icmp_seq=1 time=0.179 ms
64 bytes from 2400:caca:bebe::2: icmp_seq=2 time=0.168 ms
64 bytes from 2400:caca:bebe::2: icmp_seq=3 time=0.149 ms
64 bytes from 2400:caca:bebe::2: icmp_seq=4 time=0.168 ms
64 bytes from 2400:caca:bebe::2: icmp_seq=5 time=0.152 ms
--- 2400:caca:bebe::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.149/0.163/0.179/0.013 ms
```

5.2 Traceroute e Traceroute6

O comando traceroute é um método para realizar o diagnóstico da rede informando a conectividade salto a salto (hop-by-hop) por onde o pacote está passando até o destino final.

Para executar um traceroute com **endereçamento IPv4**, seguir o procedimento abaixo:

```
traceroute 5.178.41.1
traceroute to 5.178.41.1 (5.178.41.1), 30 hops max, 60 byte packets
 1  192.168.48.1  3.963 ms  4.631 ms  3.304 ms
 2  192.168.254.22  5.920 ms  6.512 ms  6.385 ms
 3  192.168.84.22  2.700 ms  2.388 ms  6.050 ms
 4  5.178.41.1  5.390 ms  4.330 ms  14.064 ms
```

Para executar um traceroute com **endereçamento IPv6**, seguir o procedimento abaixo:

```
tracert6 2400:caca:bebe::2
tracert to 2400:caca:bebe::2 (2400:caca:bebe::2), 30 hops max, 80 byte packets
 1  1998::c0a8:3001  4.388 ms  5.105 ms  5.573 ms
 2  2002:c0a8:fe15::22  6.199 ms  5.944 ms  8.071 ms
 3  2001::c0a8:5416  5.657 ms  6.923 ms  8.208 ms
 4  2400:caca:bebe::2  5.646 ms  25.833 ms  26.327 ms
```

5.3 SSH Client e Telnet Client

É possível acessar outros equipamentos através dos protocolos SSH e TELNET a partir de um equipamento DmSwitch.

Para acessar um equipamento com endereço IPv4 **192.168.1.254** através do **SSH**, o usuário deve usar o comando abaixo, especificando o usuário a ser autenticado, neste exemplo, o usuário **admin**:

```
ssh admin@192.168.1.254
```

Para acessar um equipamento com endereço **IPv4 192.168.1.254** através do **TELNET** o usuário deve usar o comando abaixo:

```
telnet 192.168.1.254
```


6 Autenticação de Usuários

Este capítulo contém as seguintes seções:

- Níveis de acesso
- Configurando Usuários Locais
- Configurando TACACS+
- Configurando o RADIUS
- Configurando a ordem de autenticação

6.1 Níveis de acesso

São suportados três níveis de acesso de gerenciamento para usuários (**admin**, **audit** e **normal**), com os quais é determinado o nível de acesso ao equipamento.

Nível	Descrição
admin	Permite exibir e alterar todos os parâmetros do dispositivo. É um acesso completo de leitura e gravação para todo o dispositivo.
1 (audit)	Permite algumas funções de conectividade e status do equipamento. Também permite ao usuário visualizar a configuração do equipamento.
0 (normal)	Permite algumas funções de conectividade e status do equipamento, porém, sem a possibilidade de visualizar a configuração do equipamento.



Por razões de segurança é altamente recomendado modificar a senha padrão do equipamento.

Para alterar a senha padrão do usuário admin, seguir os passos abaixo:

```
configure
username admin password 0 "new_password"
```

6.2 Configurando Usuários Locais

Os próximos passos irão demonstrar como configurar um novo usuário chamado “**joao**” com senha “**joao1234**” e privilégios de administrador “**admin**”.

```
configure
username joao access-level 15
username joao password 0 joao1234
```

Os próximos passos irão demonstrar como deletar o usuário “joao”.

```
configure
no username joao
```

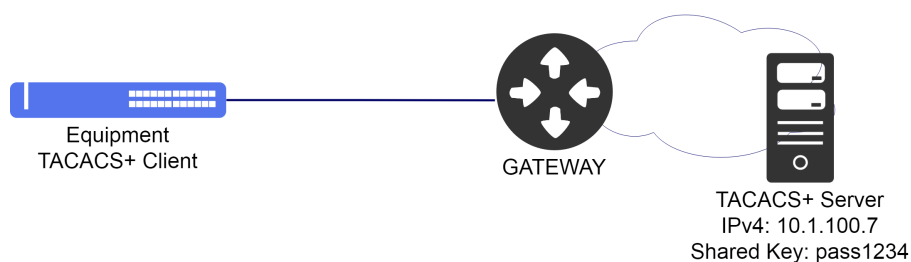
Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show users
```

6.3 Configurando o TACACS+

O TACACS+ (Terminal Access Controller Access-Control System) é um protocolo baseado no modelo AAA que fornece os serviços de autenticação, autorização e accounting de forma segura com criptografia do pacote inteiro. Esta criptografia depende de uma chave secreta compartilhada configurada no equipamento.

O cenário abaixo será usado para demonstrar a configuração do TACACS+.



Exemplo do TACACS+

O procedimento a seguir apresentará como realizar a configuração de um cliente TACACS+ com servidor com endereço IPv4 **10.1.100.7** e senha “**pass1234**”, habilitando autenticação, autorização e accounting.

```
configure
tacacs-server host 1 address 10.1.100.7
tacacs-server host 1 key pass1234
tacacs-server host 1 authentication
tacacs-server host 1 authorization
tacacs-server host 1 accounting
```

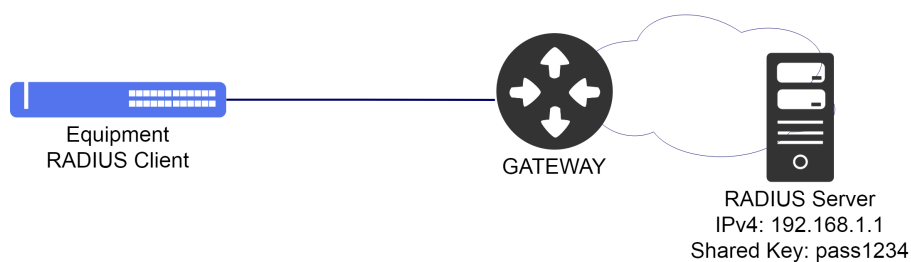
Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show tacacs-server
```

6.4 Configurando o RADIUS

O RADIUS (Remote Authentication Dial In User Service) é um protocolo baseado no modelo AAA que fornece os serviços de autenticação, autorização e contabilidade. A comunicação entre o cliente RADIUS e o servidor RADIUS é segura e uma palavra-chave exclusiva em ambos os sistemas é necessária.

O cenário abaixo será usado para demonstrar a configuração do RADIUS.



Exemplo do RADIUS

Para configurar um servidor **RADIUS** com endereço IPv4 **192.168.1.1** e senha **“pass1234”**, seguir o procedimento abaixo.

```
configure
radius-server host 1 address 192.168.1.1
radius-server host 1 key pass1234
radius-server host 1 authentication
radius-server host 1 accounting
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show radius-server
```

6.5 Configurando a ordem de autenticação

O usuário pode definir a ordem de autenticação entre: **local**, **RADIUS** e **TACACS+**. Quando um usuário tentar efetuar login no sistema, o DmSwitch tentará autenticá-lo seguindo a ordem definida pelo comando **“authentication login”**.

Para utilizar a autenticação na base local em caso de falha de comunicação com o servidor RADIUS, utilizar a configuração abaixo.

```
configure
authentication login radius local
```

7 Interfaces

Este capítulo apresentará exemplos de como configurar as interfaces disponíveis.

- Configurando as Interfaces Ethernet
- Configurando o Link-aggregation (Port-Channel Estático)
- Configurando o Link-aggregation (LACP)
- Configurando o Port Mirroring

7.1 Configurando as Interfaces Ethernet

Para configurar uma interface Ethernet, o usuário deve entrar no nível de configuração da interface.

```
configure
interface ethernet 1/1
```

Para desabilitar administrativamente uma interface ethernet, o usuário deve utilizar o procedimento abaixo.

```
configure
interface ethernet 1/1
shutdown
```

Para reativar uma interface ethernet, o usuário deve utilizar o comando **no shutdown**.

