

DATAKOM



DmOS

DATAKOM OPERATING SYSTEM

Versão 5.12.0

GUIA DE CONFIGURAÇÃO RÁPIDA

204.0309.22 - 6 de janeiro 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 disso, 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:

DATAKOM

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
- **Guia de Solução de Problemas** - Fornece orientações sobre como analisar, identificar e resolver problemas com o produto (apenas em inglês)
- **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.

Accesse <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

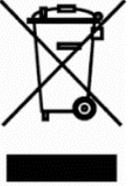
Este guia é voltado para administradores de rede, técnicos ou equipes qualificadas para instalar, configurar, planejar e manter este produto.

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 Gerenciamento básico	16
1.1 Login inicial	16
1.1.1 Instalando e energizando o equipamento	16
1.1.2 Conectando via porta Console	16
1.1.3 Conectando via porta de gerência out-of-band	16
1.1.4 Conectando pela primeira vez no equipamento	17
1.2 Gerenciamento do Firmware	17
1.2.1 Atualização do software DmOS	18
1.2.2 Realizando o downgrade do firmware	19
1.2.3 Atualização do software das ONUs	19
1.3 Visão geral do CLI	21
1.3.1 Modo Operacional	21
1.3.2 Modo de Configuração	22
1.3.3 Tipos de Configuração	23
1.3.4 Criando um Alias	24
1.4 Gerenciamento da Configuração	25
1.4.1 Configurações Salvas	25
1.4.2 Restaurando Configuração	25
1.4.3 Restaurando a Configuração de Fábrica	25
1.5 Gerenciamento dos Arquivos	26
1.5.1 Salvando a Configuração em Arquivo	26
1.5.2 Exportando os Arquivos	26
1.5.3 Importando os Arquivos	26
1.5.4 Manipulação de Arquivos	26
1.5.5 Configuração a partir de arquivos	27
1.5.6 Edição de arquivos	27
1.5.7 Exportando as MIBs SNMP	27
2 Gerenciamento do Equipamento	29
2.1 Configuração das Senhas	29
2.2 Reset de Senha	29
2.2.1 Reset de configuração	30
2.2.2 Reset de senha do usuário admin	30

2.3 Configuração das Licenças	30
2.3.1 Habilitando a licença MPLS	31
2.3.2 Habilitando a licença das portas 100 Gigabit	31
2.3.3 Verificando o Licenciamento	31
2.4 Configuração do Product Model	32
2.4.1 Configuração de Product Model no DM4270 24XS	32
2.5 Configuração dos Recursos de Encaminhamento	33
2.6 Configuração da Gerência	34
2.6.1 Configurando a Gerência Out-of-Band	34
2.6.2 Configurando a Gerência In-Band	35
2.7 Configuração do Acesso a CLI	36
2.7.1 Gerando as chaves SSH	36
2.7.2 Habilitando o suporte a versões antigas do SSH	36
2.7.3 Configurando o número máximo de conexões SSH e Telnet	36
2.7.4 Habilitando o serviço Telnet	37
2.8 Configuração do Hostname	37
2.8.1 Configurando o Hostname	37
2.9 Configuração do Banner	37
2.9.1 Configurando o Banner em linha Única	37
2.9.2 Configurando o Banner em múltiplas linhas	38
2.9.3 Verificando o Banner	38
2.10 Configuração do Relógio e Data do Sistema	38
2.10.1 Configurando o Relógio do Sistema	39
2.10.2 Configurando o Timezone	39
2.10.3 Verificando o Relógio do Sistema	39
3 Gerenciamento de Rede	40
3.1 Configuração do LLDP	40
3.1.1 Configurando o LLDP entre dois vizinhos	40
3.1.2 Verificando o LLDP	40
3.2 Configuração do SNTP	41
3.2.1 Configurando o SNTP	41
3.2.2 Configurando o SNTP com Autenticação	42
3.2.3 Verificando o SNTP	42
3.3 Configuração do Syslog	42
3.3.1 Configurando o Syslog Remoto	43
3.3.2 Verificando o Syslog	43
3.4 Configuração do SNMP	44
3.4.1 Configurando o SNMPv2	44

3.4.2 Configurando o SNMPv3	45
3.4.3 Configurando o envio de notificações SNMP	47
3.4.4 Configurando parâmetros do SNMP	49
3.4.5 Verificando o SNMP	51
3.5 Ping	52
3.6 Traceroute	52
3.7 SSH Client	53
3.8 Telnet Client	53
4 OAM	55
4.1 Configuração do CFM	55
4.1.1 Configurando o CFM	55
4.1.2 Configurando o CFM com QinQ	57
4.1.3 Habilitando o Alarm Indication Signal (ETH-AIS)	59
4.1.4 Habilitando o Action Block	60
4.1.5 Habilitando o Action Shutdown	61
4.1.6 Gerenciamento de falhas	63
4.1.7 Ethernet Delay Measurement (ETH-DM)	63
4.1.8 Verificando o CFM	65
4.2 Configuração do EFM	65
4.2.1 Configurando o EFM	65
4.2.2 Verificando o EFM	66
4.3 Configuração do RDM	66
4.3.1 Configurando o RDM como escravo	67
4.3.2 Verificando o RDM	68
4.4 Configuração do Traffic Loop	68
4.4.1 Configurando o Traffic Loop para Validação do Tráfego L2	68
4.5 Configuração do TWAMP	69
4.5.1 Configurando uma sessão TWAMP	70
4.5.2 Configurando ACLs no TWAMP Reflector	71
4.5.3 Configurando o TWAMP na VRF	72
4.5.4 Calculando o número máximo de sessões suportadas no TWAMP Reflector	72
4.5.5 Verificando o TWAMP	73
4.6 Configuração do sFLOW	73
4.6.1 Configurando o sFLOW	74
4.7 Configuração do agendamento de tarefas	74
4.7.1 Configurando um reboot automático	74
4.7.2 Configurando backup automático de configuração	75
4.7.3 Executando uma tarefa manualmente	75

4.7.4 Executando uma tarefa a partir de um padrão	76
4.7.5 Verificando o Assistant Task	77
4.8 Configuração de contadores	77
4.8.1 Configurando contadores de VLANs	77
4.8.2 Configurando contadores de interfaces	78
4.8.3 Verificando os Counters	79
5 Autenticação de Usuários	80
5.1 Configuração dos Usuário Locais	80
5.1.1 Criando um novo Usuário Local	81
5.1.2 Deletando um Usuário Local	81
5.2 Configurando o TACACS+	81
5.2.1 Configurando um servidor TACACS+	81
5.3 Configuração do RADIUS	82
5.3.1 Configurando um servidor RADIUS	82
5.4 Configuração da Ordem de Autenticação	83
5.4.1 Configurando o RADIUS como mais prioritário	83
5.4.2 Configurando o TACACS+ como mais prioritário	83
6 Interfaces	85
6.1 Configuração das Interfaces Ethernet	85
6.1.1 Configurando as Interfaces Ethernet	85
6.1.2 Configurando um range de Interfaces Ethernet	86
6.1.3 Configurando a Description das Interfaces Ethernet	86
6.1.4 Configurando o MTU das Interfaces Ethernet	87
6.1.5 Configurando o TPID das Interfaces Ethernet	87
6.1.6 Configurando uma Interface 10Gbps para operar em 1Gbps	88
6.1.7 Verificando as Interfaces Ethernet	89
6.2 Configuração do Link Aggregation	89
6.2.1 Configurando um LAG no modo estático	89
6.2.2 Configurando um LAG no modo dinâmico (LACP)	90
6.2.3 Configurando o hash para o balanceamento de carga	91
6.2.4 Configurando o modo de balanceamento de carga	91
6.2.5 Configurando o número máximo e mínimo de links ativos em um LAG	92
6.2.6 Verificando o Link Aggregation	93
6.3 Configuração do Port Mirroring	93
6.3.1 Configurando o Port Mirroring para o tráfego recebido	94
6.3.2 Configurando o Port Mirroring para o tráfego transmitido	94
6.3.3 Configurando o Port Mirroring para o tráfego transmitido e recebido	94
6.4 Configuração do Link Flap Detection	95

6.4.1 Configurando o Link Flap Detection na interface ethernet	95
6.4.2 Verificando o Link Flap	95
6.5 Configuração do Hold Time	96
6.5.1 Configurando o Hold Time	96
6.5.2 Verificando o Hold Time	97
7 GPON	98
7.1 Operações Básicas do GPON	98
7.1.1 Configurando uma interface GPON	98
7.1.2 Configurando o método de autenticação das ONUs	99
7.1.3 Descobrimo as ONUs	100
7.1.4 Provisionando a ONU	100
7.1.5 Removendo a ONU	100
7.1.6 Verificação básica do GPON	101
7.2 Perfis GPON	101
7.2.1 Carregando os Perfis Default	102
7.2.2 Bandwidth Profile	103
7.2.3 Line Profile	103
7.2.4 Media Profile	104
7.2.5 SIP Agent Profile	105
7.2.6 SNMP Profile	105
7.2.7 GEM Traffic Agent Profile	106
7.2.8 Residential Gateway Profile (RG-Profile)	107
7.2.9 TR-069 ACS Profile	110
7.2.10 Verificando os perfis GPON	111
7.3 Tipos de Serviço GPON	112
7.3.1 Service VLAN N:1	112
7.3.2 Service VLAN 1:1	112
7.3.3 Service VLAN TLS	112
7.4 Mapeando o Service Port	113
7.4.1 Service Port - Transparent	113
7.4.2 Service Port - Replace	113
7.4.3 Service Port - Add	113
7.5 Configurando Aplicações GPON	113
7.5.1 Configurando uma Aplicação N:1 com ONU bridge	114
7.5.2 Configurando uma Aplicação 1:1 com ONU bridge	115
7.5.3 Configurando uma Aplicação TLS com ONU router	116
7.5.4 Configurando uma aplicação GPON com MPLS	117
7.5.5 Verificando aplicações GPON	117

7.6 Provisionamento Automático de ONUs	118
7.6.1 Verificando o provisionamento automático	120
8 Switching	121
8.1 Configuração da Tabela MAC	121
8.1.1 Configurando o tempo de Aging	121
8.1.2 Desativando o aprendizado de endereços MAC	122
8.1.3 Verificando a tabela MAC	122
8.2 Configuração de VLAN	122
8.2.1 Configurando VLANs com interfaces Tagged	123
8.2.2 Configurando VLANs com interfaces Untagged	123
8.2.3 Configurando QinQ	124
8.2.4 Configurando QinQ Seletivo	125
8.2.5 Configurando o VLAN Translate	126
8.2.6 Verificando a configuração de VLAN	127
8.3 Configuração do RSTP	127
8.3.1 Configurando um RSTP Básico	127
8.3.2 Aplicando os parâmetros do RSTP	128
8.3.3 Verificando o RSTP	129
8.4 Configuração do MSTP	129
8.4.1 Configurando o MSTP para balanceamento do tráfego	130
8.4.2 Verificando o MSTP	131
8.5 Configuração do EAPS	132
8.5.1 Configurando um Anel EAPS Básico	132
8.5.2 Verificando o EAPS	133
8.6 Configuração do ERPS	133
8.6.1 Configurando o ERPS Single Ring	134
8.6.2 Configurando o ERPS Multi-ring	135
8.6.3 Verificando o ERPS	139
8.7 Configuração do L2CP	140
8.7.1 Configurando o L2CP no modo extended	140
8.7.2 Configurando o L2CP por protocolo específico	141
8.7.3 Configurando a transparência de PDUs	142
8.7.4 Verificando o L2CP	142
8.7.5 Comportamento default das PDUs nas OLTs	143
8.7.6 Comportamento default das PDUs nos Switches	143
8.8 Configuração do Loopback Detection	143
8.8.1 Configurando Loopback Detection para a rede de acesso	144
8.8.2 Verificando o Loopback Detection	144

8.9 Configuração do DHCP Relay L2	145
8.9.1 Verificando o DHCP Relay	145
9 Serviços IP	146
9.1 Configuração de Endereços IP	146
9.1.1 Configurando endereços IPv4	146
9.1.2 Configurando endereços IPv6	146
9.1.3 Verificando os endereços IP	147
9.1.4 Configurando MTU em interfaces L3	147
9.2 Configuração do IPv6 SLAAC	147
9.2.1 Verificando o IPv6 SLAAC	149
9.3 Configuração do DHCP Relay L3	149
9.3.1 Configurando o DHCP Relay L3	150
9.3.2 Configurando o DHCP Option globalmente	151
9.3.3 Configurando o DHCP Option por interface	151
10 Roteamento	153
10.1 Configuração de Rotas Estáticas	153
10.1.1 Configurando uma Rota Estática Padrão	153
10.1.2 Verificando as Rotas Estáticas	154
10.2 Configuração de rotas black hole	155
10.2.1 Configurando rotas black hole IPv4	155
10.2.2 Configurando rotas black hole IPv6	155
10.2.3 Sumarização com rotas black hole	156
10.3 Configuração do VLAN Routing	157
10.3.1 Configurando um Roteamento Básico entre VLANs	157
10.3.2 Verificando as Rotas	158
10.4 Configuração da VRF	158
10.4.1 Configurando a VRF Lite	158
10.4.2 Habilitando o Route Leaking entre VRFs	160
10.4.3 Verificando as VRFs	162
10.5 Configuração do PBR	162
10.5.1 Verificando o PBR	164
10.6 Configuração do OSPFv2	164
10.6.1 Configurando o OSPFv2 em rede Ponto a Ponto	164
10.6.2 Configurando o OSPFv2 em rede Broadcast	166
10.6.3 Configurando a área no OSPFv2	168
10.6.4 Filtrando rotas recebidas no OSPFv2	169
10.6.5 Filtrando rotas redistribuídas no OSPFv2	170
10.6.6 Habilitando ECMP no OSPFv2	171

10.6.7	Sumarização de rotas no OSPFv2	172
10.6.8	Verificando o OSPFv2	174
10.7	Configuração do OSPFv3	174
10.7.1	Configurando o OSPFv3 Ponto a Ponto	175
10.7.2	Habilitando ECMP no OSPFv3	176
10.7.3	Verificando o OSPFv3	178
10.8	Configuração do BGP	178
10.8.1	Configurando uma sessão eBGP IPv4 Single Homed	178
10.8.2	Configurando route-maps e prefix-lists IPv4	180
10.8.3	Configurando uma sessão iBGP IPv6 Single Homed	181
10.8.4	Configurando route-maps e prefix-lists IPv6	183
10.8.5	Configurando BGP Communities	184
10.8.6	Verificando o BGP	186
10.9	Configuração do VRRP	186
10.9.1	Configurando o VRRPv2 para fornecer Alta Disponibilidade	187
10.9.2	Verificando o VRRP	188
10.10	Configuração do BFD	189
10.10.1	Configurando o BFD no OSPFv2	189
10.10.2	Verificando o BFD	190
11	MPLS	192
11.1	Configurando o LDP	192
11.2	Configurando o RSVP	193
11.3	Configuração de VPWS	201
11.3.1	VPWS com LDP	203
11.3.2	VPWS com RSVP	209
11.3.3	VPWS com acesso GPON	210
11.4	Configuração de VPLS	215
11.4.1	VPLS com LDP	219
11.4.2	VPLS com RSVP	226
11.4.3	Habilitando o TLS em uma VPLS	227
11.5	Habilitando o FAT em uma L2VPN	227
11.6	Verificando L2VPNs	228
11.7	Configuração de L3VPNs	228
11.7.1	Configurando uma L3VPN Site-to-Site	228
11.7.2	Configurando uma L3VPN Hub and Spoke	231
11.7.3	Configurando BGP entre PEs e CEs	235
11.7.4	Habilitando o AS Override	237
11.7.5	Habilitando o Allow AS In	237

11.7.6 Configurando OSPF entre PEs e CEs	237
11.7.7 Verificando L3VPNs	239
12 Multicast	240
12.1 Configuração do IGMP Snooping	240
12.1.1 Configurando o IGMP Snooping em Aplicações Ethernet	240
12.1.2 Configurando o IGMP Snooping em Aplicações GPON	241
12.1.3 Verificando o IGMP	242
13 QoS	243
13.1 Configuração do Controle de Congestionamento	243
13.1.1 Configurando o escalonador WFQ	243
13.2 Configuração do Traffic Shapping	244
13.2.1 Configurando o Rate Limit na Interface	244
13.3 Configuração do Traffic Policing	244
13.3.1 Configurando o Traffic Policing baseado em VLANs	245
13.3.2 Configurando o Traffic Policing baseado na inner VLAN	246
13.3.3 Configurando o Traffic Policing baseado no PCP	247
13.3.4 Configurando o Traffic Policing baseado no DSCP	247
13.3.5 Verificando QoS policers	248
14 Segurança	249
14.1 Configuração do Storm Control	249
14.1.1 Configurando o Storm Control	249
14.1.2 Verificando o Storm Control	250
14.2 Configuração de ACLs	250
14.2.1 Configurando uma ACL L2 para negar o tráfego de uma VLAN	250
14.2.2 Configurando uma ACL L3 para negar o tráfego de um endereço IPv4	251
14.2.3 Configurando uma ACL para proteção do CPU	251
14.2.4 Configurando uma ACL para pacotes com origem no CPU	253
14.2.5 Verificando as ACLs	253
14.3 Configuração do Anti IP Spoofing	254
14.3.1 Configurando Anti IP Spoofing para endereço IPv4 e MAC específico	254
14.3.2 Configurando Anti IP Spoofing para endereço IPv4 específico	254
14.3.3 Configurando Anti IP Spoofing para todos endereços IPv6	255
14.3.4 Configurando Anti IP Spoofing para todos endereços IPv4 e IPv6	255
14.3.5 Verificando o Anti IP Spoofing	255
14.4 Configuração do MAC Limit	256
14.4.1 Configurando o MAC Limit na Interface	256
14.4.2 Configurando o MAC Limit na VLAN	256

14.4.3 Verificando o MAC Limit	256
14.5 Configuração do CPU DoS Protect	257
14.5.1 Configurando o CPU DoS Protect Global	257
14.5.2 Configurando o CPU DoS Protect por Protocolo	258
14.5.3 Verificando o CPU DoS Protect	258
Nota Legal	259
Garantia	259

1 Gerenciamento básico

Este capítulo contém a seguinte seção:

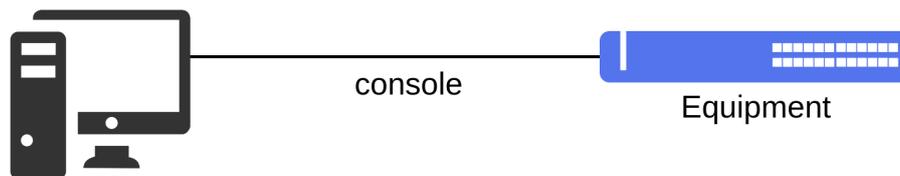
- Login inicial
- Gerenciamento do Firmware
- Visão geral do CLI
- Gerenciamento da Configuração
- Gerenciamento dos Arquivos

1.1 Login inicial

1.1.1 Instalando e energizando o equipamento

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

1.1.2 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** sem controle de fluxo por hardware ou software.

