DmSwitch - Boas Práticas

Quick Reference – Rev 2.6

DATACOM

Visão Geral

Este documento tem como objetivo demonstrar boas práticas para serem aplicadas as redes com equipamentos DATACOM.

Cenário de referência

Estas boas práticas podem ser aplicas em qualquer cenário de acordo com a necessidade, abaixo uma topologia genérica apenas para exemplificar os conceitos demonstrados a seguir.

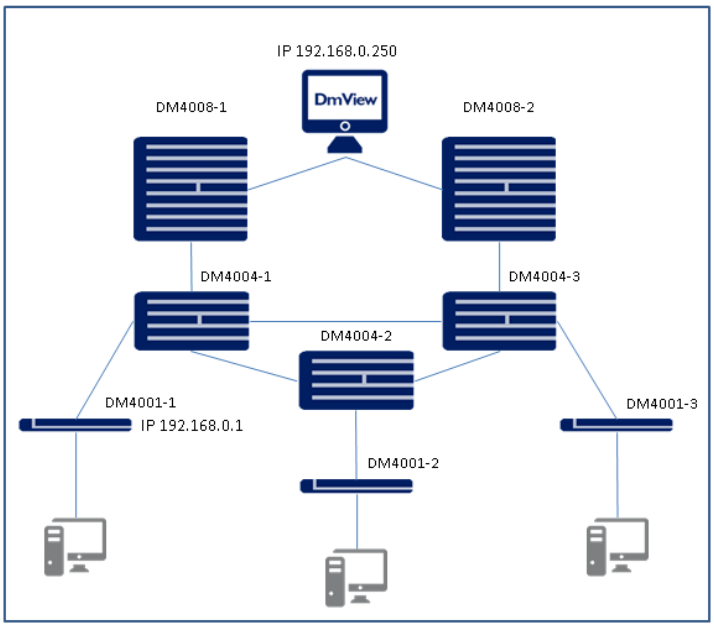

Figura 1 – Cenário de Referência.

MODEL	FIRMWARE VERSION
DM2104/DM2106	5.16.2
DmSwitch3000	11.14
DM4000/DM4100	14.10

Tabela 1 - Versão de firmware.

Configurações

Os itens serão abordados por tópicos, desta forma descrevendo a configuração pertinente para cada item. Todos os serviços irão apontar para o endereço IP do servidor DmView.

* Verificar item **Observações**.

Todas as configurações demonstradas a seguir são feitas dentro do modo de configuração.

```
!
configure
!
```

Hostname – Sempre altere o nome dos equipamentos para saber a função e localização do mesmo na rede. No exemplo: Switch de acesso Porto Alegre Rio Grande do Sul.

```
!
hostname SWACPAERS-01
!
```

Simple Network Management Protocol (SNMP) – Utilize SNMP para monitoramento do equipamento. O protocolo é habilitado na configuração *default*. É recomendado remover a comunidade *public* e alterar os nomes das comunidades de leitura e escrita para evitar ataques; especificar o servidor para as quais serão enviadas as *traps*; preencher informações adicionais para identificação do equipamento e sua funcionalidade na rede.

```
!
ip snmp-server community ComunidadeRO ro
ip snmp-server community ComunidadeRW  rw
ip snmp-server location Porto Alegre
ip snmp-server contact Suporte – 0800 0000 0000
ip snmp-server host 192.168.0.250 version 2c ComunidadeRO
ip snmp-server host 192.168.0.250 source-iface
<vlan|loopback| mgmt-eth> < ID>
ip snmp-server agent-address interface <vlan|loopback|mgmt-
eth> <ID> <ipv4|ipv6>
no ip snmp-server community public
!
```

Logs – Utilize um servidor Syslog para armazenar as mensagens dos equipamentos. Evite habilitar o modo *logging debug* para coleta de logs para não onerar o equipamento com este processo. Níveis de log: *Emergency* (0), *alert* (1), *critical* (2), *error* (3), *warning* (4), *notice* (5), *informational* (6) e *debug* (7).

```
!
logging trap 6
logging history ram 6
logging history flash 5
logging host 192.168.0.250
logging host 192.168.0.250 source-iface <vlan|loopback|mgmt-
eth> <ID>
!
```

Gerência – O acesso aos equipamentos DATACOM pode ser feito através dos protocolos TELNET, SSH, HTTP*, HTTPS, SNMP e *Remote Device Management* (RDM*). O protocolo TELNET está habilitado na configuração *default* de todos os equipamentos da linha DmSwitch*. Recomendamos definir um número máximo de conexões simultâneas dos protocolos TELNET e SSH. Sugerimos especificar um tempo para *timeout** da sessão e *login* TELNET e/ou SSH. Para o protocolo SSH é possível configurar um tempo específico para *timeout* das sessões. A porta dos serviços HTTP e HTTPS também podem ser alteradas*.

```
!
ip telnet server
ip telnet max-connections <1-16>
!
ip ssh host-key generate
ip ssh server
ip ssh max-connections <1-16>
ip ssh timeout 180
!
terminal timeout <15-3600>
terminal login-timeout <10-600>
!
ip http server
ip http port <1-65535>
ip http secure-server
ip http secure-port <1-65535>
!
```