```
configure
interface ethernet 1/1
no shutdown
```

É possível configurar várias interfaces ao mesmo tempo através do **range** de interfaces. O procedimento a seguir exemplifica como desativar as interfaces ethernet 1/1 até a interface ethernet 1/10.

```
configure
interface ethernet range 1/1 1/10
shutdown
```

Abaixo os principais comandos disponíveis para realizar a verificação das interfaces Ethernet.

```
show interfaces link
show interfaces status
show interfaces description
show interfaces switchport
show interfaces counters
```

7.2 Configurando o Link-aggregation (Port-Channel Estático)

A agregação de link **IEEE 802.3ad** permite criar uma interface lógica contendo uma ou mais interfaces físicas. A agregação de vários links ou interfaces físicas cria um único link lógico (LAG) ponto-a-ponto. O LAG possibilita dividir os fluxos entre as interfaces físicas aumentando efetivamente a largura de banda. Outra vantagem da agregação de links é o aumento da

disponibilidade do link de comunicação entre os dois equipamentos, se uma das interfaces físicas falhar, o LAG continuará a transportar o tráfego através das interfaces remanescentes.



Não é suportada agregação entre interfaces com configuração de speed, duplex ou VLANs diferentes.



O modo padrão de balanceamento de tráfego no link-aggregation pelo DmSwitch é o **src-dst-mac**.

Os próximos passos irão demonstrar como configurar o link-aggregation de forma estática usando quatro (4) interfaces Gigabit Ethernet, totalizando uma banda possível de 4Gbps.

```
configure
interface port-channel 1
set-member ethernet range 1/1 1/4
```

Posteriormente, pode-se configurar a interface port-channel de forma tagged ou untagged dentro da VLAN desejada. Abaixo os passos para inserir o port-channel 1 na VLAN 100 na forma tagged.

```
configure
interface vlan 100
set-member tagged port-channel 1
```

7.3 Configurando o Link-aggregation (LACP)

O LACP (Link Aggregation Control Protocol) é um protocolo utilizado para garantir a conectividade fim-a-fim de interfaces agregadas (LAG). Ele detecta e protege a rede contra uma variedade de configurações incorretas, garantindo que os links sejam agregados apenas em um bundle se eles forem configurados e cabeados de forma consistente. O LACP pode ser configurado de dois modos:

- **Modo Ativo (Active):** O dispositivo envia imediatamente mensagens LACP (LACP PDUs) quando a interface é ativada.
- **Modo Passivo (Passive):** Coloca uma interface em um estado de negociação passivo, no qual a interface aguarda o envio das PDUs do remoto para iniciar a negociação e estabelecimento do Link Aggregation.

Se pelo menos um dos lados (endpoints) estiver configurado como ativo, o LAG pode ser formado assumindo uma negociação bem-sucedida dos outros parâmetros.



Não é suportada agregação entre interfaces com configuração de speed, duplex ou VLANs diferentes.

Os próximos passos irão demonstrar como configurar a agregação dinâmica em modo active usando duas (2) interfaces Gigabit Ethernet, totalizando uma banda de 2Gbps ao link agregado.

```
configure
lacp mode active
!
interface port-channel 1
lacp
set-member ethernet 1/1
set-member ethernet 1/2
```

Posteriormente, pode-se configurar a interface port-channel de forma tagged ou untagged dentro da VLAN desejada. Abaixo os passos para inserir o port-channel 1 na VLAN 100 na forma tagged.

```
configure
interface vlan 100
set-member tagged port-channel 1
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show lacp neighbor
show lacp counters
show lacp internal
show lacp sysid
```

7.4 Configurando o Port Mirroring

O Port Mirroring permite que o Switch efetue a cópia dos pacotes de rede de uma porta para outra em um Switch. Esta funcionalidade é normalmente utilizada para espelhar o tráfego, permitindo que o administrador acompanhe o desempenho do Switch e consiga solucionar problemas na rede, colocando um analisador de rede ou analisador de protocolos na porta que está recebendo os dados espelhados.

Os próximos passos irão demonstrar como configurar o port mirroring para espelhar o tráfego de entrada e saída da interface ethernet 1/1 para a interface ethernet 1/2.

```
configure
interface ethernet 1/1
monitor source all
exit
!
monitor
destination 1/2
```



Os equipamentos DM4004 e DM4008, bem como equipamentos operando em stacking suportam apenas o monitor por unit. Ou seja, a interface de destino deve estar na mesma unit da interface source.

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show monitor
```

8 OAM

Este capítulo exibe um grupo de funcionalidades de Operação, Administração e Manutenção (OAM) de rede que fornecem indicação de falha de rede, localização de falhas, informações de desempenho e funções de dados e diagnóstico. Ele contém as seguintes seções:

- [Configuração do RDM](#)

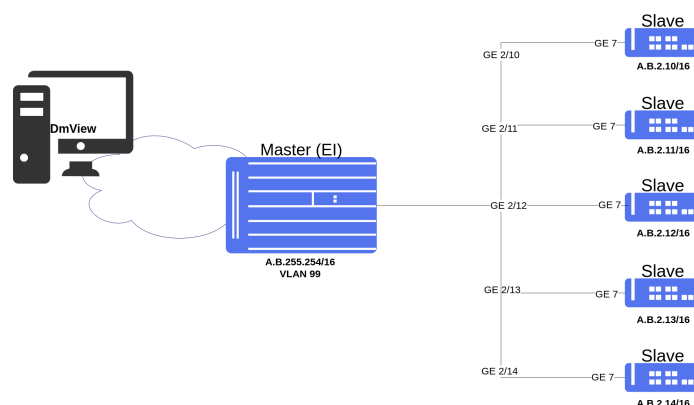
8.1 Configuração do RDM

O protocolo RDM (Remote Devices Management) é um protocolo proprietário Datacom. O objetivo desta feature é fornecer um meio de gerenciar equipamentos remotos da linha DmSwitch. No restante deste capítulo, os equipamentos da linha DM4000 serão referenciados genericamente por equipamento intermediário, ou simplesmente **EI**.

A arquitetura da solução RDM possui os seguintes componentes lógicos:

- **Dispositivos mestre/escravo:** A gerência remota é possível apenas quando um dos dispositivos é mestre e o outro é escravo. O EI é o dispositivo mestre, o remoto é o dispositivo escravo.
- **Comunicação entre EI e remoto:** O EI tem uma VLAN exclusiva para gerência de remotos. Dessa VLAN fazem parte apenas as portas em que haja um remoto conectado; a adição de portas nesta VLAN pode ser feita apenas dinamicamente, à medida que os remotos são detectados. Esta VLAN de Gerência de Remotos possui um IP da rede A.B.255.254/16, sendo A e B configuráveis na CLI pelo usuário. Cada equipamento remoto possui um IP desta mesma rede em uma VLAN (o remoto conectado à porta P da unidade U teria o IP A.B.U.P). Desta forma, existe um canal de comunicação IP entre o EI e o remoto. Vale lembrar que os endereços da rede A.B.0.0/16 não são visíveis externamente ao EI, já que VLAN dos remotos tem como membros unicamente portas nas quais há remotos conectados.

O cenário abaixo ilustra o cenário com RDM mestre/escravo.



Cenário RDM

O gerenciamento remoto é sempre feito pelo IP do mestre, ou seja, o acesso ao remoto da porta U/P é feito pelo IP de gerência do mestre usando uma porta alternativa que pode ser consultada na CLI do mestre.



O protocolo OAM deve estar habilitado, tanto no remoto quanto no EI, nas portas pelas quais os equipamentos estão conectados.

8.1.1 Configurando o RDM como mestre

Suponha que o usuário deseje habilitar o RDM para atuar como dispositivo mestre. O procedimento a seguir apresentará como realizar esta configuração:

```
config
remote-devices enable interface ethernet <unit/port>
remote-devices devices-vlan <vlan id> ip <ip address/mask>
```

8.1.2 Configurando o RDM como escravo

No padrão de fábrica o RDM está habilitado para atuar como escravo na linha EDD. Nos demais equipamentos DmSwitch é necessário habilitar manualmente. Se o dispositivo não estiver configurado com o padrão de fábrica, pode ser necessário habilitar o RDM na interface conectada com o mestre (EI).