1.1.3 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.

1.1.4 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: admin
Password: admin
Welcome to the DmOS CLI
```



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]
```



Nas interfaces do DmOS é utilizado a nomenclatura **chassis/slot/port**.



O caractere **!** é utilizado nos comandos do CLI para identificação e também pode ser utilizado para adicionar comentários em scripts de configuração do DmOS.

1.2 Gerenciamento do Firmware

O DmOS possui duas posições de memória para armazenamento de firmware. Após o download do firmware a imagem é salva na posição inativa ou vazia.



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.

1.2.1 Atualização do software DmOS

Para atualização do software via CLI será necessário utilizar um servidor TFTP, SCP ou HTTP a fim de encaminhar o arquivo de firmware para o equipamento. Os exemplos abaixo demonstram como atualizar o firmware do equipamento com o arquivo denominado **build.swu** através do servidor com endereço IPv4 **192.168.0.1**.

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

```
request firmware add tftp://192.168.0.1/build.swu
```

Para receber o arquivo de firmware através do protocolo **SCP**, usar o seguinte comando:

```
request firmware add scp://192.168.0.1/build.swu username user password "pass"
```

Para receber o arquivo de firmware através do protocolo **HTTP**, usar o seguinte comando:

```
request firmware add http://192.168.0.1/build.swu
```

O firmware recebido estará na posição *Inactive*. É possível verificar o progresso de download do firmware e o novo firmware copiado através do seguinte comando:



Como o firmware é escrito diretamente na flash, o equipamento remove o firmware que estava na posição *Inactive* durante o processo de atualização, por esse motivo em caso de falha ela ficará vazia (*Empty*).

```
show firmware
```

Para ativar o firmware que está na posição *Inactive* usar o comando abaixo. O equipamento irá reinicializar automaticamente após finalizar a ativação do firmware.

```
request firmware activate
```

```
Warning: Firmware downgrade may not be totally supported. Please, refer to  
the Hardware and Software Compatibility section in the DmOS Release Notes.  
Warning: The system will reboot automatically in order to complete the  
activation process. Once initiated this process cannot be interrupted.  
Proceed with activation? [no,yes] yes
```



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

Após o equipamento reinicializar, verificar que o novo firmware agora está no estado **Active** usando novamente o comando:

```
show firmware
```

1.2.2 Realizando o downgrade do firmware

O processo de downgrade de firmware, ou seja, atualizar para uma versão anterior, deve ser realizado de forma controlada e alguns cuidados são necessários para evitar problemas de incompatibilidade.

O DmOS não preserva a configuração atual durante o processo do downgrade de firmware, será carregada a última configuração usada na versão anterior do firmware instalado.



Caso o equipamento nunca tenha recebido o firmware mais antigo que será instalado, ao realizar o downgrade o equipamento irá iniciar com a configuração de fábrica.

Para detalhes sobre compatibilidade de versões do DmOS, o documento **DmOS Release Notes** deve ser consultado.

Abaixo os passos a serem realizados no processo de downgrade de firmware DmOS:

1- Salvar a configuração atual em um arquivo texto.

```
configure  
save <FILE_NAME>
```

2 - Efetuar o request do firmware para o equipamento.

```
request firmware add <protocol://ipaddress/path/fw_name>
```

3 - Verificar que o firmware aparece com status Inactive.

```
show firmware
```

4 - Ativar o firmware.

```
request firmware activate
```

1.2.3 Atualização do software das ONUs

Para plataformas de hardware que suportam a tecnologia GPON, a imagem de firmware da ONU pode ser copiada para o equipamento utilizando a CLI. Para os próximos passos deve ser assegurado que todas as ONUs a serem atualizadas estejam com estado operacional UP.

Realizando o download do firmware

Para realizar o download do firmware da ONU na OLT executar o seguinte procedimento:

```
request firmware onu add tftp://192.168.0.1/fw_onu.bin
```



Aguarde a mensagem “ONU firmware file download has succeeded” para proceder com os próximos passos.

Atualizando uma ONU

Para atualizar somente a ONU 1 localizada na interface gpon 1/1/1 o usuário deve proceder com o seguinte comando:

```
request firmware onu install fw_onu.bin interface gpon 1/1/1 onu 1
```

Para verificar o progresso de atualização, usar o seguinte comando:

```
show interface gpon 1/1/1 onu
ID   Serial Number   Oper State   Software Download State   Name
---   -
0    DACM00001533    Down        None                       CLIENT-01
1    DACM000001E0    Up          Download in progress (60%) CLIENT-02
126  DACM00001C7B    Up          None                       CLIENT-03
127  DTCM10000006    Up          None                       CLIENT-04
```



Durante o estado de download o status da ONU estará em **Download in progress**. Após alguns minutos a ONU irá reinicializar automaticamente com o novo firmware, alterando o status para Complete.

Alternativamente, é possível realizar a atualização do firmware de uma ONU através de uma interface L3 utilizando o seguinte comando:

```
request firmware onu install fw_onu.bin in-band-upgrade ip-address 172.24.1.158 model dm984-42x
username support password support
```



Note que a ONU é referenciada pelo seu endereço IP da VLAN de gerência do IP host, neste caso, é necessário que a VLAN configurada no lado da OLT para o IP host da ONU tenha endereço IP configurado através de uma interface L3, conforme descrito na sessão [Configuração de Endereços IP](#). Esta conectividade pode ser validada através de um ping da OLT para o IP da interface de gerência IP host da ONU. Durante o procedimento de cópia do firmware para a ONU o CLI fica indisponível para o usuário até que o processo seja finalizado.

Atualizando todas ONUs de um PON-link

Para atualizar todas as ONUs de um pon-link o usuário deve executar o procedimento a seguir. Abaixo o exemplo demonstra a atualização de todas as ONUs do pon-link 1/1/7.

```
request firmware onu install fw_onu.bin interface gpon 1/1/7 all
```



A atualização ocorrerá em grupos de 8 ONUs.

Para verificar o progresso de atualização de todas as ONUs, usar o seguinte comando:

```
show interface gpon 1/1/7 onu
```

ID	Serial Number	Oper State	Software Download State	Name
0	DACM00000B4F	Up	Download in progress (97%)	CLIENT-22
1	DACM00000B7C	Up	Download in progress (97%)	CLIENT-23
2	DACM00000B7B	Up	Download in progress (97%)	CLIENT-24
3	DACM00000B92	Up	Download in progress (97%)	CLIENT-25
4	DACM00000B73	Up	Download in progress (97%)	CLIENT-26
5	DACM00000B8A	Up	Download in progress (97%)	CLIENT-31
6	DACM00000B8E	Up	Download in progress (97%)	CLIENT-32
7	DACM00000B78	Up	Download in progress (92%)	CLIENT-33
8	DACM00000B8D	Up	None	CLIENT-34
9	DACM00000B7A	Up	None	CLIENT-35
10	DACM00000B8B	Up	None	CLIENT-36
11	DACM00000B90	Up	None	CLIENT-37
12	DACM00000B96	Up	None	CLIENT-38
13	DACM00000B74	Up	None	CLIENT-39
14	DACM00000B49	Up	None	CLIENT-40
15	DACM00000B58	Up	None	CLIENT-41
16	DACM00000B15	Up	None	CLIENT-42



Durante o estado de download o status das ONUs estará em **Download in progress**. Após alguns minutos as ONUs irão reinicializar automaticamente com o novo firmware, alterando o status para Complete.

1.3 Visão geral do CLI

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

A CLI do DmOS suporta os modos de **configuração** e **operacional** que proveem comandos de configuração, monitoramento de software, hardware e conectividade de rede com outros equipamentos.

1.3.1 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 platform	Apresenta o modelo do equipamento, módulos e firmware em uso
show inventory	Apresenta o inventário do equipamento, módulos e interfaces em uso
show environment	Apresenta os valores dos sensores de temperatura
show firmware	Apresenta a versão de firmware
show running-config	Apresenta a configuração atual do equipamento
show system cpu	Apresenta os valores da CPU em uso do equipamento
show system memory	Apresenta os valores de memória do equipamento
show system uptime	Apresenta o tempo de atividade do equipamento
who	Apresenta os usuários conectados no equipamento

É possível executar qualquer comando do modo operacional dentro do modo de configuração adicionando a palavra-chave **do** antes do comando. Abaixo um exemplo:

```
do show running-config
```

1.3.2 Modo de Configuração

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

```
config
```

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 primeiro nível de configuração, é possível usar o comando abaixo em qualquer nível hierárquico de configuração.

```
top
```

Estão disponíveis duas opções de modo de configuração: **terminal** e **exclusive**. Se o comando `config` não for completado com o modo desejado, por padrão, será utilizado o modo terminal.

Modo Terminal

Neste modo, qualquer configuração no equipamento alterada por outra sessão irá conflitar com a configuração da sessão corrente. Na tentativa de salvar uma configuração, será visualizada uma mensagem com as intruções para se resolver o conflito. O comando a seguir é usado para entrar neste modo de configuração:

```
config terminal
```

Por padrão, caso o usuário entrar no modo de configuração sem especificar algum modo específico, o modo a ser utilizado será o terminal.

```
config
```

Modo Exclusivo

Quando o usuário entra no modo **exclusive**, qualquer outra sessão simultânea não conseguirá aplicar suas configurações. O comando a seguir é usado para entrar neste modo de configuração:

```
config exclusive
```

1.3.3 Tipos de Configuração

O DmOS utiliza o protocolo **NETCONF** definido pela **RFC4741**. O NETCONF define a existência de uma ou mais configurações de dados salvas permitindo a operação de configuração em cada uma delas. O DmOS faz uso de duas configurações, porém, apenas uma está rodando de fato no equipamento, são elas:

- **Configuração Candidata (Candidate-config):** Enquanto o usuário altera a configuração e não realiza o commit, a configuração é salva temporariamente na configuração candidata. Se o dispositivo reinicializar ou sair da sessão, a configuração candidata será perdida.
- **Configuração Corrente (Running-config):** Depois que o usuário executa o comando `commit`, a configuração candidata é aplicada à configuração corrente se tornando ativa no equipamento em todos os componentes de software.

Quando o usuário entra no modo de configuração e começa a realizar configurações, a configuração ainda não está sendo de fato aplicada no equipamento. Neste caso, o usuário está escrevendo a configuração na configuração candidata. O comando a seguir exibirá a configuração da candidata do nível hierárquico em que o usuário se encontra:

```
show
```

O próximo comando exibirá apenas as alterações feitas na configuração candidata:

```
show configuration
```

Para ativar e salvar a configuração candidata é necessário copia-la para a **running-config**. O comando a seguir irá salvar a configuração candidata na **running-config**.

```
commit
```

No entanto, se o usuário deseja apenas verificar a configuração candidata, mas não quer copia-la para a **running-config** é necessário usar o comando a seguir:

```
commit check
```

O usuário também pode confirmar temporariamente uma configuração candidata e aguardar uma confirmação dentro de um determinado período de tempo (10 minutos por padrão). Se o tempo expirar e o usuário não confirmar, a configuração será revertida para a anterior. Esta opção está disponível apenas no modo de configuração **exclusive**.

```
commit confirmed
```

O usuário poderá abortar a configuração ainda a ser confirmada e antes do tempo limite através do seguinte comando:

```
commit abort
```

Para apagar todas as alterações de configuração feitas após a última configuração salva, o usuário deve usar o seguinte comando:

```
clear
```

1.3.4 Criando um Alias

O DmOS permite ao usuário criar um comando personalizado, possibilitando retornar o resultado de um ou mais comandos como resultado de apenas um comando.

Suponha que o usuário frequentemente execute uma sequência de comandos para verificar informações do sistema.

Os passos abaixo mostram como configurar um alias para retornar a saída dos comandos **show environment**, **show platform** e **show firmware** executando apenas o comando **show-system**.

```
config
alias show-system
expansion "show environment ; show platform ; show firmware"
commit
```



O comando alias não permite auto-complete.

1.4 Gerenciamento da Configuração

1.4.1 Configurações Salvas

Quando o usuário salva uma configuração, um arquivo contendo suas alterações de configuração é gerado e armazenado. Para verificar esta lista de arquivos, o usuário deve usar o seguinte comando:

```
show configuration commit list
```



São salvas as últimas 64 configurações commitadas.

1.4.2 Restaurando Configuração

Se o usuário deseja reverter para a última configuração salva, deve usar o seguinte procedimento:

```
rollback configuration  
commit
```

O usuário pode restaurar configurações salvas mais recentemente. Para isso, deve usar o seguinte procedimento:

```
rollback configuration FILE-NAME  
commit
```

No entanto, se o usuário desejar selecionar apenas um arquivo específico salvo sem retornar às mudanças mais recentes deve usar o seguinte procedimento:

```
rollback selective FILE-NAME  
commit
```

1.4.3 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:

```
load factory-config
```



É possível realizar qualquer configuração antes de executar o **commit**. Desta forma, é possível manter a configuração de gerenciamento caso desejado.

```
commit
```

1.5 Gerenciamento dos Arquivos

1.5.1 Salvando a Configuração em Arquivo

O usuário pode salvar a configuração candidata em um arquivo (incluindo as configurações padrão) sem aplicá-la no equipamento. O comando a seguir salvará a configuração candidata em um arquivo chamado **CANDIDATE-CONFIG**:

```
save CANDIDATE-CONFIG
```

O usuário também pode salvar configurações feitas em um caminho específico usando um filtro de caminho. Por exemplo, se o usuário quiser salvar apenas a configuração de uma interface MGMT (incluindo as configurações padrão) em um arquivo chamado **INTF-MGMT-CONFIG**, deve usar o seguinte comando:

```
save INTF-MGMT-CONFIG interface mgmt
```



É necessário ter cuidado para não carregar um arquivo salvo que não contenha uma configuração completa usando a opção de substituição (override).

1.5.2 Exportando os Arquivos

Após salvar um arquivo, o usuário poderá exportar este arquivo para um servidor SCP ou TFTP. O comando a seguir encaminhará o arquivo via protocolo TFTP salvo como **CANDIDATE-CONFIG** para o servidor 172.1.1.1.

```
copy file CANDIDATE-CONFIG tftp://172.1.1.1
```

1.5.3 Importando os Arquivos

Após exportar um arquivo, o usuário poderá importar este arquivo de um servidor SCP ou TFTP. O comando a seguir realiza o download do arquivo via protocolo TFTP salvo como **CANDIDATE-CONFIG** no servidor 172.1.1.1.

```
copy file tftp://172.1.1.1 CANDIDATE-CONFIG
```

1.5.4 Manipulação de Arquivos

Para exibir todos os arquivos salvos, o usuário deve usar o comando abaixo. Uma vez que é um comando de modo operacional, deve-se adicionar a palavra-chave **do** na frente do comando quando estiver no modo de configuração.

```
file list
```

É possível inspecionar o conteúdo de um arquivo salvo através do seguinte comando:

```
file show FILE-NAME
```

Para excluir um arquivo deve-se usar o seguinte comando:

```
file delete FILE-NAME
```

1.5.5 Configuração a partir de arquivos

É possível mesclar a configuração candidata com um arquivo salvo usando a opção **merge**. Assim, se houver novos comandos no arquivo, eles serão carregados para a configuração candidata. Se os comandos no arquivo entrarem em conflito com aqueles na configuração candidata, eles substituirão os comandos na configuração candidata.

```
load merge FILE-NAME  
commit
```

Através do comando **override**, o usuário poderá apagar toda a configuração candidata e carregar uma nova configuração completa de um arquivo:

```
load override FILE-NAME  
commit
```

1.5.6 Edição de arquivos

É possível editar um arquivo existente ou criar um novo, se ele ainda não existir. O nome do arquivo é limitado a 255 caracteres e não deve começar com "." ou "-", nem conter caminhos de diretório.

Para editar um arquivo deve-se utilizar o seguinte comando:

```
file edit FILE-NAME
```

O editor de arquivos será aberto. Use "CTRL + s" para salvar o arquivo e "CTRL + x" para sair do editor e retornar à CLI do DmOS.

1.5.7 Exportando as MIBs SNMP

O usuário pode exportar um arquivo com todas as MIBs SNMP suportadas pelo equipamento para um servidor SCP ou TFTP.

O comando a seguir encaminhará o arquivo com as MIBs via protocolo TFTP com o nome **datacom-mibs.tar.gz** para o servidor 172.1.1.1.

```
copy mibs tftp://172.1.1.1
```

2 Gerenciamento do Equipamento

O administrador da rede pode configurar um equipamento com DmOS de duas formas:

- **CLI (Comand-Line Interface):** Prove um conjunto de comandos para gerenciar o equipamento através de conexão Telnet, SSH ou via porta console.
- **DmView:** É o NMS (Network Management System) da DATACOM baseado em SNMP e NETCONF. O DmView é um sistema integrado de gerenciamento de rede e elementos, projetado para supervisionar e configurar equipamentos DATACOM, oferecendo monitoramento, configuração, provisionamento, auditoria, desempenho, segurança, descoberta, mapas e funcionalidades de inventário.

Este capítulo irá guiar o usuário em como proceder com a configuração de gerenciamento equipamento via CLI. Ele contém as seguintes seções:

- Configuração das Senhas
- Reset de Senha
- Configuração das Licenças
- Configuração do Product Model
- Configuração dos Recursos de Encaminhamento
- Configuração da Gerência
- Configuração do Acesso a CLI
- Configuração do Hostname
- Configuração do Banner
- Configuração do Relógio e Data do Sistema

2.1 Configuração das Senhas



É recomendado configurar as senhas dos protocolos sempre entre aspas duplas "password". Assim é possível configurar senhas sem problema referente ao uso de caracteres especiais.

2.2 Reset de Senha

Para realizar o reset de senha do usuário admin no DmOS, é necessário acessar o equipamento através do console e reiniciá-lo. Durante o boot, ao ver a mensagem **Press CTRL-C to stop booting**, pressione **CTRL+C** para acessar o *U-Boot*. Será solicitada uma senha.