Acesso à gerência – Permitir acesso a redes específicas sendo possível configurar de duas formas: A primeira é através da configuração de *management* e a segunda é através de filtros. O *management* atua na requisição quando a mesma chega a CPU do equipamento e requisições recebidas através da interface *mgmt*, já o filtro atua no hardware, quando a requisição chega pela interface ethernet. Por atuarem em diferentes interfaces e pontos de processamento do pacote, é recomendável que ambas as proteções sejam feitas. O exemplo a seguir trata de requisições de

SSH, porém recomenda-se que seja feita para todos os protocolos de gerência que estejam sendo utiilizados (TELNET, HTTP, HTTPS, SNMP).

DM2104.

```
!
management ssh-client 192.168.0.250/32
management ssh-client 192.168.0.0/24
!
filter new action permit match source-ip host 192.168.0.250 match destination-ip host 192.168.0.1 match destination-port 22 ingress ethernet all priority 1 remark Libera_HOST_especifico
!
filter new action permit match source-ip 192.168.0.0 255.255.255.0 match destination-ip host 192.168.0.1 match destination-port 22 ingress ethernet all priority 1 remark Libera_REDE_especifica
!
filter new action deny match destination-ip host 192.168.0.1 match destination-port 22 ingress ethernet all priority 0 remark Bloqueia_tudo
```

DmSwitch3000/DM4000/DM4100.

```
!
management ssh-client 192.168.0.250/32
management ssh-client 192.168.0.0/24
!
filter ingress new action permit match source-ip host 192.168.0.250 match destination-ip host 192.168.0.1 match destination-port 22 ethernet all priority 1 remark Libera_HOST_especifico
!
filter ingress new action permit match source-ip 192.168.0.0 255.255.255.0 match destination-ip host 192.168.0.1 match destination-port 22 ethernet all priority 1 remark Libera_REDE_especifica
!
filter ingress new action deny match destination-ip host 192.168.0.1 match destination-port 22 ethernet all priority 0 remark Bloqueia_tudo
!
```

Loopback-detection – Recomenda-se manter o protocolo habilitado para proteger contra loops óticos e/ou cabos elétricos em curto. O protocolo envia um pacote por interface, caso o mesmo pacote seja recebido pela interface em que foi enviada, a interface será bloqueada. Após a normalização do link, será iniciado um contador para garantir a integridade do link, este contador pode ser alterado na configuração da interface.

```
!
interface ethernet all
loopback-detection
loopback-detection unblock-time <2-86400>
!
```

Link Layer Discovery Protocol (LLDP) – Este protocolo é utilizado para descoberta dos equipamentos vizinhos. Recomenda-se mantê-lo habilitado apenas desabilitando em interfaces destinadas a clientes.

```
!
lldp ! Habilita o protocolo
!
interface ethernet <unit/port>
lldp admin-status disable ! Desabilita na interface de cliente/host
!
```

Operations, Administration and Management (OAM) – Este protocolo é utilizado para verificar um enlace ponto a ponto, é habilitado individualmente em cada interface. Recomenda-se configurar onde as interfaces são utilizadas no modo forçado e/ou onde existirem equipamentos SDH como meio de transporte. Onde houver estes equipamentos no meio de transmissão utilize a configuração *slow-protocols destination-address alternative* para evitar que estes equipamentos descartem os pacotes do protocolo OAM.

```
!
interface ethernet x/xx
oam
slow-protocols destination-address alternative
!
```

Network Time Protocol (NTP) – Protocolo utilizado para sincronismo de data e hora dos equipamentos. É importante implantar um servidor NTP na rede para que as informações de log estejam sincronizadas entre todos os equipamentos.

```
!
sntp client
sntp server 192.168.0.250
clock timezone <Name of time zone> <-23 - +23> <1-59>
!
```

Terminal Access Controller Access-Control System (TACACS) – É um protocolo para autenticação remota. Este protocolo troca informações com o servidor para saber se o usuário possui permissão ou não para se conectar ao equipamento, traz informações de comandos permitidos para cada usuário e registra em log comandos executados pelo usuário. Esta funcionalidade é importante para obter total controle e registro do que ocorre na rede. É possível configurar até cinco servidores para autenticação em cada switch.

```
!
tacacs-server host 1 address 192.168.0.250
tacacs-server host 1 key <Key_do_Servidor>
tacacs-server host 1 authentication
tacacs-server host 1 authorization
tacacs-server host 1 accounting
authentication login tacacs local
!
```

Remote Authentication Dial In User Service (RADIUS*) – Protocolo semelhante ao TACACS, porém apresenta mais funcionalidades e métodos de gerenciamento de usuário*. É possível configurar até cinco servidores para autenticação em cada switch.

```
!
radius-server host 1 address 192.168.0.250
radius-server host 1 key <Key_do_Servidor>
radius-server host 1 authentication
radius-server host 1 accounting
authentication login radius local
!
```