Suponha que o usuário queira habilitar o RDM para atuar como dispositivo remoto para ser gerenciado por um equipamento central na rede. O procedimento a seguir apresentará como realizar esta configuração:

```
config
remote-devices enable
interface ethernet <unit/port>
oam
```

Após habilitar as configurações acima o dispositivo será configurado automaticamente, criando a VLAN para gerência e uma rota estática com destino para o dispositivo mestre.

A partir desse momento o dispositivo escravo pode ser acessado via dispositivo mestre ou através de um dos serviços configurados no mestre como Telnet ou SSH, por exemplo.



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o RDM](#).

8.1.3 Comunicação Mestre/Escravo

Quando o EI e o remoto são conectados, e o remoto está plenamente funcional, é possível a partir do EI acessar diretamente o equipamento escravo através de Telnet e SSH.

Para se conectar ao remoto da unidade A e porta B segue o exemplo:


```
telnet remote-device A/B [port][número da porta]
ssh remote-device A/B [user/port][usuário/número da porta] [user/port][usuário/número da porta]
```

Caso não haja algum remoto funcional em A/B, será retornado erro.

8.1.4 Configuração do limite global de pacotes repassados para remotos

A configuração do limite global de pacotes repassados para remotos tem como objetivo proteger a CPU do EI. O range é de 10 a 10000 pacotes por segundo. Em casos de atualização de firmware do remoto, pode ser necessário aumentar o rate-limit para acelerar o processo de download do firmware.

O procedimento a seguir apresentará como realizar esta configuração:

```
config
remote-devices rate-limit <rate-limit>
```

8.1.5 Configuração de serviços disponibilizados no remoto

O usuário pode configurar serviços disponibilizados no remoto. Inicialmente foram reservados 20 serviços e a porta TCP/UDP pode ir de 1 a 1024, pois estas são as portas de serviços conhecidos.

O procedimento a seguir apresentará como realizar esta configuração:

```
config
remote-devices service <service index> tcp | udp <port>
```

8.1.6 Verificando o RDM

Abaixo os principais comandos disponíveis para realizar o Troubleshooting.



Para maiores detalhes sobre as saídas dos comandos, consultar o **Command Reference**.

```
debug rdm
show remote-devices
show remote-devices interface ethernet all
```

9 Switching

- Configurando o aging time da tabela MAC
- Configurando VLAN com interfaces tagged
- Configurando VLAN com interfaces untagged
- Configurando o QinQ
- Configurando VLAN-translate
- Configurando RSTP
- Configurando EAPS

Em uma rede da Camada 2, cada segmento de rede possui seu próprio domínio de colisão e todos os segmentos estão no mesmo domínio de transmissão. Toda transmissão é vista por todos os dispositivos da rede. O padrão 802.1Q permite a criação de VLANs que são usadas para segmentar um único domínio de broadcast para vários domínios de broadcast. O padrão 802.1Q suporta frames marcados (tagged) e não marcados (untagged) por um identificador de 1 a 4094. Alguns benefícios de utilizar VLANs são:

- Separar domínios de broadcast em domínios menores, reduzindo recursos de processamento;
- Agrupar usuário por tráfego interessante;
- Isolar tráfego sensível, proporcionando segurança;
- Trabalhar independentemente da topologia da camada física.

9.1 Configurando o aging time da tabela MAC

Os equipamentos de switching funcionam em camada L2 e realizam o encaminhamento dos frames por meio de endereços MAC. A tabela de endereços MAC armazena os endereços MACs aprendidos pelo dispositivo, associando-os a uma porta de interface.

Os endereços MAC são aprendidos dinamicamente ou estaticamente pelo dispositivo. No modo estático, o usuário salva uma entrada com endereço MAC e porta. Essa entrada persistirá na tabela até que o usuário a remova. No modo dinâmico, o switch recebe um quadro e salva o endereço MAC de origem e a porta de interface na tabela. Este endereço continuará salvo enquanto existir tráfego ou aguardará o tempo de aging para limpar essa entrada na tabela.

Os próximos passos irão demonstrar como configurar o aging time para o valor de 600 segundos. O valor padrão do aging time é 300 segundos.

```
configure
mac-address-table aging-time 600
```

Abaixo os principais comandos disponíveis para realizar a verificação dos MACs aprendidos pelo equipamento.

```
show mac-address-table
show mac-address-table aging-time
```

9.2 Configurando VLAN com interfaces tagged

O modo **tagged** é utilizado nas interfaces que realizam o encaminhamento e recebimento de tráfego com marcação de VLAN ID (802.1Q).

Os próximos passos irão demonstrar como configurar a VLAN 200 para encaminhar o tráfego de dados entre as interfaces Gigabit Ethernet 1/1 e Gigabit Ethernet 1/2 usando modo tagged.

```
configure
interface vlan 200
set-member tagged ethernet 1/1
set-member tagged ethernet 1/2
```

É possível também o usuário configurar várias VLANs através de um range e inserir as interfaces desejadas. O procedimento abaixo exemplifica a configuração de um range de VLANs do ID 1500 até o ID 2000 com a interface ethernet 1/1 em modo tagged.

```
configure
interface vlan range 1500 2000
set-member tagged ethernet 1/1
```

Abaixo os principais comandos disponíveis para realizar a verificação das VLANs.

```
show vlan
show vlan table
show vlan id <VLAN_ID>
```

9.3 Configurando VLAN com interfaces untagged

O modo **untagged** é utilizado nas interfaces que realizam o encaminhamento e recebimento de tráfego que não possuem a marcação de VLAN ID (802.1q). Este modo é utilizado principalmente nas interfaces conectadas a computadores, servidores, impressoras, etc.



Para tráfego **untagged** é necessário configurar uma native-vlan nas interfaces e removê-las da VLAN 1.

Os próximos passos irão demonstrar como configurar a VLAN 200 para tráfego entre as interfaces Ethernet 1/1 e Ethernet 1/2 usando modo untagged.

```
configure
interface vlan 200
set-member untagged ethernet 1/1
set-member untagged ethernet 1/2
!
interface ethernet 1/1
switchport native vlan 200
!
interface ethernet 1/2
switchport native vlan 200
```

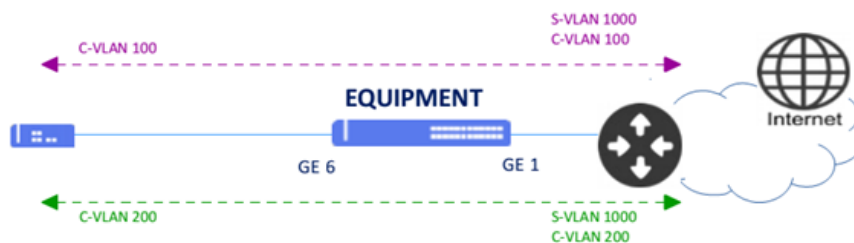
Abaixo os principais comandos disponíveis para realizar a verificação das VLANs.

```
show vlan
show vlan table
show vlan id <VLAN_ID>
```

9.4 Configurando o QinQ

O **QinQ** é uma funcionalidade L2 também conhecida por **tunneling QinQ**, **802.1q tunnel**, **VLAN Stacking** ou **double-tag**. Com esta funcionalidade, um provedor de serviços pode atribuir diferentes VLANs de serviço (S-VLANs) a um determinado tipo de tráfego de clientes diferentes, ou até mesmo uma única VLAN para todos os clientes. Isto permite uma separação entre o tráfego de cada cliente na rede do provedor de serviços. As VLANs do cliente são então transportadas de forma transparente dentro da rede do provedor de serviços.

O cenário abaixo será usado para demonstrar a configuração do QinQ.



Exemplo de cenário com QinQ

Os próximos passos irão demonstrar como configurar o QinQ para transportar todas as VLANs do cliente conectada na interface ethernet 1/6. Ambas as VLANs serão transportadas através da rede da operadora utilizando a **VLAN (S-VLAN) 1000**.

```
configure
vlan qinq
interface vlan 1000
set-member tagged ethernet 1/1
set-member untagged ethernet 1/6
!
interface ethernet 1/6
switchport native vlan 1000
switchport qinq external
```

Abaixo os principais comandos disponíveis para realizar a verificação do QinQ.

```
show qinq
```

9.5 Configurando VLAN-translate

O VLAN-Translate realiza a substituição de uma determinada VLAN para outra VLAN no sentido de saída (out) ou no sentido de entrada (in) do tráfego.