Para gerar a senha do U-Boot, é necessário entrar em contato com o Suporte Datacom e informar o serial e endereço MAC do equipamento, exibidos durante o boot, conforme demonstrado abaixo.

```
MGMT PHY: reset OK
Board ID: 0x27270100
Serial Number: 1234567
MAC Address: 00:04:DF:00:00:00
Net: Initializing Fman
SF: Detected n25q64 with page size 256 Bytes, erase size 4 KiB, total 8 MiB
Fman1: Uploading microcode version 106.4.17
FM1@DTSEC4 [PRIME]
SF: Detected n25q64 with page size 256 Bytes, erase size 4 KiB, total 8 MiB
Press CTRL-C to stop booting: (3 seconds to boot)
Password:
```

Há duas formas de reset de senha. No primeiro caso, é feito o reset total da configuração do equipamento. No segundo, a configuração é mantida e é alterada apenas a senha do usuário admin para o valor *default*.

2.2.1 Reset de configuração

Após acessar o U-Boot, entre com os comandos abaixo. O equipamento irá iniciar com a configuração de fábrica e com a senha padrão do usuário admin.

```
setenv load-factory-config 1
save
boot
```

2.2.2 Reset de senha do usuário admin

Após acessar o U-Boot, entre com os comandos abaixo. O equipamento irá iniciar sem alterações de configuração e com a senha padrão do usuário admin.

```
setenv reset-admin-password 1
save
boot
```

2.3 Configuração das Licenças

Uma licença é necessária para algumas operações do equipamento. Para verificar quais licenças o seu equipamento suporta utilize o comando **show license**. Para obter as licenças entre em contato com o time de Suporte da DATACOM informando o número de série e o endereço MAC do equipamento. Estas informações podem ser obtidas no comando **show inventory** conforme abaixo:

```
show inventory
..
Chassis/Slot      : 1/1
Product model    : 24GX+4XS+2QX
Part number      : 800.5184.01
Serial number    : 4461034
Product revision : 1
PCB revision     : 1
Hardware version : 0
Manufacture date : 01/08/2018
Manufacture hour : 12:00:00
Operat. temp.    : 0 - 55 Celsius degrees
..
Base MAC address : 00:04:df:5c:0c:77
..
```

2.3.1 Habilitando a licença MPLS

Os próximos passos irão demonstrar como ativar a licença MPLS.



A ativação é feita após o commit, não sendo necessário reiniciar o equipamento.

```
config
license mpls enabled key
(<string>): *****
commit
```



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

2.3.2 Habilitando a licença das portas 100 Gigabit

Os próximos passos irão demonstrar como ativar a licença para todas ou um determinado número de portas 100 Gigabit.



A ativação é feita após o commit, não sendo necessário reiniciar o equipamento.

```
config
license speed-100g-ports enabled key
(<string>): *****
commit
```



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

2.3.3 Verificando o Licenciamento

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



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

```
show license
Feature   Status   Number of Licenses
-----   -
mpls     enabled  N/A
speed-100g-ports  enabled  6
```

2.4 Configuração do Product Model

O DmOS suporta a configuração do Product Model para alterar a configuração de portas caso seja suportado pelo equipamento. Para verificar se o equipamento suporta esta configuração utilize o comando **card-model**.



Alterar o Product Model reinicia o equipamento e retorna para a configuração de fábrica.



Esta feature somente é suportada no DM4270 24XS e o card-model padrão é **24XS+3CX**.

2.4.1 Configuração de Product Model no DM4270 24XS

Product Model	Configurações suportadas
24XS+3CX	24 ten-gigabit-ethernet + 3 hundred-gigabit-ethernet
24XS+4QX	24 ten-gigabit-ethernet + 4 forty-gigabit-ethernet

Mapeamento de portas no DmOS:



Na versão de firmware 5.12.0, o equipamento suporta a operação de até 3 portas 100G (3CX), desta forma operando com os card-models abaixo. Em versões anteriores o modelo suportava até 2 portas 100G (2CX).

- **24XS+3CX**: DmOS usa a porta hundred-gigabit-ethernet 1/1/1, hundred-gigabit-ethernet 1/1/2 e hundred-gigabit-ethernet 1/1/3 como portas 40 ou 100 Gigabit.
- **24XS+4QX**: DmOS usa a hundred-gigabit-ethernet 1/1/1, hundred-gigabit-ethernet 1/1/2, forty-gigabit-ethernet 1/1/1 e forty-gigabit-ethernet 1/1/2 como portas 40 Gigabit.

Exemplo:

```
DmOS# card-model 24XS+4QX
Warning: The system will automatically reboot and load the factory configuration. Once initiated,
this process cannot be interrupted.
Proceed with this action? [yes,N0]
```

2.5 Configuração dos Recursos de Encaminhamento

O DmOS suporta a configuração dos recursos de encaminhamento para definir um profile de utilização para aumentar a quantidade de endereços da tabela MAC ou para aumentar a quantidade de rotas suportadas pelo equipamento.

Para verificar se o equipamento suporta esta configuração utilize o comando **forwarding-resources profile**.



Esta feature somente é suportada nas plataformas DM4270, DM4775 e DM4380.

O usuário pode escolher entre três profiles de encaminhamento.

- **default**: Perfil padrão configurado em cada plataforma.
- **extended-ip**: Perfil utilizado em cenários com escalabilidade de rotas.
- **extended-mac**: Perfil utilizado em cenários com escalabilidade de endereços MAC.

No exemplo abaixo é possível verificar os três tipos de profile disponíveis para a plataforma DM4270.

```
DM4270# forwarding-resources profile
Possible completions:
default      128000 L2 MAC / 128000 IPv4 / 32000 IPv6/64 / 4000 IPv6/128
extended-ip  32000 L2 MAC / 168000 IPv4 / 42000 IPv6/64 / 10000 IPv6/128
extended-mac 288000 L2 MAC / 16000 IPv4 / 4000 IPv6/64 / 1000 IPv6/128
```

Abaixo o procedimento para configurar o profile:



É necessário reiniciar o equipamento após realizar essa configuração.

```
DM4270# forwarding-resources profile extended-mac
This change will take effect on next reboot.
DM4270# reboot
```

Para verificar o perfil aplicado:

```
DM4270# show forwarding-resources
Profile Name  MAC      IPv4      IPv6/64  IPv6/128  Running  Startup
-----
default      128000   128000   32000    4000      false   false
extended-ip  32000    168000   42000    10000     false   false
extended-mac 288000   16000    4000     1000      true    true
```

A tabela exibe na coluna **Running**, a flag **true**. A coluna **Startup** exibe a flag **true** para informar qual a configuração que estará ativa após o próximo reboot.

Internamente, a seleção dos profiles gerencia a alocação da UFT (Unified Forwarding Table), que compartilha recursos de Hardware para MACs, IPv4, IPv6/64 e IPv6/128. É necessário entender seu funcionamento básico para saber como os valores atribuídos para cada profile se relacionam e como os limites indicados podem ser alcançados.

A partição reservada para MACs é fixa para cada profile, podendo ser preenchida completamente sem alterar as demais capacidades.

Existem outras duas partições para alocação de endereços IP:

- **partição ip-a:** Armazena endereços IPv4 e IPv6/64
 - Suporta ser preenchida com a capacidade máxima de rotas IPv4 ou a capacidade máxima de rotas IPv6/64. Uma combinação entre as duas também pode ser estabelecida, mas não é possível atingir os limites máximos simultaneamente. Endereços IPv6/64 ocupam o dobro do espaço de um endereço IPv4. Em alguns produtos, quando esta partição enche, a partição ip-b passa a armazenar endereços IPv4 ou IPv6/64, reduzindo assim a capacidade IPv6/128.
- **partição ip-b:** Armazena endereços IPv6/128
 - Atinge sempre a capacidade máxima indicada no profile. No entanto, nos produtos em que esta partição pode compartilhar endereços IPv4 ou IPv6/64, o limite pode não estar disponível se as restrições indicadas para a partição ip-a não forem respeitadas.

2.6 Configuração da Gerência

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.



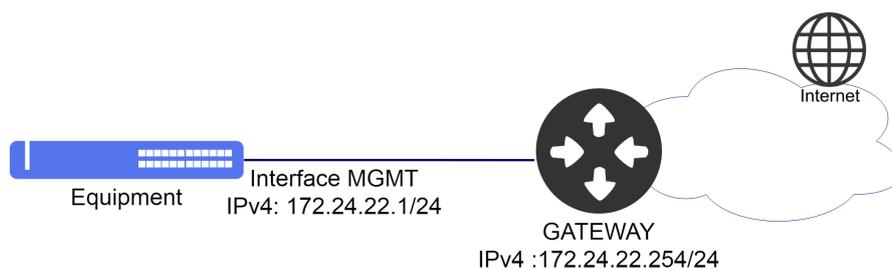
É possível configurar o gerenciamento do equipamento com endereçamento IPv4 ou IPv6.



É possível configurar o gerenciamento do equipamento com a **VRF mgmt**. Nesta aplicação apenas serviços básicos como SSH, Telnet, Autenticação Local e atualização de firmware são suportados. Consulte como configurar VRF para proceder com esta configuração.

2.6.1 Configurando a Gerência Out-of-Band

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



Exemplo de Gerenciamento Out-of-Band

Suponha que o usuário deseje utilizar a Interface MGMT com o endereço IPv4 **172.24.22.1/24** e com o gateway padrão **172.24.22.254/24**. O procedimento a seguir apresentará como realizar esta configuração a partir do modo de configuração:

```
config
interface mgmt 1/1/1
  ipv4 address 172.24.22.1/24
  !
!
router static
  address-family ipv4
    0.0.0.0/0 next-hop 172.24.22.254
  commit
```

2.6.2 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.

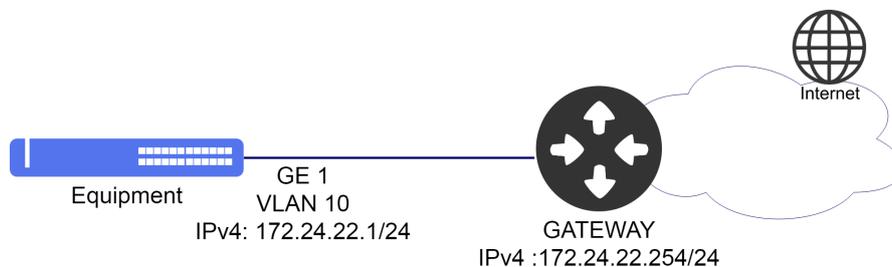


É possível configurar o gerenciamento do equipamento com endereçamento IPv4 ou IPv6.



É possível configurar o gerenciamento do equipamento utilizando endereço IPv4 secundário. Endereço IPv6 secundário não é suportado.

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



Exemplo de Gerenciamento In-Band

Suponha que o usuário deseje usar a **VLAN 10** para gerenciamento In-Band através da interface **gigabit-ethernet 1/1/1**

com endereço IPv4 **172.24.22.1/24** e gateway padrão **172.24.22.254**. O procedimento a seguir apresentará como realizar esta configuração:

```
config
dotq1 vlan 10
name In_Band-Management
interface gigabit-ethernet-1/1/1
!
!
interface l3 in-band
ipv4 address 172.24.22.1/24
lower-layer-if vlan 10
!
!
router static
address-family ipv4
0.0.0.0/0 next-hop 172.24.22.254
commit
```

2.7 Configuração do Acesso a CLI

O SSH (Secure Shell) e Telnet são protocolos utilizados para acesso ao terminal do equipamento. Por razões de segurança, o padrão de fábrica do DmOS é o protocolo SSH server habilitado e o Telnet server desativado.



O DmOS suporta o SSHv2 com criptografia de chave pública RSA (Rivest, Shamir and Adelman) e DAS (Digital System Algorithm).

2.7.1 Gerando as chaves SSH

Os próximos passos irão demonstrar como gerar a chave RSA.

```
ssh-server generate-key rsa size <1024-2048>
Really want to do this? [yes,no] yes
Generated keys
```

2.7.2 Habilitando o suporte a versões antigas do SSH

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.

```
config
ssh-server legacy-support
```

2.7.3 Configurando o número máximo de conexões SSH e Telnet

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.

```
config
ssh-server max-connections 10
telnet-server max-connections 10
commit
```

2.7.4 Habilitando o serviço Telnet

Por segurança, o Telnet server está desativado. Caso o usuário queira ativar o serviço de Telnet, deverá executar o seguinte procedimento:

```
config
telnet-server enabled
commit
```

É possível alterar a porta do servidor Telnet, a configuração abaixo altera a porta do servidor Telnet para 2323.

```
config
telnet-server port 2323
commit
```



Após executar o commit para aplicar a configuração de alteração de porta, caso haja alguma sessão de Telnet aberta será encerrada automaticamente, sendo necessário acessar o equipamento novamente utilizando a nova porta configurada.

2.8 Configuração do Hostname

2.8.1 Configurando o Hostname

Suponha que o usuário deseja utilizar o nome **DATAKOM-ROUTER-R1** para identificar o equipamento. O procedimento a seguir apresentará como realizar esta configuração:

```
config
hostname DATAKOM-ROUTER-R1
commit
```

2.9 Configuração do Banner

O banner de login é exibido antes do login ao equipamento.

2.9.1 Configurando o Banner em linha Única

É possível configurar o banner em apenas uma linha de comando, como abaixo.

```
config
banner login "\nAcesso Restrito\n"
commit
```



O caractere “\” (contrabarra) é utilizado como caractere de escape. Para exibir uma “\”, é necessário inserir “\\”.



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

2.9.2 Configurando o Banner em múltiplas linhas

Também é possível configurá-lo em múltiplas linhas.

```
config
banner login
(<Hit <cr> to enter in multi-line mode. Alternatively, enter a text between
double quotes. Remember to insert a line break at the end. See command
reference for examples. Maximum length of 3240 characters.>)
(\nAcesso restrito\n):
[Multiline mode, exit with ctrl-D.]
>
> Acesso restrito
> <CTRL-D>
commit
```



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

2.9.3 Verificando o Banner

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



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

```
show banner login
```

2.10 Configuração do Relógio e Data do Sistema

2.10.1 Configurando o Relógio 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.

Suponha que o usuário deseje configurar a data para **20 de Janeiro de 2017** e o horário para as **10 horas, 5 minutos e 30 segundos**. O procedimento a seguir apresentará como realizar esta configuração:

```
set system clock 20170120 10:05:30
```

2.10.2 Configurando o Timezone

Suponha que o usuário deseje configurar o **timezone** para -3.

```
config  
clock timezone BRA -3  
commit
```



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

2.10.3 Verificando o Relógio do Sistema

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



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

```
show system clock
```

3 Gerenciamento de Rede

O DmOS fornece alguns protocolos e ferramentas para gerenciamento da rede.

Este capítulo contém as seguintes seções:

- Configuração do LLDP
- Configuração do Sntp
- Configuração do Syslog
- Configuração do SNMP
- Ping
- Traceroute
- SSH Client
- Telnet Client

3.1 Configuração do LLDP

O protocolo Link Layer Discovery Protocol (LLDP) é utilizado para anunciar informações de interface e gerenciamento a vizinhos conectados diretamente a um equipamento.

3.1.1 Configurando o LLDP entre dois vizinhos

Abaixo, um exemplo de como habilitar o LLDP na interface gigabit-ethernet 1/1/1.

```
lldp
interface gigabit-ethernet-1/1/1
  admin-status tx-and-rx
  notification
!
commit
```



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

3.1.2 Verificando o LLDP

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



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

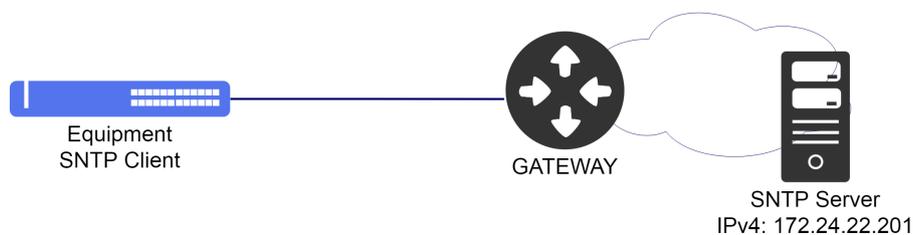
```
show lldp brief
show lldp statistics
show lldp local
debug enable proto-lldp
```

3.2 Configuração do 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.

3.2.1 Configurando o SNTP

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



Exemplo de configuração SNTP

Suponha que o usuário deseje configurar o equipamento como cliente SNTP e utilizar um servidor SNTP que possui o endereço IPv4 **172.24.22.201**. O procedimento a seguir apresentará como realizar esta configuração:

```
config
 sntp client
 sntp server 172.24.22.201
 commit
```

É possível associar o SNTP a uma interface L3 específica para permitir que o SNTP opere em VRFs. A configuração abaixo associa o servidor SNTP à interface L3 CUST-A-VLAN20, que está associada à VRF cust-a. Requisições SNTP serão enviadas nesta VRF utilizando como origem o endereço IP da interface especificada.

```
config
 sntp source interface l3-VRF-CUST-A
 sntp client
 sntp server 192.168.10.200
 !
 vrf cust-a
 !
 interface l3 CUST-A-VLAN20
 vrf cust-a
 lower-layer-if vlan 20
 address 192.168.20.1/24
 !
 commit
```



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

3.2.2 Configurando o SNTP com Autenticação

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

```
config
 sntp authenticate
 sntp client
 sntp authentication-key 1 md5 "SERVER-KEY"
 sntp server 172.24.22.201 key 1
commit
```



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

3.2.3 Verificando o SNTP

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



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

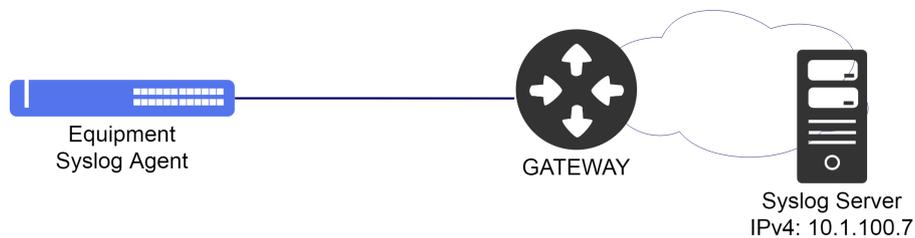
```
show sntp
```

3.3 Configuração do Syslog

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.