Proteções DoS - É possível limitar o número máximo de pacotes que podem ser enviados à CPU. Há uma configuração global que limita a quantidade máxima de pacotes que podem ser enviados para a CPU e também há configuração para limitar por protocolos (*show cpu-dos-protect queues*), configuráveis somente nos equipamentos DM4000 e DM4100. A seguir a tabela 2 indica valores recomendados para configuração global, esses valores poderão ser alterados de acordo com a funcionalidade do equipamento na rede. O equipamento possui proteções* presentes no hardware do equipamento. A proteção *l3-slow-path** bloqueia pacotes com TTL = 1. A proteção *subnet-broadcast* irá descartar pacotes com endereço IP de *broadcast* e pacotes com endereço IP de rede configurado em alguma VLAN do equipamento. A configuração de *Destination Lookup-up Failure*

(DLF) protege a CPU de receber pacotes com destino *unicast* desconhecido nas VLANs onde o equipamento possui endereço IP configurado.

DM2104.

```
cpu-dos-protect rate-limit global <1-1000>
cpu-dos-protect block dlf
cpu-dos-protect block l3-slow-path
cpu-dos-protect block reserved-multicast
```

DmSwitch3000.

```
cpu-dos-protect rate-limit global <1-2000000000>
cpu-dos-protect block dlf
cpu-dos-protect block l3-hdr-err
```

DM4000/DM4100.

```
cpu-dos-protect max-pps <0-5000>
cpu-dos-protect block dlf
cpu-dos-protect block l3-slow-path
cpu-dos-protect block subnet-broadcast
cpu-dos-protect max-pps <valor> queue <Num. Fila>
```

VLAN default – Não recomendamos a utilização da VLAN 1 para aplicações L2 e L3, desta forma, sugerimos a criação de uma VLAN para ser utilizada como default das interfaces.

```
!
configure
interface vlan <2-4094>
set-member untagged ethernet all
exit
!
interface ethernet all
switchport native vlan <2-4094>
end
!
```

MODEL	RATE-LIMIT GLOBAL
DM2104/DM2106	150
DmSwitch3000	180
DM4000/DM4100	2000

Tabela 2 – *Rate-limit* global recomendado.

Verificações

Abaixo os comandos relacionados às funcionalidades abordadas no tópico anterior.

```
show running-config
show ip snmp-server
show logging trap
show logging flash
show logging ram
show logging terminal
show logging commands
show ip telnet
show ip ssh
show terminal
show ip http
show management all-client
show filter
show loopback-detection
show lldp neighbor
show sntp
show tacacs-server
show radius-server
show cpu-dos-protect
show cpu-dos-protect queues
```

Observações

- O DM2100 não possui configurações de *source-iface* em alguns comandos de configurações. Consulte a ajuda do comando através do caractere '**?**'.
- O DM2100 não possui interface web, os protocolos HTTP e HTTPS atendem somente a ferramenta de gerência DmView DATACOM.
- Apenas o DM2100 possui acesso através do protocolo RDM.
- Para acessar o equipamento via TELNET utilize o endereço IP 192.168.0.25 e usuário/senha admin, caso o equipamento possua interface mgmt, o endereço IP estará configurado nesta interface.
- A configuração de *timeout* global é válida para os protocolos TELNET e SSH.
- Alterar a porta de comunicação de um protocolo é recomendado somente para administradores avançados.
- O serviço de RADIUS ainda não possui *Authorization*, consultar o Suporte DATACOM para mais informações.
- Para mais informações sobre métodos de gerenciamento de usuário, leia a documentação do protocolo.
- Proteções presentes no *hardware*: Pacotes com IP de origem igual à IP de destino, pacotes com porta UDP de origem igual à porta UDP de destino, pacotes com porta TCP de origem igual à porta TCP de destino, pacotes TCP com cabeçalho menor que 20 Bytes, pacotes TCP com *flags* incorretas (SYN, FIN, URG, PSH marcados ou com *sequence number* incorreto), pacotes TCP em que o primeiro fragmento não contenha o cabeçalho TCP, pacotes com cabeçalho TCP com *offset* igual a 1, pacotes ICMP fragmentados.
- A proteção *l3-slow-path* impacta nos protocolos de roteamento como OSPF. Alguns pacotes de troca de mensagem podem ter TTL=1 o que prejudica a comunicação. Nestes casos, a configuração ***ip ospf network point-to-point*** altera o pacote do OSPF de broadcast para unicast fazendo com que este seja enviado para CPU.
- Os equipamentos DM2100, DM3000 e DM4100 não possuem filtro *pre-ingress*, o mesmo filtro pode ser feito utilizando *ingress*.
- Para remover alguma configuração, utilize ***no*** na frente do comando. Por exemplo, para desabilitar o protocolo TELNET utilize o comando ***no ip telnet server***.

Contato

Suporte DATACOM
suporte@datacom.ind.br
Fone: +55 51 3933.3122
Rua América nº 1000
Eldorado do Sul - RS
CEP: 92990-000 - Brasil
www.datacom.ind.br