Os próximos passos irão demonstrar como configurar o VLAN Translate para traduzir a VLAN 10 para a VLAN 40 na **entrada (in)** da interface ethernet 1/1.

```

configure
vlan qinq
!
interface vlan 40
set-member tagged ethernet 1/2
!
vlan-translate ingress-table replace ethernet 1/1 source-vlan 10 new-vlan 40
!
interface ethernet 1/1
switchport qinq external
switchport vlan-translate ingress

```

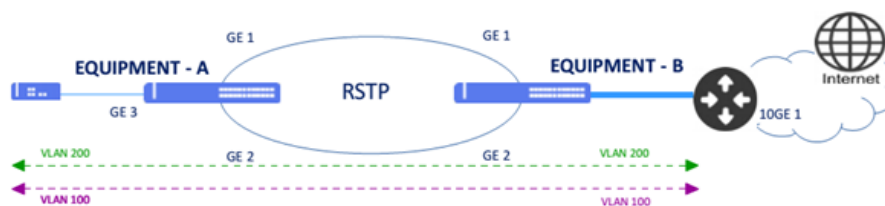
Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show vlan-translate table
```

9.6 Configurando RSTP

O protocolo **RSTP** (Rapid Spanning Tree Protocol) definido pela norma **IEEE 802.1w** é utilizado para fornecer um caminho único na rede, eliminando loops entre os equipamentos.

O cenário abaixo será usado para demonstrar a configuração do RSTP.



Exemplo de cenário com RSTP

Os seguintes parâmetros serão utilizados nas configurações:

- **EQUIPMENT - A:** VLAN ID 100 a 200 para tráfego com a interface ethernet 1/3 como interface de acesso e prioridade 8192.
- **EQUIPMENT - B:** VLAN ID 100 a 200 para tráfego com a interface ethernet 1/3 como interface de acesso e prioridade 32768

EQUIPMENT - A

```

configure
interface vlan range 100 200
set-member tagged ethernet 1/1
set-member tagged ethernet 1/2
set-member tagged ethernet 1/3
!
!
vlan-group 1
vlan-group 1 vlan all
!
spanning-tree 1
spanning-tree 1 bpdu-tag untagged
spanning-tree 1 vlan-group 1

```

EQUIPMENT - B

```

configure
interface vlan range 100 200
  set-member tagged ethernet 1/1
  set-member tagged ethernet 1/2
  set-member tagged ethernet 1/3
!
!
vlan-group 1
vlan-group 1 vlan all
!
spanning-tree 1
spanning-tree 1 bpdu-tag untagged
spanning-tree 1 vlan-group 1

```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```

show spanning-tree
show spanning-tree configuration
show spanning-tree interface ethernet <interface>

```

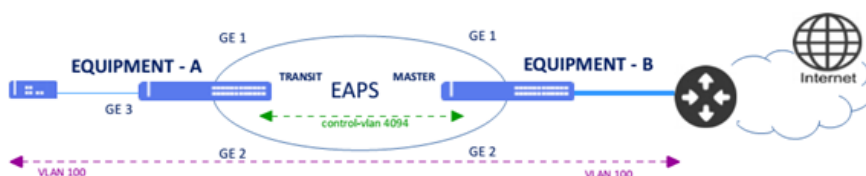
9.7 Configurando EAPS

O protocolo **EAPS** (Ethernet Automatic Protection Switching) é utilizado para fornecer um caminho único na rede e eliminando loops entre os equipamentos. Também fornece uma convergência mais rápida em relação ao protocolo RSTP.



O protocolo **EAPS** funciona adequadamente apenas em topologias em anel.

O cenário abaixo será usado para demonstrar a configuração do EAPS.



Exemplo de cenário com EAPS



Os protocolos xSTP e ERPS deverão ser desabilitados nas interfaces do EAPS.

Os seguintes parâmetros serão utilizados nas configurações:

- **EQUIPMENT - A:** VLAN 1500 a 1600 para tráfego com a interface ethernet 1/3 como interface de acesso e a VLAN100 para VLAN de controle do EAPS em modo Transit através das interfaces ethernet 1/1 e 1/2.
- **EQUIPMENT - B:** VLAN 1500 a 1600 para tráfego com a interface ethernet 1/3 como interface de acesso e a VLAN100 para VLAN de controle do EAPS em modo Master através das interfaces ethernet 1/1 e 1/2.

EQUIPMENT - A

```
configure
interface vlan 100
set-member tagged ethernet 1/1
set-member tagged ethernet 1/2
!
interface vlan range 1500 1600
set-member tagged ethernet 1/1
set-member tagged ethernet 1/2
set-member tagged ethernet 1/3
!
!
vlan-group 0
vlan-group 0 vlan range 1500 1600
!
eaps 0
eaps 0 port primary ethernet 1/1
eaps 0 port secondary ethernet 1/2
eaps 0 control-vlan id 100
eaps 0 protected-vlans vlan-group 0
```

EQUIPMENT - B

```
configure
interface vlan 100
set-member tagged ethernet 1/1
set-member tagged ethernet 1/2
!
interface vlan range 1500 1600
set-member tagged ethernet 1/1
set-member tagged ethernet 1/2
set-member tagged ethernet 1/3
!
!
vlan-group 0
vlan-group 0 vlan range 1500 1600
!
eaps 0
eaps 0 mode master
eaps 0 port primary ethernet 1/1
eaps 0 port secondary ethernet 1/2
eaps 0 control-vlan id 100
eaps 0 protected-vlans vlan-group 0
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show eaps
show eaps detail
```

10 Roteamento

- Configurando Roteamento Estático
- Configurando Roteamento Entre VLANs
- Configurando OSPFv2
- Configurando BGP IPv4

O roteamento é o processo de encaminhar pacotes ao seu destino usando endereços de rede. O roteamento é executado por dispositivos capazes de trocar informações necessárias para criar tabelas contendo informações de caminho para chegar a um destino, usando protocolos específicos ou entradas atribuídas manualmente.

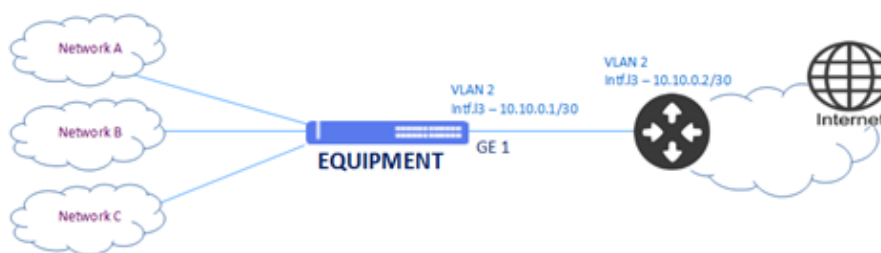
Os protocolos de roteamento dinâmico, como o OSPF, reúnem as informações necessárias dos dispositivos vizinhos para criar sua tabela de roteamento, usada para determinar para onde o tráfego será enviado.

Como alternativas aos métodos dinâmicos, existem rotas estáticas. As rotas estáticas são recomendadas em roteadores que possuem poucas redes e menos caminhos para o destino.

As informações recebidas através dos protocolos de roteamento são adicionadas em uma tabela chamada RIB (Routing Information Base) que é a base para o cálculo da definição do melhor caminho. O resultado do cálculo da rota é a FIB (Forwarding Information Base) que contém as informações que os dispositivos utilizam para rotear o tráfego.

10.1 Configurando Roteamento Estático

O roteamento estático tem por objetivo encaminhar pacotes entre redes distintas com a configuração das rotas de forma manual pelos administradores de rede. O cenário abaixo será usado para demonstrar a configuração do roteamento estático.



Exemplo de cenário com roteamento estático

Para que todo o tráfego seja encaminhado através da interface L3 (VLAN 2) com endereço IPv4 **10.10.0.1/30**, deve ser configurada uma rota default. Os próximos passos irão mostrar como realizar estas configurações.

```
configure
ip routing
interface vlan 2
set-member untagged ethernet 1/1
ip address 10.10.0.1/30
!
interface ethernet 1/1
switchport native vlan 2
!
ip default-gateway 10.10.0.2/30
```


Abaixo os principais comandos disponíveis para realizar a verificação do roteamento estático.

```
show ip route
show ip route static
show ip interface
show ip default-gateway
```

10.2 Configurando Roteamento Entre VLANs

Por padrão, VLANs diferentes não se comunicam, pois estão em domínios de broadcast exclusivos. Para que a comunicação entre duas VLANs seja realizada, é necessário utilizar um roteador ou uma forma de roteamento no próprio equipamento. O roteamento entre VLANs permite esta comunicação através da configuração de interfaces L3 associadas às VLANs desejadas. A rede associada à interface L3 é inserida na tabela de roteamento e pode ser acessada por outras redes.