3.3.1 Configurando o Syslog Remoto

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



Exemplo de configuração do Syslog Remoto

Suponha que o usuário deseja utilizar um servidor **syslog remoto** que possui o endereço IPv4 **10.1.100.7**. O procedimento a seguir apresentará como realizar esta configuração:

```
config
log syslog 10.1.100.7
commit
```

É possível alterar a porta do serviço Syslog, a configuração abaixo altera a porta do serviço Syslog no servidor 10.1.100.7 de 514 (porta padrão) para 9000.

```
config
log syslog 10.1.100.7 port 9000
commit
```

É possível associar o serviço Syslog com uma VRF específica. A configuração abaixo associa o servidor Syslog 10.1.100.7 à VRF de cliente *vrf_client_a*.

```
config
log syslog 10.1.100.7 vrf vrf_client_a
commit
```



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

3.3.2 Verificando o Syslog

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



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

```
show log
```

3.4 Configuração do 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.

Por padrão, o DmOS possui na configuração de fábrica diversos comandos necessários para a utilização do SNMP. Os tópicos abaixo irão demonstrar como habilitar os recursos necessários para alguns dos cenários atendidos com SNMP no DmOS.

3.4.1 Configurando o SNMPv2

O cenário abaixo será usado para demonstrar as configurações do SNMP.



Exemplo de cenário com SNMP

A configuração abaixo demonstra como habilitar o agente SNMPv2 para responder a requisições. Será utilizada a comunidade **datacom** para consultar o agente.

```
config
snmp agent enabled
snmp agent version v2c
snmp community datacom
  sec-name datacom
!
snmp vacm group datacom
  member datacom
  sec-model [ v2c ]
!
access "" v2c no-auth-no-priv
  read-view root
  write-view root
!
snmp vacm view root
  subtree 1.3
  included
!
commit
```

Após aplicar a configuração acima, o agente irá responder requisições SNMPv2 através da *community datacom*.

Caso necessário é possível atribuir uma VRF utilizando o contexto do SNMP em vez da VRF global. Neste caso as informações retornadas serão as mesmas da VRF global, exceto na parte do BGP que será específica da VRF com nome *vrf-client-datacom* atribuída na configuração do contexto.

```
config
snmp agent enabled
snmp agent version v2c
snmp agent context vrf-client-datacom
snmp community datacom
  sec-name datacom
  context-map vrf-client-datacom
!
snmp vacm group datacom
  member datacom
  sec-model [ v2c ]
!
access vrf-client-datacom v2c no-auth-no-priv
  read-view root
  write-view root
!
snmp vacm view root
  subtree 1.3
  included
!
commit
```

Após aplicar a configuração acima, o agente irá responder requisições SNMPv2 através da *community datacom* na VRF *vrf-client-datacom*.



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

3.4.2 Configurando o SNMPv3

Para habilitar o agente SNMPv3 para responder a requisições de forma segura através do **usuário dmview** com senha de autenticação e senha de privacidade utilizando o modo de criptografia abaixo:

- Autenticação SHA com senha **dmview123-sha**.
- Privacidade AES com senha **dmview123-aes**.

Deverá realizar a seguinte configuração:

```
config
snmp agent enabled
snmp agent version v3
!
snmp vacm group VACM-SNMPv3
  member dmview
  sec-model [ usm ]
!
access "" usm auth-priv
  read-view root
  write-view root
!
snmp vacm view root
  subtree 1.3
  included
!
snmp usm local user dmview
  auth sha password "dmview123-sha"
  priv aes password "dmview123-aes"
!
commit
```

Caso necessário é possível atribuir uma VRF utilizando o context do SNMP em vez da VRF global. Neste caso as informações retornadas serão as mesmas da VRF global, exceto na parte do BGP que será específica da VRF com nome *vrf-client-datacom* atribuída na configuração do context.



Para acessar os objetos no SNMPv3 utilizando o context é necessário especificar o context na ferramenta ou comando utilizado nos servidores.

```
config
snmp agent enabled
snmp agent version v3
snmp agent context vrf-client-datacom
!
snmp vacm group VACM-SNMPv3
  member dmview
  sec-model [ usm ]
!
access vrf-client-datacom usm auth-priv
  read-view root
  write-view root
!
snmp vacm view root
  subtree 1.3
  included
!
snmp usm local user dmview
  auth sha password "dmview123-sha"
  priv aes password "dmview123-aes"
!
commit
```



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

3.4.3 Configurando o envio de notificações SNMP

É possível configurar o SNMP para envio de mensagens de notificação sobre eventos ocorridos no sistema. Essas mensagens podem ser de dois tipos:

- **Traps:** Mensagens são enviadas mas não recebem confirmação.
- **Inform:** Mensagens são enviadas e recebem confirmação.

Traps

Para que o equipamento envie **traps** ao servidor **172.22.1.152**, a configuração abaixo pode ser utilizada.



Todas as traps estão habilitadas por padrão podendo desabilitar conforme necessidade.

```
config
!
snmp notify std_v2_trap
tag std_v2_trap
type trap
!
snmp target SNMP-Trap-Server
ip 172.22.1.252
tag [ std_v2_trap ]
v2c sec-name public
!
commit
```

Se necessário, o target SNMP pode ser associado a uma VRF.

```
config
snmp target SNMP-Trap-Server
vrf myvrf
ip 172.22.1.252
tag [ std_v2_trap ]
v2c sec-name public
!
commit
```

O usuário pode desabilitar algum tipo de trap conforme o exemplo abaixo.

```
config
!
no snmp traps login-success
!
commit
```



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

Informs

Para que o equipamento envie **informs** ao servidor SNMPv2, a configuração abaixo pode ser utilizada.

```
config
!
snmp notify std_v2_inform
tag std_v2_inform
type inform
!
snmp target SNMP-Notify-Server
ip 172.22.1.252
tag [ std_v2_inform ]
v2c sec-name public
!
commit
```

Para que o equipamento envie **informs** ao servidor SNMPv3, a configuração abaixo pode ser utilizada.

```
config
!
snmp notify std_v3_inform
tag std_v3_inform
type inform
!
snmp target SNMP-Notify-Server
ip 172.22.1.252
tag [ std_v3_inform ]
engine-id 12:34:00:00:00:00:00:00:00:00:00
usm user-name dmview
usm sec-level auth-priv
!
snmp usm remote 12:34:00:00:00:00:00:00:00:00:00
user dmview
auth sha password "dmview123-sha"
priv aes password "dmview123-aes"
!
commit
```



Para que o servidor SNMPv3 receba as notificações, é necessário ter configurado na base de dados do servidor o nome do **usuário** e o **engineID**. Caso contrário o servidor irá rejeitar as mensagens de notificação.

Se necessário, o target SNMP pode ser associado a uma VRF.

```
config
snmp target SNMP-Trap-Server
vrf myvrf
ip 172.22.1.252
tag [ std_v3_inform ]
engine-id 12:34:00:00:00:00:00:00:00:00:00
usm user-name dmview
usm sec-level auth-priv
!
commit
```



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

3.4.4 Configurando parâmetros do SNMP

Neste tópico serão demonstrados como configurar ou alterar parâmetros que são opcionais para o usuário como:

- Versão do agente SNMP.
- Endereço IP do agente SNMP.
- Interface do agente SNMP.
- Comunidade SNMP.
- Informações de sistema para *MIB-2 System*.
- Usuários.
- Controle de acesso.

Alterando a versão do agente

Na configuração padrão do SNMP o agente nas versões v2 e v3 já estão configurados. Caso o usuário deseje alterar a configuração do agente, removendo o agente v3, por exemplo, a configuração abaixo deve ser aplicada.

```
config
no snmp agent version v3
commit
```

A partir desse momento as consultas SNMPv3 não serão mais respondidas pelo agente.

Especificando o IP de origem do agente SNMP

É possível especificar qual o endereço IPv4 ou IPV6 o agente SNMP usará como endereço de origem, configurando o **agent ip**.



O endereço IP utilizado deve estar configurado no equipamento.

```
config
snmp agent ip <IP>
commit
```

Especificando a interface do agente SNMP

É possível especificar em quais interfaces L3 o SNMP deve receber requisições através da configuração **listen interface**. Desta forma, é possível utilizar o SNMP em VRFs.

```
config
snmp agent listen interface <l3-myintf1>
snmp agent listen interface <l3-myintf2>
commit
```

Configurando comunidades

Na configuração padrão do SNMP a comunidade **public** já está configurada com permissão de **leitura, escrita e notificação** para SNMPv2. Por questões de segurança é recomendado alterar a comunidade padrão. Caso o usuário deseje remover ou incluir uma nova comunidade os passos seguintes irão demonstrar como realizar estas operações.

Removendo a comunidade padrão (**public**):

```
config
no snmp community public
no snmp vacm group public
commit
```

Configurando uma comunidade **datacom-ro** com **permissão somente leitura**:

```
config
snmp community datacom-ro
  sec-name datacom-ro
!
snmp vacm group datacom-ro
  member datacom-ro
  sec-model [ v2c ]
!
access "" v2c no-auth-no-priv
  read-view root
!
commit
```

Configurando uma comunidade **datacom-rw** com **permissão de leitura e escrita**:

```
config
snmp community datacom-rw
  sec-name datacom-rw
!
snmp vacm group datacom-rw
  member datacom-rw
  sec-model [ v2c ]
!
access "" v2c no-auth-no-priv
  read-view root
  write-view root
!
commit
```

Configurando informações de sistema

Algumas informações do sistema podem ser configuradas para serem informadas através do agente SNMP usando a **MIB-2 System**. Caso o usuário deseje incluir informações de contato e localização, por exemplo, a configuração abaixo deve ser aplicada:

```
config
snmp system contact datacom@datacom.com.br
snmp system location Eldorado-RS
commit
```

A partir desse momento os objetos **sysContact** e **sysLocation** da MIB-2 System irão retornar as informações configuradas.

Configurando usuários

Quando um agente SNMPv3 é utilizado, é necessário configurar os usuários que irão responder as requisições. Para configurar o usuário **datacom** com autenticação e privacidade, a configuração abaixo deve ser aplicada:

```
config
snmp usm local user datacom
  auth sha password "datacom-sha"
  priv aes password "datacom-aes"
commit
```

Configurando controle de acesso

Na configuração padrão do SNMP, o grupo de controle de acesso **snmp vacm view root** permite que todos os objetos (OIDs) da base local respondam a partir do ramo 1.3 da MIB. Caso o usuário deseje criar um novo nível de acesso para permitir consultas a partir do ramo 1.3.6.1.4.1 (private enterprises) por exemplo, a configuração abaixo deve ser aplicada:

```
config
snmp vacm view ENTERPRISE
  subtree 1.3.6.1.4.1
  included
commit
```

A partir desse momento a view ENTERPRISE pode ser aplicada no grupo de acesso.

```
config
snmp vacm group datacom
  member datacom
  sec-model [ v2c ]
  !
  access "" v2c no-auth-no-priv
  read-view ENTERPRISE
  !
  !
snmp vacm view ENTERPRISE
  subtree 1.3.6.1.4.1
  included
commit
```



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

3.4.5 Verificando o SNMP

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



Para maiores detalhes sobre as saídas dos comandos, consultar o [Command Reference](#).

```
show running-config snmp
```

3.5 Ping

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



O usuário deve usar a palavra-chave **do** antes do comando caso estiver no modo de configuração.

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_seq=1 ttl=61 time=2.15 ms
64 bytes from 5.178.41.1: icmp_seq=2 ttl=61 time=2.06 ms
64 bytes from 5.178.41.1: icmp_seq=3 ttl=61 time=2.12 ms
64 bytes from 5.178.41.1: icmp_seq=4 ttl=61 time=2.27 ms
64 bytes from 5.178.41.1: icmp_seq=5 ttl=61 time=2.07 ms
--- 5.178.41.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.065/2.139/2.272/0.074 ms
```

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

```
ping6 2002:c0a8:fe05::6
PING 2002:c0a8:fe05::6(2002:c0a8:fe05::6) 56 data bytes
64 bytes from 2002:c0a8:fe05::6: icmp_seq=1 ttl=62 time=7.94 ms
64 bytes from 2002:c0a8:fe05::6: icmp_seq=2 ttl=62 time=4.66 ms
64 bytes from 2002:c0a8:fe05::6: icmp_seq=3 ttl=62 time=5.05 ms
64 bytes from 2002:c0a8:fe05::6: icmp_seq=4 ttl=62 time=5.00 ms
64 bytes from 2002:c0a8:fe05::6: icmp_seq=5 ttl=62 time=6.84 ms
--- 2002:c0a8:fe05::6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 4.664/5.903/7.948/1.274 ms
```

Pode-se especificar um endereço IP como origem dos pacotes ICMP utilizando o parâmetro **source**. Pode-se também especificar uma interface de origem.

Para realizar ping para endereços em uma VRF (apenas IPv4), pode ser utilizado o parâmetro **vrf** ou especificar uma interface associada à VRF no parâmetro **source**.

3.6 Traceroute

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.



O usuário deve usar a palavra-chave **do** antes do comando caso estiver no modo de configuração.

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, 38 byte packets
 1 192.168.48.3 (192.168.48.3)  2.029 ms  4.345 ms  1.751 ms
 2 192.168.48.1 (192.168.48.1)  2.842 ms  2.488 ms  3.226 ms
 3 192.168.254.22 (192.168.254.22)  3.582 ms  3.403 ms  3.622 ms
 4 192.168.84.22 (192.168.84.22)  2.306 ms  1.802 ms  2.264 ms
 5 5.178.41.1 (5.178.41.1)  2.219 ms  1.651 ms  54.376 ms
```

Pode-se especificar um endereço IP como origem dos pacotes utilizando o parâmetro **source**. Pode-se também especificar uma interface de origem.

Para realizar traceroute para endereços em uma VRF, pode ser utilizado o parâmetro **vrf** ou especificar uma interface associada à VRF no parâmetro **source**.

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

```
traceroute6 2002:c0a8:fe05::6
traceroute to 2002:c0a8:fe05::6 (2002:c0a8:fe05::6) from 1997::c0a8:3002,
30 hops max, 16 byte packets
 1 1997::c0a8:3001 (1997::c0a8:3001)  13.877 ms  2.298 ms  2.249 ms
 2 2001::c0a8:3001 (2001::c0a8:3001)  3.64 ms  2.969 ms  2.869 ms
 3 2002:c0a8:fe05::6 (2002:c0a8:fe05::6)  4.444 ms  3.624 ms  5.787 ms
```

3.7 SSH Client

É possível acessar outros equipamentos utilizando o protocolo SSH a partir de um equipamento com DmOS.



O usuário deve usar a palavra-chave **do** antes do comando caso estiver no modo de configuração.

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
```

3.8 Telnet Client

É possível acessar outros equipamentos utilizando o protocolo TELNET a partir de um equipamento com DmOS.



O usuário deve usar a palavra-chave **do** antes do comando caso estiver no modo de configuração.

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
```

4 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 CFM
- Configuração do EFM
- Configuração do RDM
- Configuração do TWAMP
- Configuração do sFlow
- Configuração do Traffic Loop
- Configuração do agendamento de tarefas
- Configuração de Contadores

4.1 Configuração do CFM

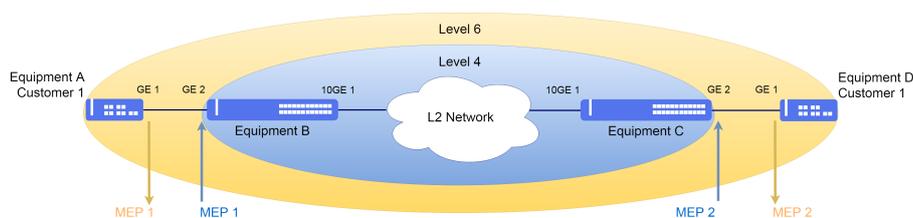
O protocolo CFM (Connectivity Fault Management) é definido no padrão **IEEE 802.1ag** e provê a garantia de caminho completo fim-a-fim, ponto-a-ponto ou numa LAN formada por diversos equipamentos. No CFM, entidades de rede formadas por operadoras de rede, provedores de serviço e clientes finais fazem parte de diferentes domínios de redes administradas por diferentes pessoas. No CFM, os domínios são os MD (Maintenance Domain) que possuem níveis que por sua vez possui uma ou mais MAs (Maintenance Association) que são responsáveis por proteger uma lista de VLANs onde os MEP se comunicarão. Os MEPs (Maintenance End Point) são entidades ativas responsáveis pelo envio das PDUs do CFM.



O DmOS não suporta MIPs.

4.1.1 Configurando o CFM

O cenário abaixo será usado para demonstrar a configuração do CFM entre o Cliente e o Provedor de Serviço.



Exemplo de cenário com CFM

Suponha que o usuário queira realizar as seguintes configurações:

- **Equipment A:** VLAN 2000 para o CFM com a interface gigabit-ethernet-1/1/1 como MEP 1 – Down no nível 6.
- **Equipment B:** VLAN 2000 para CFM com a interface gigabit-ethernet-1/1/2 como MEP 1 – Up no nível 4 e a interface ten-gigabit-ethernet-1/1/1 como Uplink da VLAN 2000.
- **Equipment C:** VLAN 2000 para CFM com a interface gigabit-ethernet-1/1/2 como MEP 2 – Up no nível 4 e a interface ten-gigabit-ethernet-1/1/1 como Uplink da VLAN 2000.
- **Equipment D:** VLAN 2000 para o CFM com a interface gigabit-ethernet-1/1/1 como MEP 2 – Down no nível 6.
- Todos os MEPs configurados com notificação de alarme para todos os erros.

```
!Equipment A
config
dot1q
vlan 2000
interface gigabit-ethernet-1/1/1 tagged
!
!
oam
cfm
md Client
level 6
ma Client
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 2
mep 1
interface gigabit-ethernet-1/1/1
direction down
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit
```

```
!Equipment B
config
dot1q
vlan 2000
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
!
!
oam
cfm
md ServiceProvider
level 4
ma ServiceProvider
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 2
mep 1
interface gigabit-ethernet-1/1/2
direction up
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit
```

```
!Equipment C
config
dot1q
vlan 2000
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
!
!
oam
cfm
md ServiceProvider
level 4
ma ServiceProvider
primary-vlan-id 2000
vlan-list 2000
```

```

cmm-interval 1s
remote-meps 1
mep 2
interface gigabit-ethernet-1/1/2
direction up
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit

```

```

!Equipment D
config
dot1q
vlan 2000
interface gigabit-ethernet-1/1/1 tagged
!
!
oam
cfm
md Client
level 6
ma Client
primary-vlan-id 2000
vlan-list 2000
cmm-interval 1s
remote-meps 1
mep 2
interface gigabit-ethernet-1/1/1
direction down
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit

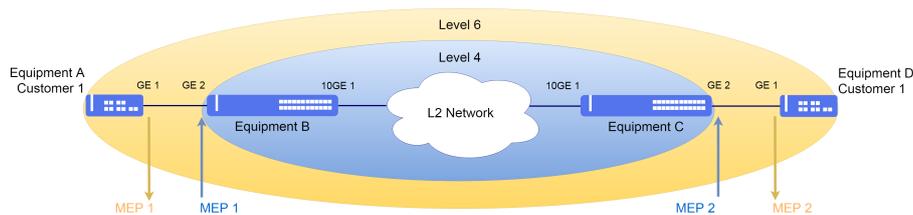
```



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

4.1.2 Configurando o CFM com QinQ

O cenário abaixo será usado para demonstrar a configuração do CFM entre o Cliente e o Provedor de Serviço com QinQ para agregar vários clientes em uma VLAN de serviço.



Exemplo de cenário com CFM

Suponha que o usuário queira realizar as seguintes configurações:

- **Equipment A:** VLAN 2000 para o CFM com a interface gigabit-ethernet-1/1/1 como MEP 1 – Down no nível 6.
- **Equipment B:** VLAN 3000 para o CFM com QinQ na interface gigabit-ethernet-1/1/2 como MEP 1 – Up no nível 4 e a interface ten-gigabit-ethernet-1/1/1 como Uplink da VLAN 3000.
- **Equipment C:** VLAN 3000 para o CFM com QinQ na interface gigabit-ethernet-1/1/2 como MEP 2 – Up no nível 4 e a interface ten-gigabit-ethernet-1/1/1 como Uplink da VLAN 3000.

- **Equipment D:** VLAN 2000 para o CFM com a interface gigabit-ethernet-1/1/1 como MEP 2 – Down no nível 6.
- Todos os MEPs configurados com notificação de alarme para todos os erros.

```

!Equipment A
config
dot1q
vlan 2000
interface gigabit-ethernet-1/1/1 tagged
!
!
oam
cfm
md Client
level 6
ma Client
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 2
mep 1
interface gigabit-ethernet-1/1/1
direction down
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit

```

```

!Equipment B
config
dot1q
vlan 3000
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 untagged
!
!
switchport
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 3000
!
qinq
!
oam
cfm
md ServiceProvider
level 4
ma ServiceProvider
primary-vlan-id 3000
vlan-list 3000
ccm-interval 1s
remote-meps 2
mep 1
interface gigabit-ethernet-1/1/2
direction up
primary-vlan-id 3000
inner-vlan-id 2000
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit

```

```

!Equipment C
config
dot1q
vlan 3000
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 untagged
!
!
switchport
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 3000
!
qinq
!
oam
cfm
md ServiceProvider
level 4

```

```
ma ServiceProvider
primary-vlan-id 3000
vlan-list 3000
ccm-interval 1s
remote-meps 1
mep 2
interface gigabit-ethernet-1/1/2
direction up
primary-vlan-id 3000
inner-vlan-id 2000
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit
```

```
!Equipment D
config
dot1q
vlan 2000
interface gigabit-ethernet-1/1/1 tagged
!
!
oam
cfm
md Client
level 6
ma Client
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 1
mep 2
interface gigabit-ethernet-1/1/1
direction down
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
commit
```



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

4.1.3 Habilitando o Alarm Indication Signal (ETH-AIS)

O Ethernet Alarm Indication Signal ETH-AIS foi proposto pela ITU-Y.1731 para evitar a sinalização da mesma falha repetidas vezes em um cenário com mais de um domínio quando ocorrer falha no domínio interno.

Para que as mensagens de AIS sejam emitidas, é necessário que a configuração seja habilitada no MA. As mensagens de AIS serão enviadas para o domínio com nível imediatamente superior ao seu, ou seja, um domínio externo.

Quando a transmissão é ativada, os quadros AIS são transmitidos quando uma falha é detectada, independente de qualquer configuração de alarme e relatório. Quando a supressão de alarme AIS é ativada, os alarmes não são reportados se os quadros AIS forem recebidos.



A recepção do AIS aceita apenas o parâmetro de supressão de alarme.

Abaixo um exemplo de configuração para transmissão e a recepção de AIS para um determinado MA.

```

oam
 cfm
  md Client
  level 6
  ma Client
  primary-vlan-id 2000
  vlan-list 2000
  ccm-interval 1s
  ais
  transmission
  level 7
  interval 1min
  !
  reception
  alarm-suppression
  !
  !
commit

```



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

4.1.4 Habilitando o Action Block

O CFM suporta a configuração de bloqueio das interfaces quando os MEPs estão em falha. Quando as interfaces estão no estado de bloqueio, os protocolos layer 2 (RSTP, EAPS, ERPS, LLDP) configurados nesta interface são sinalizados alterando para status de falha. Esta feature auxilia a convergência dos protocolos e suporta cenários nos quais os equipamentos não estão diretamente conectados.



A feature somente é suportada no MEP Down.

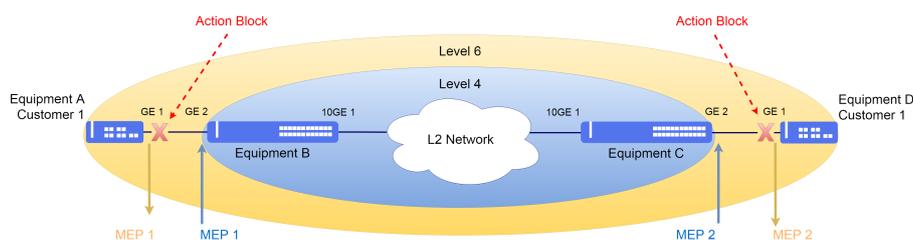


LACP, Link-flap e loopback-detection não são acionados pelo CFM.



Para a aplicação funcionar adequadamente todos os MEPs utilizados precisam suportar o action block para que não haja bloqueio da interface somente em um dos equipamentos.

A figura ilustra o ponto onde ocorre o bloqueio na topologia caso seja configurada a ação de bloqueio da interface do MEP.



Cenário com CFM action block

Abaixo é demonstrada a configuração dos equipamentos A e D com ação de bloqueio no MEP.

```
!Equipment A
config
dot1q
vlan 2000
interface gigabit-ethernet-1/1/1 tagged
!
!
oam
cfm
md Client
level 6
ma Client
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 2
mep 1
interface gigabit-ethernet-1/1/1
direction down
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
fault-action block-port
commit
```

```
!Equipment D
config
dot1q
vlan 2000
interface gigabit-ethernet-1/1/1 tagged
!
!
oam
cfm
md Client
level 6
ma Client
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 1
mep 2
interface gigabit-ethernet-1/1/1
direction down
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
fault-action block-port
commit
```



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

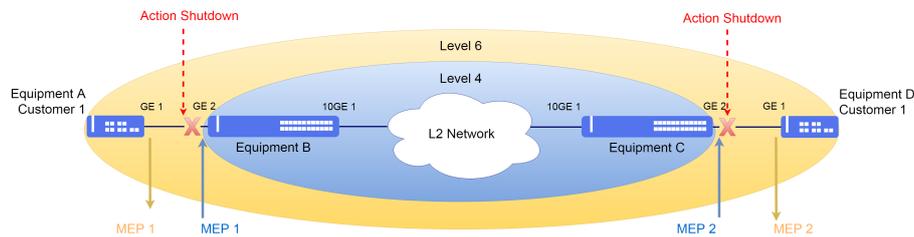
4.1.5 Habilitando o Action Shutdown

O CFM suporta a configuração de shutdown das interfaces quando os MEPs estão em falha. Quando as interfaces estão no estado de shutdown, os outros protocolos configurados nesta interface são sinalizados alterando para status de falha.



A feature somente é suportada no MEP Up.

A figura ilustra o ponto onde ocorre o shutdown na topologia caso seja configurada a ação de shutdown na interface do MEP.



Cenário com CFM action shutdown

Abaixo é demonstrada a configuração dos equipamentos B e C com ação de shutdown no MEP.

```

!Equipment B
config
dot1q
vlan 2000
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
!
!
!oam
cfm
md ServiceProvider
level 4
ma ServiceProvider
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 2
mep 1
interface gigabit-ethernet-1/1/2
direction up
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
fault-action shutdown-port
commit

```

```

!Equipment C
config
dot1q
vlan 2000
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
!
!
!oam
cfm
md ServiceProvider
level 4
ma ServiceProvider
primary-vlan-id 2000
vlan-list 2000
ccm-interval 1s
remote-meps 1
mep 2
interface gigabit-ethernet-1/1/2
direction up
continuity-check
cci-enabled
lowest-fault-priority-defect remote-rdi
fault-action shutdown-port
commit

```



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

4.1.6 Gerenciamento de falhas



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

Protocolo Continuity Check

O protocolo Continuity Check é utilizado para detecção, notificação e recuperação de falhas. Seguem os comandos para verificar o status da troca de comunicação entre os MEPs.

Protocolo Loopback

O protocolo Loopback do CFM é semelhante ao Ping, só que em camada Ethernet, sendo possível verificar as falhas de comunicação entre os MEPs.

```
oam cfm loopback md <md_name> ma <ma_name> mep <local_mep_id> remote-mep <remote_mep_id>
```

Protocolo Linktrace

O protocolo LinkTrace CFM é semelhante ao Traceroute, só que em camada Ethernet, sendo possível descobrir o caminho e isolar as falhas.

```
oam cfm linktrace md <md_name> ma <ma_name> mep <local_mep_id> remote-mep <remote_mep_id>
```

4.1.7 Ethernet Delay Measurement (ETH-DM)

O Ethernet Delay Measurement (ETH-DM) do CFM possibilita medir o delay e jitter entre dois MEPs, podendo estes MEPs serem referentes à circuitos dos clientes, transporte de uma operadora, entre outras possibilidades. Existem dois modos de mensurar o delay que serão explicados a seguir.

O modo one-way é baseado em uma comunicação unidirecional entre dois MEPs usando frames na camada 2. Este delay é calculado com base em dois valores de timestamps adicionados pelo MEP de origem e o MEP de destino. Para estatísticas precisas, é necessário a sincronização de tempo entre os dois equipamentos. Observe que, neste cenário, as estatísticas são consolidadas pelo MEP de destino, o que não é conveniente quando os equipamentos não estão sob a mesma administração.

Por sua vez, a medição de delay two-way que é bidirecional não requer qualquer sincronização de tempo entre os equipamentos envolvidos. Isto é possível porque cada equipamento de rede usa dois timestamps, e as estatísticas são calculadas com base na diferença entre um par de timestamps adicionados pelo mesmo equipamento. Considerando um exemplo com MEP_A e MEP_B, o delay de rede entre eles é calculado da seguinte forma:

- MEP_A: envia um frame DMM, inserindo o primeiro timestamp (TX_A)
- MEP_B: recebe o frame DMM, inserindo o segundo timestamp (RX_B)
- MEP_B: cria o frame DMR, baseado no DMM recebido, inserindo o terceiro timestamp (TX_B)
- MEP_A: recebe o frame DMR, inserindo o último timestamp (RX_A)

O equipamento de rede que contém o MEP_A mensura o delay da rede da seguinte forma:

$$Delay = RX_A - TX_A - (TX_B - RX_B)$$



No DmOS somente é suportado o modo two-way do ETH-DM.

Para mensurar o delay sob demanda use o comando a seguir:

```
oam cfm delay-measurement md <md_name> ma <ma_name> mep <local_mep_id> remote-mep <remote_mep_id>
```



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

Habilitando a probe Ethernet Delay Measurement

O CFM suporta a configuração da probe Ethernet Delay Measurement (ETH-DM) para periodicamente executar o comando de delay measurement armazenando os resultados.

Abaixo é demonstrada a configuração da probe partindo da premissa que o CFM já esteja configurado no equipamento.

```
config
oam
 cfm
  delay-measurement probe 1
    md <md_name>
    ma <opér_name>
    mep <local_mep_id>
    remote-mep <remote_mep_id>
    session 1
    pcp 7
  !
!
!
!
commit
```

O resultado da probe pode ser coletado por SNMP. Para obter as MIBs do DmOS utilize o procedimento descrito no capítulo [Exportando as MIBs SNMP](#).



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

4.1.8 Verificando o CFM

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



Se alguma interface Ethernet for bloqueada pelo CFM, a sigla **CFM** irá aparecer no campo **Blocked by** do comando **show interface link**.

```
show interface link
show oam cfm
show oam cfm brief
show oam cfm detail
show oam cfm local
show oam cfm remote
show oam cfm statistics
show oam cfm delay-measurement
show oam cfm delay-measurement detail
show oam cfm delay-measurement probe <probe_id>
show oam cfm delay-measurement probe <probe_id> detail
show oam cfm linktrace
show oam cfm linktrace md <md_name> ma <ma_name> mep <local_mep_id>
show alarm
debug enable cfm-ais-rx
debug enable cfm-ais-tx
debug enable cfm-discard
debug enable cfm-dm
debug enable cfm-loopback
debug enable cfm-linktrace
```



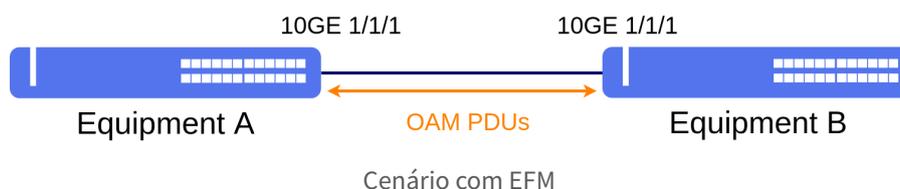
Para maiores detalhes sobre as saídas dos comandos, consulte o **Command Reference**.

4.2 Configuração do EFM

O EFM (Ethernet in the First Mile) é um protocolo de OAM (Operations, Administration and Maintenance) definido no padrão **IEEE 802.3ah** com objetivo de monitorar o enlace, bloqueando a interface assim que a comunicação for interrompida.

4.2.1 Configurando o EFM

O cenário abaixo será usado para demonstrar a configuração do EFM no enlace entre o equipamento A e o equipamento B.



```
config
oam
 efm
  interface ten-gigabit-ethernet-1/1/1
  !
!
```

```
!
commit
```



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

4.2.2 Verificando o EFM

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



Se alguma interface Ethernet for bloqueada pelo EFM, a sigla **EFM** irá aparecer no campo **Blocked by** do comando **show interface link**.

```
show interface link
show oam efm
show oam efm interface <interface>
debug enable proto-efm
```



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

4.3 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 DmOS. No restante deste capítulo, os equipamentos da linha DM4000 serão referenciados genericamente por equipamento intermediário, ou simplesmente **IE**.

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 IE é o dispositivo mestre, o remoto é o dispositivo escravo.
- **Comunicação entre IE e remoto:** O IE 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 IE e o remoto. Vale lembrar que os endereços da rede A.B.0.0/16 não são visíveis externamente ao IE, já que VLAN dos remotos tem como membros unicamente portas nas quais há remotos

conectados.

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.

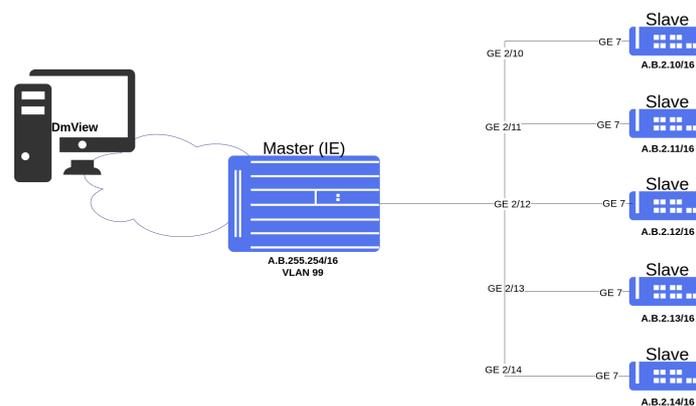


O DmOS não possui suporte para atuar como dispositivo mestre nesta versão.

4.3.1 Configurando o RDM como escravo

No padrão de fábrica do DmOS, o RDM está habilitado em todas as portas dos dispositivos que suportam o protocolo. Se o dispositivo não estiver configurado com o padrão de fábrica, pode ser necessário habilitar o RDM na interface conectada com o mestre (IE).

O cenário abaixo considera que o IE já esteja configurado para operar como RDM mestre.



Cenário RDM

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:



O protocolo EFM deve estar habilitado para o funcionamento do RDM.

```
config
remote-devices interface gigabit-ethernet-1/1/1
oam efm interface gigabit-ethernet-1/1/1 mode passive
commit
```

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, SSH ou Netconf, por exemplo.

Para uso dos protocolos SSH (22) e NETCONF (830) no escravo, é necessário habilitar os serviços no dispositivo mestre.



Entre em contato com o Suporte Técnico DATACOM para verificar a documentação disponível para configuração do dispositivo mestre.



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

4.3.2 Verificando o RDM

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



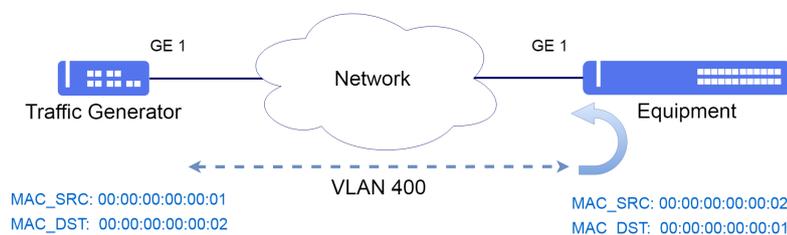
Para maiores detalhes sobre as saídas dos comandos, consultar o [Command Reference](#).

```
debug enable remote-devices
show log component rdm_proto
show remote-devices
show running-config dot1q
show running-config router static
```

4.4 Configuração do Traffic Loop

4.4.1 Configurando o Traffic Loop para Validação do Tráfego L2

O DmOS permite realizar loop de fluxos L2 para atender testes de RFC 2544 ou outro teste de tráfego com objetivo de validar a entrega do circuito para o cliente. A seguir é apresentado um exemplo de configuração da funcionalidade.



Cenário com Traffic loop

Suponha que o usuário queira fazer um loop do tráfego utilizando a VLAN 400 com a interface gigabit-ethernet-1/1/1 como uplink. Os endereços MAC configurados devem respeitar o fluxo de dados configurado no gerador.



Para evitar o risco de perda de acesso a gerencia do equipamento, é recomendado utilizar a funcionalidade de Traffic Loop no modo de gerenciamento exclusivo.

```
config exclusive
dot1q
vlan 400
interface gigabit-ethernet-1/1/1
!
traffic-loop 1
interface gigabit-ethernet-1/1/1
source-mac-address 00:00:00:00:00:01
destination-mac-address 00:00:00:00:00:02
vlan 400
!
```

O usuário deve usar o comando **commit confirmed** para salvar e aplicar a configuração. No exemplo abaixo o commit irá aplicar a configuração temporariamente por 10 minutos. O usuário pode alterar o tempo do commit confirmed caso necessário.

```
commit confirmed 10
```



Não há comandos de troubleshooting para esta funcionalidade.