O cenário abaixo será usado para demonstrar a configuração do roteamento entre VLANs.



Exemplo de cenário com roteamento entre VLANs

Para configurar o roteamento entre a VLAN 100, que possui o endereço 192.168.100.1/24, e a VLAN 200, que possui o endereço 192.168.200.1/24, seguis os passos abaixo.

```
configure
ip routing
interface vlan 100
ip address 192.168.100.1/24
set-member untagged ethernet 1/11
!
interface vlan 200
ip address 192.168.200.1/24
set-member untagged ethernet 1/12
!
interface ethernet 1/11
switchport native vlan 100
!
interface ethernet 1/12
switchport native vlan 200
```

Abaixo os principais comandos disponíveis para realizar a verificação do roteamento estático.

```
show ip route
show ip route static
show ip interface
```

10.3 Configurando OSPFv2

O OSPFv2 (Open Shortest Path First version 2) é o Internal Gateway Protocol descrito pela RFC 2328 (versão 2) para roteamento de endereços IPv4. Este protocolo é utilizado dentro de um mesmo AS (Autonomous System), justificando a

sua denominação de Internal. É baseado no algoritmo de Dijkstra, que calcula o caminho mais curto para cada destino com base nos custos de cada link.

O cenário abaixo será usado para demonstrar a configuração do OSPFv2.



Exemplo de cenário com configuração básica de OSPFv2

Para configurar uma sessão OSPF na área 0, com network-type do tipo ponto-a-ponto, seguir as configurações abaixo.

- **EQUIPMENT - A:** Interface L3 na VLAN 1000 com endereço IPv4 192.168.10.1/30 e interface loopback com IPv4 10.10.10.10/32 sendo utilizada como router-id no OSPFv2 na área 0.
- **EQUIPMENT - B:** Interface L3 na VLAN 1000 com endereço IPv4 192.168.10.2/30 e interface loopback com IPv4 20.20.20.20/32 sendo utilizada como router-id no OSPFv2 na área 0.



Recomenda-se usar a interface **loopback** ao invés das interfaces físicas devido à estabilidade, pois estão sempre ativas.

EQUIPMENT - A

```
config
ip routing
interface vlan 1000
ip address 192.168.10.1/30
set-member untagged ethernet 1/1
exit
!
interface ethernet 1/1
switchport native vlan 1000
exit
!
interface loopback 0
ip address 10.10.10.10/32
exit
!
router ospf
router-id 10.10.10.10
network 10.10.10.10/32 area 0
network 192.168.10.0/30 area 0
log-adjacency-changes
```

EQUIPMENT - B

```
config
ip routing
interface vlan 1000
ip address 192.168.10.2/30
set-member untagged ethernet 1/1
exit
!
interface ethernet 1/1
switchport native vlan 1000
exit
```

```

!
interface loopback 0
 ip address 20.20.20.20/32
 exit
!
router ospf
 router-id 20.20.20.20
 network 20.20.20.20/32 area 0
 network 192.168.10.0/30 area 0
 log-adjacency-changes

```

Abaixo os principais comandos disponíveis para realizar a verificação do OSPFv2.

```

show ip ospf
show ip ospf neighbor
show ip ospf database

```

10.4 Configurando BGP IPv4

O protocolo BGP (Border Gateway Protocol) é o protocolo usado para a troca de informações de roteamento entre AS (autonomous-system) na Internet. Ao estabelecer uma vizinhança com um AS diferente, o BGP é chamado conceitualmente de **eBGP** (external BGP) enquanto que, quando a vizinhança é estabelecida entre roteadores do mesmo AS, o BGP é chamado conceitualmente de **iBGP** (internal BGP).

O cenário abaixo será usado para demonstrar a configuração do protocolo BGP com endereçamento IPv4 em diferentes AS, ou seja, eBGP.



Exemplo de cenário com configuração básica do protocolo BGP IPv4

Abaixo estão os parâmetros utilizados nas configurações apresentadas a seguir.

- **EQUIPMENT - A:** Interface L3 na VLAN 2000 com endereço IPv4 192.168.20.1/30 e interface loopback com IPv4 10.10.10.10/32 sendo utilizada como router-id no BGP com AS local 20000 e AS remoto 40000.
- **EQUIPMENT - B:** Interface L3 na VLAN 2000 com endereço IPv4 192.168.20.2/30 e interface loopback com IPv4 20.20.20.20/32 sendo utilizada como router-id no BGP com AS local 40000 e AS remoto 20000.



Recomenda-se usar o endereço da interface loopback ao invés das interfaces físicas na configuração da vizinhança iBGP. Já para o eBGP é, necessário utilizar os endereços das interfaces físicas ao invés da loopback.

EQUIPMENT - A

```
configure
ip routing
interface vlan 2000
 ip address 192.168.10.1/30
 set-member untagged ethernet 1/1
!
interface ethernet 1/1
 switchport native vlan 2000
!
interface loopback 0
 ip address 10.10.10.10/32
!
router bgp 20000
 bgp graceful-restart
 bgp router-id 10.10.10.10
 neighbor 192.168.10.2 remote-as 40000
 neighbor 192.168.10.2 ebgp-multihop 2
 neighbor 192.168.10.2 local-address 192.168.10.1
 neighbor 192.168.10.2 soft-reconfiguration inbound
```

EQUIPMENT - B

```
configure
ip routing
interface vlan 2000
 ip address 192.168.10.2/30
 set-member untagged ethernet 1/1
!
interface ethernet 1/1
 switchport native vlan 2000
!
interface loopback 0
 ip address 20.20.20.20/32
!
router bgp 40000
 bgp graceful-restart
 bgp router-id 20.20.20.20
 neighbor 192.168.10.1 remote-as 20000
 neighbor 192.168.10.1 ebgp-multihop 2
 neighbor 192.168.10.1 local-address 192.168.10.2
 neighbor 192.168.10.1 soft-reconfiguration inbound
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show ip bgp
show ip bgp neighbor
show ip bgp summary
show ip route bgp
```

11 MPLS

- Configurando uma L2VPN VPWS Port-Based
- Configurando uma L2VPN VPWS VLAN-Based
- Configurando uma L2VPN VPLS VLAN-Based
- Configurando uma L3VPN

O MPLS (Multi-Protocol Label Switching) é definido pela RFC 3031 e é baseada no encaminhamento de pacotes baseada em rótulos ou labels. O MPLS fornece uma maior velocidade no transporte dos pacotes em roteadores disponibilizando também várias funcionalidades de controle, engenharia de tráfego, redes privadas virtuais (VPNs) e qualidade de serviço a fim de aumentar a eficiência da rede.

11.1 Configurando uma L2VPN VPWS Port-Based

O **VPWS** (Virtual Private Wire Service) permite a emulação de serviços Ethernet ponto-a-ponto em uma rede MPLS. Os provedores têm a opção de oferecer este serviço baseado em porta ou VLAN. O serviço VPWS baseado em porta fornece uma interface ethernet exclusiva para um circuito L2.



Com L2VPN Port Based não é possível concentrar diversas VPNs em um único link. Portanto, é necessária uma interface exclusiva para cada VPN.

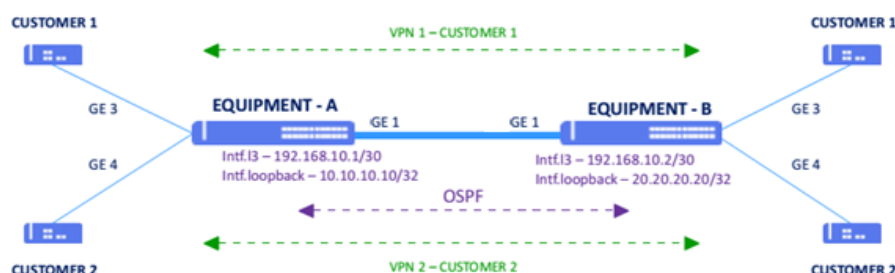


Para configuração de L2VPNs, é necessário configurar o protocolo LDP e um protocolo de roteamento IGP, como o OSPF, por exemplo.