4.5 Configuração do TWAMP

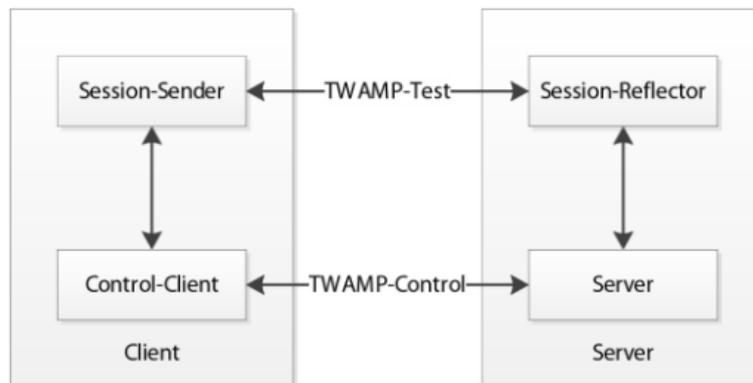
O protocolo TWAMP (Two-Way Active Measurement Protocol) mede parâmetros de desempenho da rede, sendo eles: latência, variação de latência (jitter) e perda de pacotes. A implementação do servidor TWAMP é baseada nas especificações descritas na RFC 5357.

A arquitetura da solução de servidor no TWAMP possui os seguintes componentes lógicos:

- **Session Reflector:** Adiciona informações aos pacotes de teste recebidos e os envia de volta.
- **Server:** Gerencia várias sessões do TWAMP.

A arquitetura da solução de cliente no TWAMP possui os seguintes componentes lógicos:

- **Session Sender:** Cria e envia pacotes de teste TWAMP para o Session Reflector.
- **Control Client:** Envia solicitações ao servidor TWAMP para estabelecer novas sessões.



Arquitetura do TWAMP



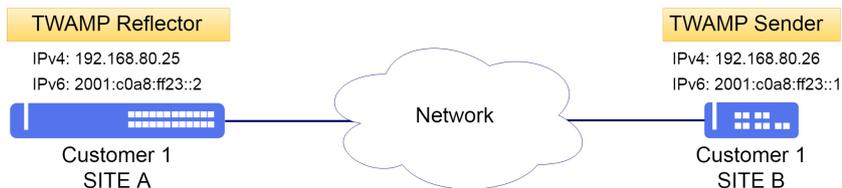
Não há suporte a autenticação/criptografia.



Por padrão, o TWAMP utiliza a porta 862, porém esta pode ser alterada.

4.5.1 Configurando uma sessão TWAMP

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



Cenário TWAMP

Suponha que o usuário queira configurar uma sessão TWAMP através da porta 4000 para monitorar serviços IPv4 e IPv6.

- **Reflector:** IPv4: 192.168.80.25 e IPv6: target-address 2001:c0a8:ff23::2
- **Sender:** IPv4: 192.168.80.26 e IPv6: target-address 2001:c0a8:ff23::1

O procedimento a seguir apresentará como realizar esta configuração:

```
!Equipment REFLECTOR - SITE A
config
oam twamp reflector port 4000
commit
```

```
!Equipment SENDER- SITE B
config
oam
twamp
  sender connection 1
  server-port 4000
  description TWAMP-IPv4
  ipv4 source-address 192.168.80.26
  !
  ipv4 target-address 192.168.80.25
  !
  test-session 1
  description SITE_B-SITE_A
  ipv4 source-address 192.168.80.26
  !
  ipv4 target-address 192.168.80.25
  !
  !
  sender connection 2
  server-port 4000
  description TWAMP-IPv6
  ipv6 source-address 2001:c0a8:ff23::1
  !
  ipv6 target-address 2001:c0a8:ff23::2
  !
  test-session 2
  description SITE_B-SITE_A
  ipv6 source-address 2001:c0a8:ff23::1
  !
  ipv6 target-address 2001:c0a8:ff23::2
  !
  !
commit
```



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

4.5.2 Configurando ACLs no TWAMP Reflector

Também é possível limitar quais clientes podem comunicar-se com o refletor. Na configuração abaixo, apenas os clientes da rede 10.1.15.0/24, endereço IPv4 192.168.80.26 e endereço IPv6 2001:c0a8:ff23::1 serão aceitos pelo refletor.

Caso o usuário não especifique um endereço IP no TWAMP Reflector, todos os endereços serão aceitos.

```
config
oam
twamp
  reflector
  ipv4
  client-address 192.168.80.26
  !
  client-network 10.1.15.0/24
  !
  ipv6
  client-address 2001:c0a8:ff23::1
  !
  !
  !
commit
```



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

4.5.3 Configurando o TWAMP na VRF

Também é possível configurar o TWAMP (Reflector/Sender) na VRF.

Abaixo a configuração do TWAMP Reflector na VRF TWAMP. Para configuração da VRF, consultar o tópico [Configuração da VRF](#).

```
config
oam
twamp
  reflector
  vrf TWAMP
commit
```



Só pode existir uma instância de TWAMP Reflector no equipamento. O TWAMP Reflector não aceita a configuração de mais de uma instância, mesmo em VRFs distintas.

Abaixo a configuração do TWAMP Sender na VRF TWAMP. Para configuração da VRF, consultar o tópico [Configuração da VRF](#).

```
config
oam
twamp
  sender_connection 1
  vrf TWAMP
```



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

4.5.4 Calculando o número máximo de sessões suportadas no TWAMP Reflector

O TWAMP Reflector suporta um número máximo de sessões *simultâneas*. Demais testes acima do valor máximo são rejeitados pelo reflector e o TWAMP Sender irá fazer retries até conseguir estabelecer a sessão.

Para determinar o número máximo de sessões não simultâneas suportadas pelo reflector, deve-se utilizar a fórmula *test-sessions simultâneas x (intervalo entre testes / duração do teste)*.

Como exemplo, para um número máximo de sessões simultâneas de 8, com valor de duração do teste de 20s e intervalo entre testes de 300s, o valor máximo teórico de sessões não simultâneas é $8 \times (300/20) = 120$.



O Descritivo do Produto deve ser consultado para obter os valores de máximas sessões simultâneas de cada plataforma.

4.5.5 Verificando o TWAMP

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



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

```
show oam twamp reflector
show oam twamp reflector connection brief
show oam twamp reflector connection detail
show oam twamp reflector test-session brief
show oam twamp reflector test-session detail
show oam twamp sender connection all brief
show oam twamp sender connection all test-session
show oam twamp sender connection all test-session-statistics
debug enable proto-twamp
```

4.6 Configuração do sFLOW

O sFlow é uma tecnologia para monitoramento dos dados que trafegam na rede. Uma grande vantagem do sFlow é não encaminhar todo o tráfego coletado, em vez disso, o fluxo só encaminha amostras de tráfego para o coletor em uma taxa configurável, reduzindo a carga computacional.

Para o funcionamento do sFlow, são necessários dois componentes:

- **sFlow Agent:** Função atribuída a switches, roteadores, pontos de acesso que amostram pacotes transmitidos e/ou recebidos e encaminham para um coletor sFlow.
- **sFlow Collector:** Função atribuída para analisar as informações recebidas de cada agente sFlow.

Tendo como técnica de amostragem:

- **Flow Sampling:** Baseado na amostra de pacotes, usado para obter informações do conteúdo do pacote como protocolos e etc.
- **Counter sampling:** Baseado na amostra de tempo, usado para obter estatísticas de interfaces.



É suportado somente Flow Sampling.



É permitido configurar apenas um sFlow collector.



No tráfego de saída só serão amostrados pacotes unicast.

4.6.1 Configurando o sFLOW

Suponha que o usuário deseje monitorar os fluxos de dados que trafegam através da interface gigabit-ethernet-1/1/10.

Abaixo, um exemplo de como configurar o agente sFlow na interface gigabit-ethernet 1/1/10 enviando as amostras para o COLLECTOR-1 na porta 1555. Por padrão a porta do collector é a 6343.

```
config
oam
sflow
  collector COLLECTOR-1
  ipv4 172.22.107.14
  port 1555
!
interface gigabit-ethernet-1/1/10
  flow-sampling-collector COLLECTOR-1
!
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

4.7 Configuração do agendamento de tarefas

É possível agendar a execução de tarefas através da funcionalidade chamada **assistant-task**.

Primeiramente é preciso criar um arquivo com os comandos a serem executados. Para criar um arquivo de comandos, consultar o tópico **Editando Arquivos** no capítulo [Gerenciamento dos Arquivos](#).

Também é possível criar o arquivo em outro equipamento e posteriormente importar para ser executado.

O arquivo deve ser copiado para o equipamento através do TFTP ou SCP. Consultar o tópico **Importando os Arquivos** no capítulo [Gerenciamento dos Arquivos](#).



O DmOS suporta apenas arquivos no formato ASCII.

4.7.1 Configurando um reboot automático

No exemplo abaixo, foi agendado um reboot automático para o dia **30/09/2019 as 02:00**.

Foi criado o arquivo **reboot.cli**. O conteúdo pode ser visualizado com o comando **file show**.

```
reboot
```

Em seguida o reboot pode ser agendado. Esta tarefa será executada uma única vez, então foi agendada com o parâmetro **once**.

```
config
assistant-task reboot
action cli-file reboot.cli
schedule once day 30 month 9 hour 2 minute 0
commit
```



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

4.7.2 Configurando backup automático de configuração

Outro uso possível da assistant-task é o backup agendado da configuração.

No exemplo abaixo, foi criado um script que salva a configuração atual no arquivo **config.txt** e o envia ao servidor TFTP **192.168.0.1**. Abaixo o conteúdo do script **config-backup.cli**.

```
show running-config | save overwrite config.txt
copy file config.txt tftp://192.168.0.1/
```



Foi utilizado o parâmetro **overwrite** para salvar o arquivo. Desta forma, caso o arquivo já exista, ele será automaticamente sobrescrito sem confirmação.

A execução do script é agendada para todos os dias as 06:00.

```
config
assistant-task config-backup
action cli-file config-backup.cli
schedule recursive hour 6
commit
```



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

4.7.3 Executando uma tarefa manualmente

Para executar a tarefa manualmente um única vez, pode-se usar o comando abaixo.

```
assistant-task config-backup run-now
```



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

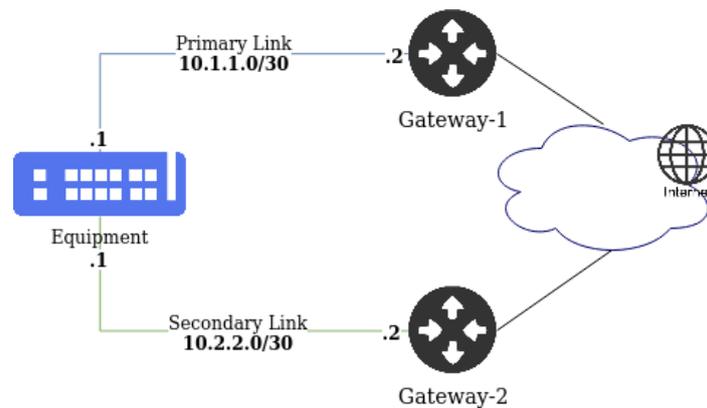
4.7.4 Executando uma tarefa a partir de um padrão

O assistant-task permite realizar ações com base na saída de um comando. Para utilizar esse recurso deve-se utilizar o parâmetro **watch**.

Abaixo um exemplo de uma tarefa para ser executada a cada minuto (sem data/hora especificada), verificando a conectividade do link. Quando ocorre a falha de conectividade no link primário, altera a rota padrão para o link secundário e vice versa. Para esta tarefa será utilizado o script **connectGw1.cli** para habilitar o link primário e o script **connectGw2.cli** para habilitar o link secundário.



Não use "| repeat" ou outros comandos que não tenham retorno, caso contrário, a tarefa do assistente não poderá registrar sua saída e será executada indefinidamente, até que seja interrompida através do comando "logout".



Cenário Assistant Task com watch.

Abaixo o conteúdo do script **connectGw1.cli**.

```
config
no router static address-family ipv4 0.0.0.0/0 next-hop 10.2.2.2
router static address-family ipv4 0.0.0.0/0 next-hop 10.1.1.2
commit
```

Abaixo o conteúdo do script **connectGw2.cli**.

```
config
no router static address-family ipv4 0.0.0.0/0 next-hop 10.1.1.2
router static address-family ipv4 0.0.0.0/0 next-hop 10.2.2.2
commit
```

Criando uma ação de mudança de gateway quando ocorre falha de conectividade no link primário. Repare que o parâmetro

regex define um padrão para corresponder ao retorno do comando configurado em **watch cli-cmd**.

Todas as ações em **watch match** que tiverem correspondência com **watch cli-cmd** serão executadas.

```
config
assistant-task ChangeGW
schedule recursive hour *
schedule recursive minute 0-59
action watch cli-cmd "ping 10.1.1.2 | include loss"
action watch match M0
cli-file connectGw2.cli
regex "received, \+5 errors, 100\% packet loss"
!
action watch match M1
cli-file connectGw1.cli
regex "received, 0\% packet loss"
commit
```



É necessário utilizar o caractere de escape "\\" antes de caracteres especiais para que o regex funcione corretamente.

4.7.5 Verificando o Assistant Task

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



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

```
show assistant-task
show assistant-task <task-name> last-success output
show assistant-task <task-name> last-failure output
```

4.8 Configuração de contadores

Contadores definidos pelo usuário podem ser utilizados para medir tráfego de VLANs ou interfaces.

4.8.1 Configurando contadores de VLANs

No exemplo abaixo, foi configurado um contador para medir o tráfego de entrada (ingress) na VLAN 13.

```
counters
ingress id 1
description "VLAN 13 ingress counter"
type octets
vlan 13
!
```

Para medir o tráfego de saída, configura-se de forma semelhante.

```
counters
 egress id 1
  description "VLAN 13 egress counter"
  type octets
  vlan 13
!
```



Interfaces com VLAN untagged não terão seu tráfego contabilizado.



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

4.8.2 Configurando contadores de interfaces

No exemplo anterior, são medidos os pacotes de todas as interfaces associadas à VLAN 13. Para limitar o contador ao tráfego da VLAN 13 em uma porta específica, pode-se especificá-la como a seguir.

```
counters
 egress id 1
  description "VLAN 13 egress counter"
  type octets
  vlan 13
  interface ten-gigabit-ethernet-1/1/1
!
```

Pode-se utilizar os contadores para medir o tráfego de duas ou mais interfaces ao mesmo tempo. Na configuração abaixo, foi criado um contador que irá medir o tráfego de saída das interface TenGigabitEthernet 1/1/1 e 1/1/2.

```
counters
 egress id 1
  description "Interface egress counter"
  type octets
  interface ten-gigabit-ethernet-1/1/1 ten-gigabit-ethernet-1/1/2
!
```

O valor dos contadores pode ser coletado por SNMP. Para obter as MIBs do DmOS utilize o procedimento descrito no capítulo [Exportando as MIBs SNMP](#).



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

4.8.3 Verificando os Counters

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



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

```
show counters
show counters ingress
show counters ingress id <id>
show counters egress
show counters egress id <id>
```

5 Autenticação de Usuários

O DmOS utiliza níveis de privilégios para determinar quais informações estarão disponíveis para uma conta de usuário. São suportados três níveis de acesso de gerenciamento para usuários: admin, config e audit.

Nível	Descrição
admin	Permite exibir e alterar todos os parâmetros do dispositivo. É um acesso completo de leitura e gravação para todo o dispositivo.
config	Permite algumas funções mais que somente leitura, porém, menos que o nível admin. Permite ao usuário visualizar todos os parâmetros do dispositivo. Permite todos os comandos de configuração, exceto aqueles para fins de administração de dispositivos, como: hostname, SNMP, monitor, RADIUS, SNTP, TACACS+ e Usuários locais.
audit	Permite apenas funções de leitura.

Apenas uma conta de usuário é configurada por padrão no DmOS. O usuário é o **admin** com senha **admin** e possui nível de privilégio **admin**.



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



É recomendado configurar as senhas dos protocolos sempre entre aspas duplas "password". Assim é possível configurar senhas sem problema referente ao uso de caracteres especiais.

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

```
config
aaa user admin password "new-password"
commit
```

Este capítulo contém as seguintes seções:

- Configuração dos Usuário Locais
- Configuração do TACACS+
- Configuração do RADIUS
- Configuração da Ordem de Autenticação

5.1 Configuração dos Usuário Locais

5.1.1 Criando um novo Usuário Local

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

```
config
aaa user joao password "joao1234"
group admin
commit
```

5.1.2 Deletando um Usuário Local

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

```
config
no aaa user joao
commit
```



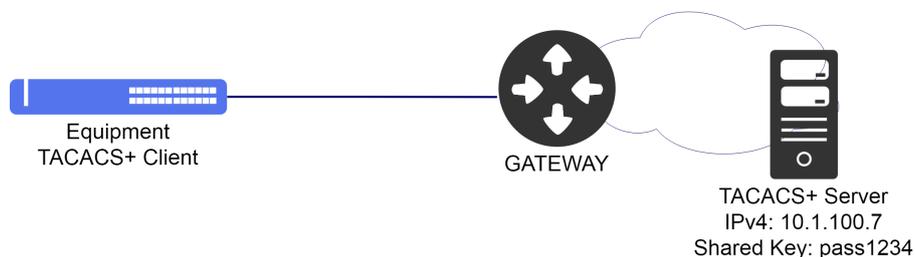
Não há comandos de troubleshooting para esta funcionalidade.

5.2 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.

5.2.1 Configurando um servidor TACACS+

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



Exemplo do TACACS+



Para que o serviço de accounting seja funcional, é necessário que a autenticação seja feita pelo 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.

```
config
aaa server tacacs TACACS-SERVER host 10.1.100.7
shared-secret "pass1234"
 authentication
 authorization
 accounting
commit
```

Pode-se especificar uma interface na configuração do TACACS+, que será utilizada como endereço de origem para os pacotes gerados pelo cliente TACACS+. A interface especificada por estar ou não associada a uma VRF.

```
config
aaa server tacacs TACACS-SERVER host 10.1.100.7
shared-secret "pass1234"
 authentication
 authorization
 accounting
 source interface l3-myintf
commit
```

Pode-se alterar o *authentication-type* na configuração do TACACS+ para ASCII, a configuração default é PAP. Esta configuração é válida para todos os servidores TACACS+ configurados.

```
config
aaa authentication-type tacacs ascii
commit
```



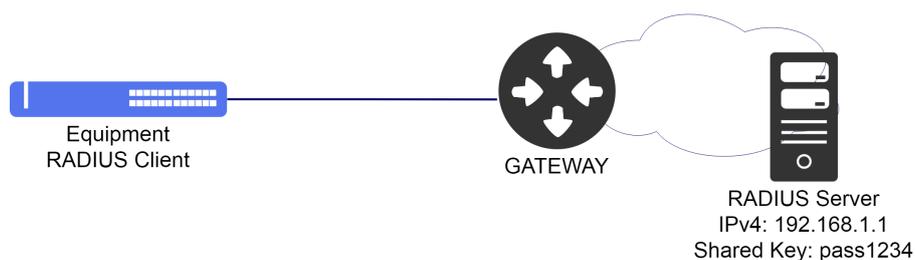
Não há comandos de troubleshooting para esta funcionalidade.

5.3 Configuração do 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.

5.3.1 Configurando um servidor RADIUS

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



Exemplo do RADIUS

Suponha que o usuário deseje configurar um servidor **RADIUS** que possui o endereço IPv4 **192.168.1.1** e senha de autenticação igual a **“pass1234”**. O procedimento a seguir apresentará como realizar esta configuração habilitando a autenticação, autorização e contabilidade:

```
config
aaa server radius RADIUS-SERVER host 192.168.1.1
  shared-secret "pass1234"
  authentication
  accounting
commit
```

Pode-se especificar uma interface na configuração do RADIUS, que será utilizada como endereço de origem para os pacotes gerados pelo cliente RADIUS. A interface especificada por estar ou não associada a uma VRF.

```
config
aaa server tacacs TACACS-SERVER host 10.1.100.7
  shared-secret "pass1234"
  authentication
  authorization
  accounting
  source interface l3-myintf
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

5.4 Configuração da 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 DmOS tentará autenticá-lo seguindo a ordem definida pelo comando da CLI **“authentication-order”**.

5.4.1 Configurando o RADIUS como mais prioritário

Suponha que o usuário configurou um servidor RADIUS para ser utilizado como método de autenticação e quer utilizá-lo como método preferencial, porém, deseja utilizar a autenticação na base local em caso de falha de comunicação com o servidor RADIUS. O procedimento para realizar esta configuração segue abaixo:

```
config
aaa authentication order [radius local]
commit
```

5.4.2 Configurando o TACACS+ como mais prioritário

Suponha que o usuário configurou um servidor TACACS+ para ser utilizado como método de autenticação e quer utilizá-lo como método preferencial. O procedimento para realizar esta configuração segue abaixo:

```
config
aaa authentication order [tacacs local]
commit
```

6 Interfaces

Este capítulo apresentará exemplos de como configurar as interfaces disponíveis. Para interfaces GPON, consultar o capítulo GPON.

Este capítulo contém as seguintes seções:

- Configuração das Interfaces Ethernet
- Configuração do Link Aggregation
- Configuração do Port Mirroring
- Configuração do Link Flap Detection
- Configuração do Hold Time

6.1 Configuração das Interfaces Ethernet

6.1.1 Configurando as Interfaces Ethernet

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

Para configurar a interface 1G localizada no Chassi 1, Slot 1 e Port 1 (1/1/1), o usuário deve usar o seguinte comando:

```
config
interface gigabit-ethernet 1/1/1
```

Para configurar a interface 10G localizada no Chassi 1, Slot 1 e Port 1 (1/1/1), o usuário deve usar o seguinte comando:

```
config
interface ten-gigabit-ethernet 1/1/1
```

Para configurar a interface 40G localizada no Chassi 1, Slot 1 e Port 1 (1/1/1), o usuário deve usar o seguinte comando:

```
config
interface forty-gigabit-ethernet 1/1/1
```

Para configurar a interface 100G localizada no Chassi 1, Slot 1 e Port 1 (1/1/1), o usuário deve usar o seguinte comando:

```
config
interface hundred-gigabit-ethernet 1/1/1
```



O esquema de numeração da porta do chassis/slot/port foi projetado para a padronização com os equipamentos de vários slots e chassis. Portanto, é sempre necessário digitar a localização completa, mesmo que o equipamento não tenha vários slots ou chassis.

Para desabilitar administrativamente uma interface 1G, o usuário deve utilizar o procedimento abaixo. O mesmo procedimento é utilizado caso o usuário queira desativar interfaces de outras capacidades, como 10G, 40G ou 100G.

```
config
interface gigabit-ethernet 1/1/1
shutdown
commit
```



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

Para reativar uma interface 1G, o usuário deve utilizar o comando “no shutdown”. O mesmo procedimento é utilizado caso o usuário queira reativar interfaces de outras capacidades, como 10G ou 40G.

```
config
interface gigabit-ethernet 1/1/1
no shutdown
commit
```



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

6.1.2 Configurando um range de Interfaces Ethernet

É possível configurar várias interfaces ao mesmo tempo através do range de interfaces. O procedimento a seguir exemplifica como desativar as interfaces gigabit-ethernet 1/1/1, 1/1/2, 1/1/3 e 1/1/4 através do range.

```
config
interface gigabit-ethernet 1/1/1-4
shutdown
commit
```



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

6.1.3 Configurando a Description das Interfaces Ethernet

Pode-se adicionar descrições às interfaces Ethernet, como demonstrado a seguir. Para visualizar as descrições das interfaces, usa-se o comando `show interface link`.

```
config
interface gigabit-ethernet 1/1/1
description "Link to switch 2"
commit
```



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

6.1.4 Configurando o MTU das Interfaces Ethernet

É possível alterar o MTU de uma interface Ethernet através da configuração abaixo.

```
config
interface gigabit-ethernet 1/1/1
mtu 1500
commit
```



O valor padrão de MTU é diferente para cada plataforma. Consulte o [Descritivo do DmOS](#) para verificar os valores máximos para cada plataforma de hardware.



O valor de MTU configurado nas interfaces não é utilizado pelos protocolos do equipamento.



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

6.1.5 Configurando o TPID das Interfaces Ethernet

É possível alterar o TPID de uma interface ethernet através da configuração abaixo.

```
config
switchport
interface gigabit-ethernet 1/1/1
tpid <tpid>
commit
```



O TPID default é 0x8100.

Os valores possíveis de TPID são:

- **0x88a8**: TPID para bridges 802.1ad
- **0x8100**: TPID padrão para VLANs 802.1Q

- **0x9100:** TPID alternative



PDU's originados no equipamento por protocolos como EAPS, ERPS e CFM serão enviados com o TPID configurado na interface.



Caso seja recebido um tráfego tagged com TPID diferente do configurado, o tráfego será encaminhado utilizando a VLAN nativa.



Não há comandos de troubleshooting para esta funcionalidade.

6.1.6 Configurando uma Interface 10Gbps para operar em 1Gbps

O DmOS permite a utilização de módulos óticos 1G em interfaces 10G de duas formas:

- **Modo Forçado ou Não Negociado**
- **Modo Negociado**



A configuração de auto-negociação esta desabilitada por padrão.



O DmOS não suporta operação de SFP+ operando a 1G.

Para utilizar uma interface 10G operando em 1G forçado, é necessário realizar as configurações abaixo:

```
config
interface ten-gigabit-ethernet 1/1/1
speed 1G
no negotiation
commit
```



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

Para utilizar uma interface 10G operando em 1G no modo negociado, é necessário realizar as configurações abaixo:

```
config
interface ten-gigabit-ethernet 1/1/1
  advertising-abilities 1Gfull
  negotiation
commit
```



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

6.1.7 Verificando as Interfaces Ethernet

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



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

```
show interface <interface-type> <chassis/slot/port>
show interface link
```

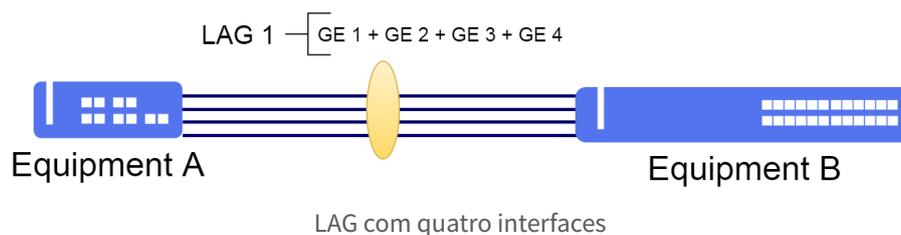
6.2 Configuração do Link Aggregation

6.2.1 Configurando um LAG no modo estático

A agregação de links definida pelo 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). 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. Caso uma das interfaces falhe, 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.



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

```
config
link-aggregation interface lag 1
interface gigabit-ethernet-1/1/1
interface gigabit-ethernet-1/1/2
interface gigabit-ethernet-1/1/3
interface gigabit-ethernet-1/1/4
commit
```



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

6.2.2 Configurando um LAG no modo dinâmico (LACP)

O LACP (Link Aggregation Control Protocol) é um protocolo utilizado para garantir a conectividade fim-a-fim entre interfaces agregadas (LAG). Ele detecta e protege a rede contra configurações incorretas, garantindo que os links sejam agregados apenas 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.

```
config
link-aggregation interface lag 1
mode active
interface gigabit-ethernet-1/1/1
interface gigabit-ethernet-1/1/2
commit
```



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

6.2.3 Configurando o hash para o balanceamento de carga

É possível modificar o algoritmo de hash utilizado no cálculo para o balanceamento de carga a ser aplicado ao tráfego encaminhado nos LAGs.



O DmOS suporta diferentes modos de hash, sendo o modo **crc16xor8** o default.



A funcionalidade é global, sendo válida para todos os LAGs utilizados no equipamento.

Os próximos passos irão demonstrar como configurar o hash para o modo **xor16**.

```
config
link-aggregation load-balance hash-function xor16
commit
```



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

6.2.4 Configurando o modo de balanceamento de carga

É possível modificar o algoritmo de balanceamento de carga a ser aplicado ao tráfego encaminhado no LAG.



O DmOS suporta diferentes modos de balanceamento de carga, sendo o modo **enhanced** o default.

Abaixo a lista de modos de balanceamento suportados:

- enhanced
- dst-ip
- dst-mac
- src-dst-ip
- src-dst-mac
- src-ip
- src-mac

- dynamic

O tipo de balanceamento dinâmico (**dynamic**) fornece uma distribuição de carga uniforme entre os membros do LAG. Considerando os valores instantâneos para a carga dos membros do LAG, os fluxos podem ser movidos dinamicamente de membros com carga maior para os membros com carga menor.

Os demais tipos de balanceamento baseiam-se em um hash (combinação de valores). Os campos dos pacotes são analisados conforme o algoritmo de balanceamento configurado, para decidir os membros do LAG que irão transmitir. Nesses modos a ordem dos pacotes é sempre mantida.

O desempenho do balanceamento dependerá da variabilidade do conteúdo dos pacotes. Pacotes com a mesma informação serão transmitidos para o mesmo membro do LAG.

Os próximos passos irão demonstrar como configurar o link-aggregation de forma estática usando quatro (4) interfaces Gigabit Ethernet, totalizando uma banda disponível de até 4Gbps. O modo de balanceamento utilizado será o **dynamic**.

```
config
link-aggregation interface lag 1
load-balance dynamic
interface gigabit-ethernet-1/1/1
interface gigabit-ethernet-1/1/2
interface gigabit-ethernet-1/1/3
interface gigabit-ethernet-1/1/4
commit
```



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

6.2.5 Configurando o número máximo e mínimo de links ativos em um LAG

- **Máximo de Links:** Ao configurar um número máximo de links ativos é possível manter links redundantes inativos, para caso algum link ativo falhar, o link redundante assumir como ativo.
- **Mínimo de Links:** Ao configurar um número mínimo de links ativos, caso a quantidade de links ativos seja menor que a número mínimo de links configurados, todas as interfaces do Link-Aggregation serão desativadas.



O número máximo de links ativos por padrão é 16.



O número mínimo de links ativos por default é 1.

Os próximos passos irão demonstrar como configurar o Link-Aggregation usando duas (2) interfaces Gigabit Ethernet com número máximo de um (1) link ativo:

```
config
link-aggregation interface lag 1
  maximum-active links 1
  interface gigabit-ethernet-1/1/1
  interface gigabit-ethernet-1/1/2
commit
```



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

Os próximos passos irão demonstrar como configurar o Link-Aggregation usando duas (2) interfaces Gigabit Ethernet com número mínimo de dois (2) links ativos:

```
config
link-aggregation interface lag 1
  minimum-active links 2
  interface gigabit-ethernet-1/1/1
  interface gigabit-ethernet-1/1/2
commit
```



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

6.2.6 Verificando o Link Aggregation

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



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

```
show link-aggregation
show link-aggregation brief
show link-aggregation interfaces
show link-aggregation lacp brief
show link-aggregation lacp extensive
show link-aggregation lacp statistics
```

6.3 Configuração do 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.

6.3.1 Configurando o Port Mirroring para o tráfego recebido

Os próximos passos irão demonstrar como configurar o port mirroring para espelhar o tráfego recebido na interface gigabit-ethernet-1/1/1 para a interface gigabit-ethernet-1/1/2.

```
config
monitor
session 1
destination
interface gigabit-ethernet-1/1/2
|
source
interface gigabit-ethernet-1/1/1
rx
!
!
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

6.3.2 Configurando o Port Mirroring para o tráfego transmitido

Os próximos passos irão demonstrar como configurar o port mirroring para espelhar o tráfego transmitido na interface gigabit-ethernet-1/1/1 para a interface gigabit-ethernet-1/1/2.

```
config
monitor
session 1
destination
interface gigabit-ethernet-1/1/2
|
source
interface gigabit-ethernet-1/1/1
tx
!
!
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

6.3.3 Configurando o Port Mirroring para o tráfego transmitido e recebido

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

```
config
monitor
session 1
destination
interface gigabit-ethernet-1/1/2
|
source
interface gigabit-ethernet-1/1/1
all
!
!
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

6.4 Configuração do Link Flap Detection

Link-Flap Detection é uma funcionalidade que visa eliminar os efeitos colaterais da variação intermitente do estado de link de uma porta. Essa funcionalidade é ativada por um determinado número de alterações do estado do link em um determinado intervalo de tempo.

A funcionalidade de Link-Flap Detection atua bloqueando um link quando dois ou mais eventos de mudança de estado de link ocorrem dentro de um intervalo de tempo configurável. Quando a porta está bloqueada, as mudanças de estado são ignoradas, trazendo estabilidade para a rede. A porta será desbloqueada após um intervalo configurável de tempo livre de eventos.

6.4.1 Configurando o Link Flap Detection na interface ethernet

Os próximos passos irão demonstrar como configurar o link flap detection na interface gigabit-ethernet-1/1/1. Na configuração abaixo o bloqueio da interface irá ocorrer caso sejam detectadas 20 transições de estado dentro do intervalo de 60 segundos. Caso as transições de estado cessem, após 90 segundos a interface será desbloqueada.

```
config
link-flap
interface gigabit-ethernet-1/1/1
  detection transitions 20
  detection interval 60
  detection restore-timeout 90
!
commit
```



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

6.4.2 Verificando o Link Flap

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



Se alguma interface Ethernet for bloqueada pelo Link Flap, a sigla **LFD** irá aparecer no campo **Blocked by** do comando **show interface link**.



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

```
show interface link
show link-flap
show link-flap config-interval
show link-flap config-restore-timeout
show link-flap config-transitions
show link-flap detected-transitions
show link-flap detection-timeout
show link-flap restore-timeout
show link-flap link-flap
```

6.5 Configuração do Hold Time

O Hold Time permite configurar um temporizador para o anúncio de transição do estado do link até que a interface tenha se mantido no novo estado pelo tempo configurado.

Quando o *hold-down* é configurado e ocorre a transição de estado de *Up* para *Down*, o temporizador de *down-hold-time* é disparado. Se ocorrer a transição de estado da interface de *Down* para *Up*, o temporizador é resetado.

Se a interface se mantiver inativa pelo tempo configurado, o estado *Down* é anunciado para os protocolos.



O DmOS suporta apenas a configuração de hold-down.



O valor do hold time nas interfaces que possuem OSPFv2 e BFD configurados devem ser inferiores à 200 ms.

6.5.1 Configurando o Hold Time

Os próximos passos irão demonstrar como configurar o hold time na interface gigabit-ethernet-1/1/1. Na configuração o anúncio de interface down só irá ocorrer após 2 segundos (2000 milissegundos). Após 2 segundos o equipamento passa a anunciar que a interface está inativa.

```
config
hold time interface gigabit-ethernet-1/1/1
down 2000
commit
```



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

6.5.2 Verificando o Hold Time

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



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

```
show log component lim_l2 | include HOLD_TIME
```

7 GPON

O GPON usa a tecnologia WDM (Wavelength Division Multiplexing), permitindo a transmissão bidirecional sobre uma única fibra (comprimento de onda diferente para downstream e upstream). Para segregar o tráfego de vários usuários, o GPON usa broadcast na direção downstream (OLT para ONU) e TDMA (Time Division Multiple Access), na direção upstream (ONU para OLT).

Como os dados são transmitidos da OLT para a ONU, as ONUs (unidades de redes ópticas) devem filtrar o tráfego de dados do usuário e também coordenar, multiplexando os sinais, a saída do cliente para não entrar em conflito com os dados de outros usuários.

Como os pacotes de dados são transmitidos de maneira broadcast para todas as ONUs, o padrão GPON usa AES (Advanced Encryption Standard) para criptografar o fluxo de dados na direção downstream (OLT para ONU). A criptografia é uma maneira segura de evitar a interceptação e garantir que apenas o usuário permitido acesse as informações.



Leia o Descritivo do equipamento para verificar se estas funcionalidades estão disponíveis em sua plataforma de hardware.

Este capítulo contém as seguintes seções:

- [Operações Básicas do GPON](#)
- [Profiles GPON](#)
- [Tipos de Serviço GPON](#)
- [Mapeando o Service Port](#)
- [Configurando Aplicações GPON](#)
- [Provisionamento Automático de ONUs](#)

7.1 Operações Básicas do GPON

7.1.1 Configurando uma interface GPON

Para configurar uma interface GPON, o usuário deve entrar no nível de configuração da interface. Para configurar a interface GPON localizada no Chassi 1, Slot 1 e Port 1 (1/1/1), o usuário deve usar o seguinte comando:

```
config
interface gpon 1/1/1
```



Por padrão, todas as interfaces GPON estão administrativamente desativadas.

Para ativar uma interface GPON, o usuário deve utilizar o procedimento abaixo.

```
config
interface gpon 1/1/1
no shutdown
commit
```

Para desativar administrativamente uma interface GPON, o usuário deve utilizar o procedimento abaixo.