É importante que a MTU configurada na PW para sinalização LDP seja igual entre os dois equipamentos envolvidos na VPN. Caso não seja especificado o valor da PW MTU, o valor considerado será o especificado na AC (access-interface) que por padrão utiliza 9198 Bytes.

O cenário abaixo será usado para demonstrar a configuração de duas L2VPNs Port Based com VPWS.



Exemplo de cenário com L2VPN VPWS port-based

Os próximos passos irão mostrar como configurar duas VPNs do tipo VPWS port-based entre dois equipamentos.

- **EQUIPMENT - A:** Interface VLAN 1000 com endereço IPv4 192.168.10.1/30 e interface loopback com IPv4 10.10.10.10/32 sendo utilizada como router-id no OSPFv2 na área 0 e como lsr-id no LDP. VPN1 com pw-id 100 e interface gigabit 1//3 como interface de acesso. VPN2 com pw-id 200 e interface gigabit 1//4 como interface de acesso.
- **EQUIPMENT - B:** Interface VLAN 1000 com endereço IPv4 192.168.10.2/30 e interface loopback com IPv4 20.20.20.20/32 sendo utilizada como router-id no OSPFv2 na área 0 e como lsr-id no LDP. VPN1 com pw-id 100 e interface gigabit 1//3 como interface de acesso. VPN2 com pw-id 200 e interface gigabit 1//4 como interface de acesso.

EQUIPMENT - A

```

config
ip routing
!
interface vlan 100
 name VPN-1
 set-member untagged ethernet 1/3
!
interface vlan 200
 name VPN-2
 set-member untagged ethernet 1/4
!
interface vlan 1000
 ip address 192.168.10.1/30
 set-member untagged ethernet 1/1
 ldp enable
!
!
interface ethernet 1/1
 switchport native vlan 1000
!
interface ethernet 1/3
 switchport native vlan 100
!
interface ethernet 1/4
 switchport native vlan 200
!
interface loopback 0
 ip address 10.10.10.10/32
 mpls enable
!
!
router ospf
 router-id 10.10.10.10
 network 10.10.10.10/32 area 0
 network 192.168.10.0/30 area 0
 log-adjacency-changes
!
mpls ldp graceful-restart
!
mpls ldp neighbor 20.20.20.1
!
mpls vpws
 vpn 1
  name VPWS-VPN-1
  xconnect vlan 100 vc-type ethernet
  neighbor 20.20.20.1 pwid 100 mpls-type non-te
  no shutdown
 vpn 2
  name VPWS-VPN-2
  xconnect vlan 200 vc-type ethernet
  neighbor 20.20.20.1 pwid 200 mpls-type non-te
  no shutdown

```

EQUIPMENT - B

```

config
ip routing
!
interface vlan 100
 name VPN-1
 set-member untagged ethernet 1/3
!
interface vlan 200
 name VPN-2
 set-member untagged ethernet 1/4
!

```

```
interface vlan 1000
ip address 192.168.10.2/30
set-member untagged ethernet 1/1
ldp enable
!
interface ethernet 1/1
switchport native vlan 1000
!
interface ethernet 1/3
switchport native vlan 100
!
interface ethernet 1/4
switchport native vlan 200
!
interface loopback 0
ip address 20.20.20.20/32
mpls enable
!
router ospf
router-id 20.20.20.20
network 20.20.20.20/32 area 0
network 192.168.10.0/30 area 0
log-adjacency-changes
!
mpls ldp graceful-restart
!
mpls ldp neighbor 10.10.10.1
!
mpls vpws
vpn 1
name VPWS-VPN-1
xconnect vlan 100 vc-type ethernet
neighbor 10.10.10.1 pwid 100 mplstype non-te
no shutdown
vpn 2
name VPWS-VPN-2
xconnect vlan 200 vc-type ethernet
neighbor 10.10.10.1 pwid 200 mplstype non-te
no shutdown
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show mpls l2vpn
show mpls l2vpn summary
show mpls l2vpn detail
show mpls l2vpn counters
```

11.2 Configurando uma L2VPN VPWS VLAN-Based

O **VPWS** (Virtual Private Wire Service) permite a emulação de serviços Ethernet ponto-a-ponto em uma rede MPLS. Os provedores têm a opção de oferecer este serviço baseado em porta ou VLAN. O serviço VPWS baseado em VLAN fornece a possibilidade que vários circuitos L2 de clientes sejam provisionados na mesma interface Ethernet.



Com L2VPN VLAN Based é possível concentrar diversas VPNs em um único link.

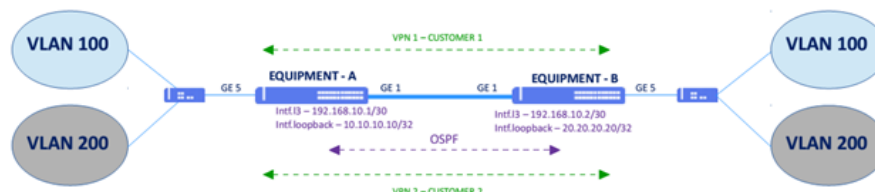


Para configuração de L2VPNs, é necessário configurar o protocolo LDP e um protocolo de roteamento IGP, como o OSPF, por exemplo.



É importante que a MTU configurada na PW para sinalização LDP seja igual entre os dois equipamentos envolvidos na VPN. Caso não seja especificado o valor da PW MTU, o valor considerado será o especificado na AC (access-interface) que por padrão utiliza 9198 Bytes.

O cenário abaixo será usado para demonstrar a configuração de duas L2VPNs VLAN Based com VPWS



Exemplo de cenário com L2VPN VPWS VLAN-based

Os próximos passos irão mostrar como configurar duas VPNs do tipo VPWS VLAN-based entre dois equipamentos.

- **EQUIPMENT - A:** Interface VLAN 1000 com endereço IPv4 192.168.10.1/30 e interface loopback com IPv4 10.10.10.10/32 sendo utilizada como router-id no OSPFv2 na área 0 e como lsr-id no LDP. VPN1 com pw-id 100 e VLAN 100. VPN2 com pw-id 200 e VLAN 200.
- **EQUIPMENT - B:** Interface VLAN 1000 com endereço IPv4 192.168.10.2/30 e interface loopback com IPv4 20.20.20.20/32 sendo utilizada como router-id no OSPFv2 na área 0 e como lsr-id no LDP. VPN1 com pw-id 10 e interface gigabit 1/3 como interface de acesso. VPN1 com pw-id 100 e VLAN 100. VPN2 com pw-id 200 e VLAN 200.

EQUIPMENT - A

```
config
ip routing
interface vlan 100
set-member tagged ethernet 1/5
!
interface vlan 200
set-member tagged ethernet 1/5
!
interface vlan 1000
ip address 192.168.10.1/30
set-member untagged ethernet 1/1
ldp enable
!
!
interface ethernet 1/1
switchport native vlan 1000
!
!
interface loopback 0
ip address 10.10.10.10/32
mpls enable
!
!
router ospf
router-id 10.10.10.10
network 10.10.10.10/32 area 0
network 192.168.10.0/30 area 0
log-adjacency-changes
!
mpls ldp graceful-restart
!
mpls ldp neighbor 20.20.20.1
!
mpls vpws
vpn 1
name VPWS-VPN1
xconnect vlan 100 vc-type vlan
neighbor 20.20.20.1 pwid 100 mpls-type non-te
no shutdown
vpn 2
```



```
name VPWS-VPN1
xconnect vlan 200 vc-type vlan
neighbor 20.20.20.1 pwid 200 mplstype non-te
no shutdown
```

EQUIPMENT - B

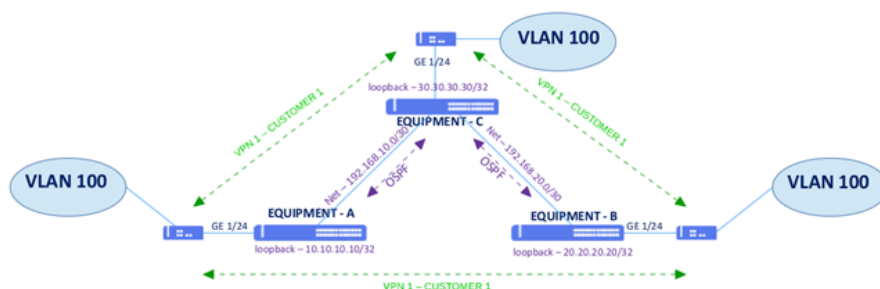
```
config
ip routing
interface vlan 100
set-member tagged ethernet 1/5
!
interface vlan 200
set-member tagged ethernet 1/5
!
interface vlan 1000
ip address 192.168.10.2/30
set-member untagged ethernet 1/1
ldp enable
!
!
interface ethernet 1/1
switchport native vlan 1000
!
!
interface loopback 0
ip address 20.20.20.20/32
mpls enable
!
!
router ospf
router-id 20.20.20.20
network 20.20.20.20/32 area 0
network 192.168.10.0/30 area 0
log-adjacency-changes
!
mpls ldp graceful-restart
!
mpls ldp neighbor 10.10.10.1
!
mpls vpws
vpn 1
name VPWS-VPN1
xconnect vlan 1000 vc-type vlan
neighbor 10.10.10.1 pwid 100 mplstype non-te
no shutdown
vpn 2
name VPWS-VPN2
xconnect vlan 200 vc-type vlan
neighbor 10.10.10.1 pwid 200 mplstype non-te
no shutdown
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show mpls l2vpn
show mpls l2vpn summary
show mpls l2vpn detail
show mpls l2vpn counters
```

11.3 Configurando uma L2VPN VPLS VLAN-Based

VPLS (Virtual Private LAN Service) é um serviço L2VPN que utiliza MPLS para interligar redes em diferentes sites através de uma rede IP/MPLS, fazendo com que os sites fiquem no mesmo L2. Realiza a emulação de serviços Ethernet ponto-multiponto permitindo que sites geograficamente isolados sejam conectados por meio de uma MAN (Metropolitan Area Network) ou de uma WAN (Wide Area Network). Todos os serviços em uma VPLS estão no mesmo domínio de broadcast.



Exemplo de cenário com L2VPN VPLS VLAN-based

Para conectar os sites A, B e C através de uma VPLS VLAN-based, realizar as configurações a seguir. Como se trata de uma VPLS VLAN-based, somente a VLAN configurada será encaminhada através da VPN.

EQUIPMENT - A

```

ip routing
!
router ospf
  router-id 10.10.10.10
  network 10.10.10.10/32 area 0
  network 192.168.10.0/30 area 0
  log-adjacency-changes
!
interface vlan 100
  set-member tagged ethernet 1/24
!
interface vlan 1000
  ip address 192.168.10.1/30
  set-member untagged ethernet 1/1
  ldp enable
!
interface ethernet 1/1
  switchport native vlan 1000
!
interface loopback 0
  ip address 10.10.10.10/32
  mpls enable
!
mpls ldp graceful-restart
!
mpls ldp neighbor 20.20.20.20
!
mpls vpls mac-address limit global 1024
!
mpls vpls
  vpn 1
    name VPN-DATACOM
    xconnect vlan 100 vc-type vlan
    neighbor 20.20.20.20 pwid 100 mplstype non-te
      no shutdown
    neighbor 30.30.30.30 pwid 100 mplstype non-te
      no shutdown
!

```

EQUIPMENT - B

```
ip routing
!
router ospf
router-id 20.20.20.20
network 20.20.20.20/32 area 0
network 192.168.20.0/30 area 0
log-adjacency-changes
!
interface vlan 100
set-member tagged ethernet 1/24
!
interface vlan 2000
ip address 192.168.20.1/30
set-member untagged ethernet 1/1
ldp enable
!
```

```

interface ethernet 1/1
  switchport native vlan 2000
!
interface loopback 0
  ip address 20.20.20.20/32
  mpls enable
!
mpls ldp graceful-restart
!
mpls ldp neighbor 10.10.10.10
!
mpls vpls mac-address limit global 1024
!
mpls vpls
  vpn 1
    name VPN-DATACOM
    xconnect vlan 100 vc-type vlan
    neighbor 10.10.10.10 pwid 100 mplstype non-te
    no shutdown
    neighbor 30.30.30.30 pwid 100 mplstype non-te
    no shutdown
!

```

EQUIPMENT - C

```

ip routing
!
router ospf
  router-id 30.30.30.30
  network 30.30.30.30/32 area 0
  network 192.168.30.0/30 area 0
  network 192.168.20.0/30 area 0
  network 192.168.10.0/30 area 0
  log-adjacency-changes
!
interface vlan 100
  set-member tagged ethernet 1/24
!
interface vlan 1000
  ip address 192.168.10.2/30
  set-member untagged ethernet 1/4
  ldp enable
!
interface vlan 2000
  ip address 192.168.20.2/30
  set-member untagged ethernet 1/3
  ldp enable
!
interface ethernet 1/3
  switchport native vlan 2000
!
interface ethernet 1/4
  switchport native vlan 1000
!
interface loopback 0
  ip address 30.30.30.30/32
  mpls enable
!
mpls ldp graceful-restart
!
mpls ldp neighbor 10.10.10.10
mpls ldp neighbor 20.20.20.20
!
mpls vpls mac-address limit global 1024
!
mpls vpls
  vpn 1
    name VPN-DATACOM
    xconnect vlan 100 vc-type vlan
    neighbor 10.10.10.10 pwid 100 mplstype non-te
    no shutdown
    neighbor 20.20.20.20 pwid 100 mplstype non-te
    no shutdown
!

```

Abaixo os principais comandos disponíveis para realizar a verificação das L2VPNs VPLS.

```

show mpls l2vpn
show mpls l2vpn summary
show mpls l2vpn detail
show mpls l2vpn counters

```

11.4 Configurando uma L3VPN

Enquanto uma L2VPN fornece um serviço L2 transparente ao usuário, em uma L3VPN o roteamento é realizado pela operadora. O encaminhamento de pacotes é feito através de labels do MPLS e a troca de rotas e labels é realizada através do BGP.

Cada rota é identificada por um route-distinguisher (RD), que deve ser único para cada cliente, permitindo existir overlapping de endereços IP entre diferentes clientes. As rotas também são marcadas com communities BGP chamadas route-targets, que são utilizados para definir em quais VPNs estas rotas serão instaladas.

Na topologia a seguir, serão configurados dois switches PE (EQUIPMENT A e EQUIPMENT B) ligados a três CEs.

Loopbacks:

- **EQUIPMENT - A** – 1.1.1.1/32
- **EQUIPMENT - B** – 2.2.2.2/32

Interfaces entre PEs e CEs:

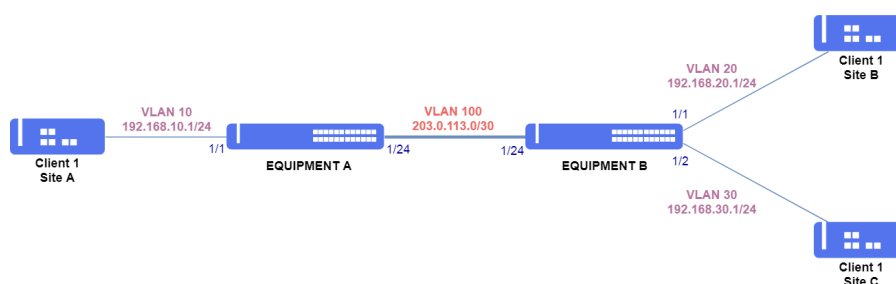
- Client 1 Site A – VLAN 10 – 192.168.10.0/24
- Client 1 Site B – VLAN 20 – 192.168.20.0/24
- Client 1 Site C – VLAN 30 – 192.168.30.0/24

Interface entre os PEs:

- VLAN 100 – 203.0.113.0/30



Não é suportada o overlapping de endereços IPs em VPNs na linha DM4000.



Exemplo de cenário com L3VPN

EQUIPMENT - A

```
ip vrf CUSTOMER1
 rd 1000:1
 route-target both 1000:1
!
interface vlan 100
 ip address 203.0.113.1/30
 set-member tagged ethernet 1/24
 ip ospf network point-to-point
 ldp enable
```

```

!
interface vlan 10
 ip vrf forwarding CUSTOMER1
 ip address 192.168.10.1/24
 set-member tagged ethernet 1/1
!
interface loopback 0
 ip address 1.1.1.1/32
 mpls enable
!
router ospf
 router-id 1.1.1.1
 network 1.1.1.1/32 area 0
 network 203.0.113.0/30 area 0
!
router bgp 1000
 bgp router-id 1.1.1.1
 neighbor 2.2.2.2 remote-as 1000
 neighbor 2.2.2.2 local-address 1.1.1.1
 neighbor 2.2.2.2 next-hop-self
 address-family vpnv4
  neighbor 2.2.2.2 activate
 address-family ipv4 vrf CUSTOMER1
  redistribute connected
!

```

EQUIPMENT - B

```

ip vrf CUSTOMER1
 rd 1000:1
 route-target both 1000:1
!
interface vlan 100
 ip address 203.0.113.2/30
 set-member tagged ethernet 1/24
 ip ospf network point-to-point
 ldp enable
!
interface vlan 20
 ip vrf forwarding CUSTOMER1
 ip address 192.168.20.1/24
 set-member tagged ethernet 1/1
!
interface vlan 30
 ip vrf forwarding CUSTOMER1
 ip address 192.168.30.1/24
 set-member tagged ethernet 1/2
!
interface loopback 0
 ip address 2.2.2.2/32
 mpls enable
!
router ospf
 router-id 2.2.2.2
 network 2.2.2.2/32 area 0
 network 203.0.113.0/30 area 0
!
router bgp 1000
 bgp router-id 2.2.2.2
 neighbor 1.1.1.1 remote-as 1000
 neighbor 1.1.1.1 local-address 2.2.2.2
 neighbor 1.1.1.1 next-hop-self
 address-family vpnv4
  neighbor 1.1.1.1 activate
 address-family ipv4 vrf CUSTOMER1
  redistribute connected
!

```



Traceroute e ping em VRFs somente são suportados entre PEs e CEs diretamente conectados. Não é possível realizar ping ou traceroute entre diferentes PEs.

Abaixo os principais comandos disponíveis para realizar a verificação das L3VPNs.

```
show ip vrf
show ip route vrf <vrf-name>
show ip bgp vrf <vrf-name>
ping vrf <vrf-name> <ip-address>
traceroute vrf <vrf-name> <ip-address>
```

12 Segurança

- Configurando Rate Limit
- Configurando Storm Control
- Configurando Port Security
- Configurando SSH e Telnet

Manter a segurança na rede consiste em adotar políticas de acesso, monitoramento dos recursos e proteção dos equipamentos para evitar ataques indesejados.

Este capítulo descreve como configurar algumas funcionalidades e recursos de segurança disponíveis na linha DmSwitch.

12.1 Configurando Rate Limit

O Rate limit é a funcionalidade que limita a taxa máxima de tráfego e o burst que uma interface poderá encaminhar (output) ou receber (input).



A taxa inserida deverá estar na unidade kbps e múltiplo de 64Kbps. O burst inserido deverá estar na unidade kB e ser potência de 2. O CLI informa os valores aproximados para o usuário.



O rate-limit só é aconselhado quando a taxa de entrada for menor de 50Mbit/s devido ao burst pequeno para a janela do TCP/IP. Para valores maiores, sugerimos o uso de meter e filtros, consulte o suporte.

Os próximos passos irão demonstrar como configurar o Rate limit na entrada com o valor de 30 Mbps (30000 kbps) com burst de 2 MB (2000 kB) e na saída com o valor de 30 Mbps (30000 kbps) com burst de 2 MB (2000 kB) na interface ethernet 1/1

```
configure
interface ethernet 1/1
rate-limit input rate 30016 burst 2048
rate-limit output rate 30016 burst 2048
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show interfaces switchport ethernet <ID>
show interfaces table utilization bandwidth
```

12.2 Configurando Storm Control

O Storm Control é um recurso de controle de ataque de tráfego para evitar que as interfaces físicas sejam impactadas por um ataque de tráfego de broadcast, multicast ou unicast. Um ataque de tráfego ocorre quando os pacotes inundam a rede, criando tráfego excessivo e degradando o desempenho da rede.



A especificação de 100 fará com que todo o tráfego do tipo configurado seja suprimido.



É possível configurar tanto em **porcentagem** como por **pps** (pacotes por segundo).

Os próximos passos irão demonstrar como configurar o Storm Control na **interface ethernet 1/1** para suprimir o tráfego broadcast em **95%** da interface, o tráfego multicast em **70%** e o tráfego unicast em **5%**.

```
configure
interface ethernet 1/1
switchport storm-control mode percent
switchport storm-control broadcast percent 95
switchport storm-control multicast percent 70
switchport storm-control unicast percent 5
```

É possível também configurar uma ação para que, ao chegar à taxa configurada, o switch execute algum comportamento. As ações podem ser:

- **shutdown**: desligar a interface durante determinado período e notificar o usuário.
- **notify**: notificar o usuário.
- **limit**: apenas limitar a taxa na interface conforme especificado na configuração.

Os próximos passos irão demonstrar como configurar o Storm Control na **interface ethernet 1/1** para que ao receber um ataque de broadcast baseado na taxa configurada, o switch coloque para down a interface após 15 segundos.

```
configure
storm-control action
interface ethernet 1/1
switchport storm-control broadcast action shutdown after 15
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show storm-control
show interfaces switchport
```

12.3 Configurando Port Security

O Port Security é a quantidade de endereços MAC que uma interface ethernet pode aprender.



É suportada a configuração do MAC Limit tanto na interface como na VLAN.

Os próximos passos irão demonstrar como configurar o Port Security para o valor de 100 endereços MACs na interface ethernet 1/1.

```
configure
interface ethernet 1/1
switchport port-security maximum 100
switchport port-security mac-address sticky
switchport port-security violation restrict
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show port-security
show interfaces switchport
```

12.4 Configurando SSH e Telnet

O SSH (Secure Shell) e TELNET são protocolos utilizados para acesso ao terminal do equipamento.



A linha DM4100 e DM4000 suporta o SSHv2 com criptografia de chave pública **RSA** (Rivest, Shamir and Adelman) e **DSA** (Digital System Algorithm).



A linha DM4100 e DM4000 tem o protocolo TELNET habilitado por padrão na configuração de fábrica.

Os próximos passos irão demonstrar como ativar o SSH e gerar a chave RSA.

```
configure
ip ssh host-key generate rsa
Generating rsa keys...
Fingerprint: SHA256:...
!
ip ssh server
```

Por questões de segurança, são suportados clientes SSH rodando o OpenSSH com versões superiores a versão 7.0. Para ter compatibilidade com versões anteriores, o usuário deverá executar o seguinte procedimento.

```
configure
ip ssh server legacy-support
% Warning:
  Enabling legacy SSH key exchange algorithms may expose equipment to security
  vulnerabilities.
Do you wish to continue? <y/N> y
```

Por padrão são suportados 8 conexões SSH e 8 conexões TELNET, com máximo de 16 conexões para cada protocolo. Para alterar o número máximo de conexões para o valor 10, o usuário deverá realizar o seguinte procedimento.

```
configure
ip ssh max-connections 10
ip telnet max-connections 10
```

Caso o usuário queira ativar o serviço de TELNET, deverá executar o seguinte procedimento:

```
configure
ip telnet server
```

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade.

```
show ip
show ip telnet
show ip ssh
```

Nota Legal

Apesar de terem sido tomadas todas as precauções na elaboração deste documento, a DATACOM não assume qualquer responsabilidade por eventuais erros ou omissão bem como nenhuma obrigação é assumida por danos resultantes do uso das informações contidas neste guia. As especificações fornecidas neste manual estão sujeitas a alterações sem aviso prévio e não são reconhecidas como qualquer espécie de contrato.

© 2021 DATACOM - Todos direitos reservados.

Garantia

Os produtos da DATACOM possuem garantia contra defeitos de fabricação pelo período mínimo de 12 (doze) meses, incluído o prazo legal de 90 dias, a contar da data de emissão da Nota Fiscal de fornecimento.

Nossa garantia é padrão balcão, ou seja, para o exercício da garantia o cliente deverá enviar o produto para a Assistência Técnica Autorizada DATACOM, com frete pago. O frete de retorno dos equipamentos será de responsabilidade da DATACOM.

Para maiores detalhes, consulte nossa política de garantia no site <https://www.datacom.com.br>.

Para contato telefônico: **+55 51 3933-3094**