```
config
interface gpon 1/1/1
shutdown
commit
```

Por padrão, o FEC está habilitado nas interfaces GPON para fluxos nos sentidos downstream e upstream. O usuário pode desativá-lo com as seguintes configurações:

```
interface gpon 1/1/1
no upstream-fec
no downstream-fec
commit
```



Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificação básica do GPON](#).

7.1.2 Configurando o método de autenticação das ONUs

O método de autenticação da ONU é uma configuração global do GPON. Portanto, ele é aplicado em todas as interfaces GPON.

O método padrão de autenticação é via **serial-number**.

Os métodos de autenticação disponíveis são:

- **serial-number**: Autenticação via número de série da ONU.
- **password-only**: Autenticação por senha. A senha das ONUs DATACOM é composta pelo número de série da ONU sem as letras "DA".
Exemplo: Se o número serial for DACM12345678 a senha para autenticação será CM123456789.
- **serial-number-and-password**: Autenticação via combinação de número de série mais senha.

O procedimento abaixo apresenta como configurar o método de autenticação por senha.

```
config
gpon 1/1
onu-auth-method password
commit
```



Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificação básica do GPON](#).

7.1.3 Descobrimo as ONUs

Para descobrir as ONUs que estão ligadas em alguma das portas GPON da OLT, o usuário pode realizar o procedimento descrito abaixo:

```
show interface gpon discovered-onus
```



Será informado o SN (Serial Number) de todas as ONUs que ainda não estão provisionadas na OLT.

```
# show interface gpon discovered-onus
Chassis / Slot / Port  Serial Number
-----
1/1/1                 DACM00001B30
```

7.1.4 Provisionando a ONU

Antes de provisionar uma ONU é necessário que ela conste na lista de ONUs descobertas, conforme verificado no tópico anterior. De posse do número serial da ONU, o usuário pode realizar o procedimento descrito abaixo:



Antes de realizar esse procedimento, é necessário ter o line-profile configurado. Para maiores detalhes sobre a configuração do line-profile, consultar o tópico [Profiles GPON](#).

```
config
interface gpon 1/1/1
no shutdown
onu 1
serial-number DACM00001B30
line-profile <LINE_PROFILE_NAME>
!
commit
```

7.1.5 Removendo a ONU

É possível remover uma ONU configurada. Esse processo serve para os casos onde o usuário necessita utilizar a ONU em outro PONLINK ou apenas remover uma configuração que não está em uso. Para esse processo o usuário pode realizar o procedimento descrito abaixo:



Antes de realizar esse procedimento, é necessário remover todos os service-ports vinculados a ONU que será removida.

```
config
interface gpon 1/1/1
no onu 1
!
commit
```

Para remover o service-port o usuário pode realizar o procedimento descrito abaixo:

```
config
no service-port <SERVICE_PORT_ID>
commit
```



Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificação básica do GPON](#).

7.1.6 Verificação básica do GPON

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade. O usuário deve usar a palavra-chave **do** antes do comando caso estiver no modo de configuração.



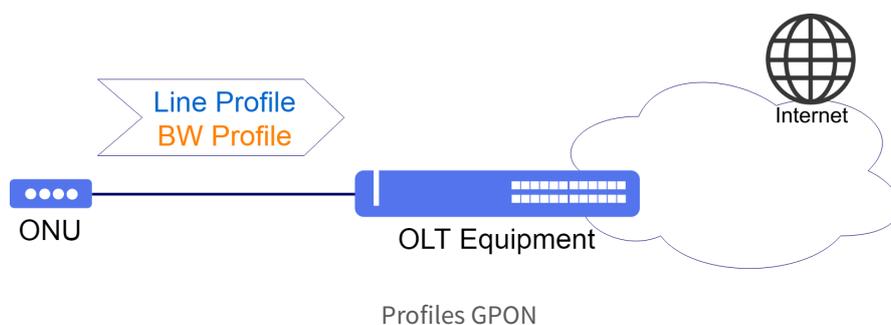
Para maiores detalhes sobre as saídas dos comandos, consultar o **Command Reference**.

```
show running-config gpon chassis/slot
show interface gpon chassis/slot/port
show interface gpon chassis/slot/port brief
show interface gpon discovered-onus
```

7.2 Profiles GPON

Em uma típica rede PON, existem muitos usuários finais, mas poucos tipos de serviços e modelos de ONU. Assim, para evitar tarefas de provisionamento repetitivo, os perfis GPON permitem definir atributos comuns que podem ser reutilizados muitas vezes e aplicados em várias portas de serviço.

A figura abaixo pretende facilitar a visualização de onde cada perfil é aplicado.



Após a configuração dos perfis GPON, eles devem ser associados a configuração das ONUs para que o serviço configurado passe a operar.

7.2.1 Carregando os Perfis Default

É possível carregar os perfis GPON que viabilizam uma rápida configuração nos serviços de GPON. É possível carregar os perfis default para ONUs Bridge, para ONUs Router ou para ambos os tipos de ONUs.

Para carregar os perfis default para ambos os tipos de ONUs, o usuário deverá realizar o procedimento abaixo:

```
config
load default-gpon-profiles
commit
```

Para verificar os perfis que foram carregados é possível executar o comando de show dentro do modo de configuração conforme apresentado abaixo:

```
(config)# show profile gpon
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
traffic type-4 max-bw 1106944
!
profile gpon line-profile DEFAULT-LINE
upstream-fec
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
gem 1
  tcont 1 priority 1
  map any-ethernet
    ethernet any vlan any cos any
  !
  map any-veip
    veip 1 vlan any cos any
  !
gem 2
  tcont 1 priority 0
  map any-iphost
    iphost vlan any cos any
  !
!
profile gpon media-profile DEFAULT-MEDIA
no oob-dtmf
jitter target dynamic-buffer
jitter maximum onu-internal-buffer
codec-order 1
  type pcma
  no silence-suppression
!
codec-order 2
  type pcmu
  no silence-suppression
!
codec-order 3
  type g723
  no silence-suppression
!
codec-order 4
  type g729
  no silence-suppression
!
!
profile gpon snmp-profile DEFAULT-SNMP
if-type
if-descr
if-oper-status
if-onu-power-rx
statistics-in-bw-usage
statistics-out-bw-usage
!
```

7.2.2 Bandwidth Profile

O perfil de largura de banda define as características de alocação de largura de banda de upstream, como tipo T-CONT, largura de banda fixa, largura de banda assegurada e largura de banda máxima, de acordo com a tabela abaixo.

Tipo BW	Sensível ao Delay	Tipos de T-CONT aplicáveis				
		Tipo1	Tipo2	Tipo3	Tipo4	Tipo5
Fixo	Sim	X				X
Assured	Não		X	X		X
Non-Assured	Não			X		X
Best-Effort	Não				X	X
Max	Não			X	X	X

Tipos de Banda vs Tipos de T-CONT aplicáveis

Os comandos a seguir exemplificam a criação de um perfil que configura um T-CONT tipo 3, com 2 Mbit/s de banda assegurada e 10 Mbit/s de banda máxima. Apenas são permitidas bandas múltiplas de 64 Kbit/s.

```
config
profile gpon bandwidth-profile <BANDWIDTH_PROFILE_NAME>
traffic type-3 assured-bw 2048 max-bw 9984
commit
```

7.2.3 Line Profile

Este perfil é usado para associar portas GEM a um T-CONT e mapear uma porta GEM com os serviços da ONU. A porta GEM representa um fluxo de dados, que deve ser associada a um perfil de banda.

Configuração para ONU bridge

Os seguintes comandos exemplificam a definição de um perfil de banda para um tráfego chegando à interface Ethernet 1 com VLAN ID 100 na ONU bridge:

```
config
profile gpon line-profile <LINE_PROFILE_NAME>
tcont 1 bandwidth-profile <BANDWIDTH_PROFILE_NAME>
gem 1
tcont 1
map <MAPPING_NAME>
  ethernet 1 vlan 100 cos any
!
!
commit
```

Configuração para ONU router

Os seguintes comandos exemplificam a definição de um perfil de banda para um tráfego chegando à interface VEIP 1 com VLAN ID 100 na ONU router:

```
config
profile gpon line-profile <LINE_PROFILE_NAME>
tcont 1 bandwidth-profile <BANDWIDTH_PROFILE_NAME>
gem 1
tcont 1
map <MAPPING_NAME>
veip 1 vlan 100 cos any
!
!
commit
```

7.2.4 Media Profile

O media-profile é usado para configurar parâmetros de mídia para serviços de VoIP, permitindo que o usuário defina uma lista de codecs ordenados prioritariamente, onde é definido o tipo de codec, o período do pacote e a supressão de silêncio para cada entrada na lista. O media-profile também permite ativar/desativar o DTMF fora da banda (**oob-dtmf**), configurar o jitter buffer e o valor máximo do jitter buffer e também configurar a variante do protocolo PSTN (código de país) para definir a sinalização POTS que será utilizada.



É mandatório que a ONU possua suporte à configuração via protocolo OMCI.

Os comandos a seguir exemplificam a criação de um perfil de media que configura o out-of-band DTMF desativado, o jitter target no modo dinâmico e jitter máximo definido pela ONU. A sinalização POTS será configurada para uso no Brasil.

A ordem dos codecs de áudio que será configurada:

- **1 PCMA**: Sem compressão, largura de banda de 64 Kbps. Usado na Europa.
- **2 PCMU**: Sem compressão, largura de banda de 64 Kbps. Usado nos Estados Unidos.
- **3 G723**: Com compressão, largura de banda de 5.3/6.3 Kbps.
- **4 G729**: Com compressão, largura de banda de 8 Kbps.



É necessário configurar pelo menos 4 tipos de codecs no media-profile.

```
config
profile gpon media-profile <MEDIA_PROFILE_NAME>
no oob-dtmf
jitter target dynamic-buffer
jitter maximum onu-internal-buffer
pstn-protocol-variant BRA
codec-order 1
```

```

type pcma
no silence-suppression
!
codec-order 2
type pcmu
no silence-suppression
!
codec-order 3
type g723
no silence-suppression
!
codec-order 4
type g729
no silence-suppression
!
!
commit

```

7.2.5 SIP Agent Profile

O perfil do Agente SIP define os endereços IP dos servidores para o serviço POTS que registrará a linha analógica e controlará o processo de chamada. Existem três servidores para configurar.

- **Register Server:** É o servidor que aceita solicitações de REGISTRO e coloca as informações recebidas nesses pedidos no serviço de localização para o domínio com o qual ele lida.
- **Proxy Server:** É uma entidade intermediária que age como um servidor e um cliente com o objetivo de fazer solicitações em nome de outros clientes. Um servidor proxy desempenha basicamente o papel de roteamento, o que significa que seu trabalho é garantir que uma solicitação seja enviada para outra entidade "mais próxima" do usuário visado.
- **Outbond Proxy:** O proxy de saída recebe a solicitação de um cliente, mesmo que não seja o servidor resolvido pelo URI de solicitação.



O SIP Agent Profile é válido somente para ONUs que possuem interface POTS.

Se o usuário deseja definir um perfil do Agente SIP deve usar os seguintes comandos:

```

config
profile gpon sip-agent-profile <SIP_AGENT_PROFILE_NAME>
  registrar <REGISTRAR_IP_ADDRESS>
  proxy-server <PROXY_SERVER_IP_ADDRESS>
  outbound-proxy <OUTBOUND-PROXY-IP-ADDRESS>
!
commit

```

7.2.6 SNMP Profile

O perfil SNMP define quais objetos (OIDs) estarão disponíveis para consulta na ONU através do gerente SNMP. Após configurar o perfil SNMP, deve-se adicioná-lo na configuração da ONU na interface GPON.

Abaixo a lista de alguns objetos que podem ser habilitados para consulta SNMP através da ONU.



Para consulta dos demais objetos que podem ser configurados, consultar o manual de Referência de Comandos.

- **if-admin-status:** Status administrativo da interface.
- **if-descr:** Descrição da interface.
- **if-name:** Nome da interface.
- **if-onu-power-rx:** Potencia ótica recebida.
- **if-onu-power-tx:** Potencia ótica transmitida.
- **if-onu-sysuptime:** Uptime da ONU.
- **if-oper-status:** Status operacional da interface.
- **if-type:** IANA global tipo de interface.
- **statistics-in-bw-usage:** Banda utilizada de entrada na Ethernet UNI.
- **statistics-out-bw-usage:** Banda utilizada de saída na Ethernet UNI.



É necessário habilitar na OLT o agente SNMP para consultas. Consultar o capítulo [Configurando o SNMP](#)

Se o usuário deseja definir um perfil SNMP para as ONUs deve usar os seguintes comandos:

```
config
profile gpon snmp-profile <GPON-SNMP-PROFILE>
if-type
if-descr
if-oper-status
if-onu-power-rx
statistics-in-bw-usage
statistics-out-bw-usage
!
commit
```

7.2.7 GEM Traffic Agent Profile

Este serviço é usado para aplicar um limite de taxa de Downstream na ONU. É importante para o ISP (Internet Service Provider) permitir a autenticação DHCP com o limite de tráfego da rede de acordo com a assinatura. O perfil de tráfego GEM define a banda de CIR e EIR para uma ONU.

- **CIR - Committed Information Rate:** É a taxa em Kbps garantida para passar pela interface.
- **EIR - Excess Information Rate:** É a taxa adicional em Kbps, que em caso de disponibilidade de banda fará com o que o tráfego máximo da ONU seja o CIR + EIR.

Se o usuário deseja configurar um perfil de tráfego GEM, o qual é configurado junto ao T-CONT, que por sua vez foi declarado no profile de linha, deve usar os seguintes comandos:

```
config
profile gpon gem-traffic-profile <GEM_TRAFFIC_PROFILE_NAME>
  cir <COMMITTED-RATE>
  eir <EXCESS-RATE>
!
profile gpon line-profile <LINE_PROFILE_NAME>
  tcont 1 bandwidth-profile <BANDWIDTH_PROFILE_NAME>
  gem 1
  tcont 1 gem-traffic-profile <GEM_TRAFFIC_PROFILE_NAME>
!
!
commit
```

7.2.8 Residential Gateway Profile (RG-Profile)

O perfil de RG define as características de roteador que devem ser configuradas nas ONUs. Este perfil implementa uma solução proprietária DATACOM e deve ser utilizada apenas com ONUs DATACOM modelos DM984-42x com função router.

É possível configurar três principais tipos de conexões:

- **wan-pppoe-connection:** Configuração de conexão WAN PPPoE. Cada conexão representa uma conexão WAN na ONU. Utilizado para autenticação PPPoE da ONU.
- **wan-ip-connection:** Configura um endereço de gateway padrão para conexão IP relacionada no Perfil RG. Utilizado para comunicação IP da ONU.
- **wan-bridge-connection:** Configuração de conexão WAN bridge. Cada conexão representa uma conexão WAN bridge da ONU. Utilizado para cenários LAN-to-LAN.

É permitido configurar **filtros de IP (ip-filtering)** dentro das conexões de wan-pppoe-connection e wan-ip-connection. Esta configuração é **opcional**, mas estará disponível nos exemplos de configuração que serão apresentados a seguir.

Caso seja necessário alterar a senha dos usuários **admin** e/ou **support**, o comando **user-mgmt priv-lvl-support password custom support2** pode ser adicionado ao profile durante a criação ou edição. No exemplo abaixo, a senha do usuário **support** é alterada para **support2**:

```
config
profile gpon rg-profile PPPoE
  user-mgmt priv-lvl-support password custom support2
!
commit
```

wan-pppoe-connection

Se o usuário desejar configurar um perfil de Residencial Gateway para aplicação com **autenticação PPPoE** na WAN da ONU usando a **VLAN 2000**, deve configurar uma **wan-pppoe-connection** no RG-Profile. O filtro de IP para permitir pacotes com protocolo TCP será incluído.

O procedimento a seguir apresentará como realizar esta configuração:

```
config
profile gpon rg-profile PPPoE
wan-pppoe-connection PPPoE
vlan-mux vlan 2000
nat
no fullcone-nat
firewall
no multicast-proxy igmp
no multicast-source igmp
auth-type auto
ip-filtering 0
  incoming
  match protocol tcp
  action permit
!
!
commit
```

wan-ip-connection

Se o usuário desejar configurar um perfil de Residencial Gateway para aplicação IP com **autenticação DHCP** na WAN da ONU usando a **VLAN 2100**, deve configurar uma **wan-ip-connection** no RG-Profile. O filtro de IP para permitir pacotes com protocolo TCP ou UDP será incluído.

O procedimento a seguir apresentará como realizar esta configuração:

```
config
profile gpon rg-profile DHCP
wan-ip-connection DHCP
vlan-mux vlan 2100
nat
no fullcone-nat
firewall
no multicast-proxy igmp
no multicast-source igmp
ipv4 dhcp
primary-dns 10.0.1.1
secondary-dns 10.0.1.2
ip-filtering 1
  incoming
  match protocol tcp-udp
  action permit
!
!
commit
```

wan-bridge-connection

Se o usuário desejar configurar um perfil de Residencial Gateway para aplicação **LAN-to-LAN** usando a **VLAN 520** na interface eth1 da ONU, deve configurar uma **wan-bridge-connection** no RG-Profile.

O procedimento a seguir apresentará como realizar esta configuração:

```
config
profile gpon rg-profile RG-ROUTER-520
wan-bridge-connection VLAN-520
vlan-mux vlan 520
no multicast-source igmp
itf-grouping
  igmp-snooping
  ports eth1 vlan 520
!
!
commit
```

one-shot-provisioning

As características de roteamento que não são configuráveis através do perfil de Residencial Gateway podem ser configuradas diretamente nas ONUs através da interface WEB, porém, a cada reboot das ONUs estas alterações são perdidas devido à característica de aplicação do perfil de Residencial Gateway a cada subida das ONUs, sobrescrevendo as configurações realizadas através da interface WEB. Para tornar estas configurações persistentes, é possível habilitar globalmente na OLT a opção de **rg-one-shot-prov**.

O procedimento a seguir apresentará como realizar esta configuração:

```
config
gpon 1/1
  rg-one-shot-prov
!
commit
```

Após ativar a configuração de **rg-one-shot-prov**, todas as novas ONUs ativadas na OLT terão a configuração que for realizada pela interface WEB persistente, impedindo que a OLT aplique o perfil de Residencial Gateway a cada nova subida das ONUs. As ONUs que foram configuradas antes da ativação do **rg-one-shot-prov** só terão a configuração persistida após um reboot ou a reaplicação do perfil de Residencial Gateway, operação esta que pode ser realizada com o seguinte comando:

```
config
interface gpon 1/1/12 onu 4
  rg-reprovision
!
commit
```

O comando **rg-reprovision** é aplicado no nível de configuração da ONU e não necessita de commit, uma vez que ele apenas executa uma reaplicação do perfil de Residencial Gateway e não indica uma configuração de fato.



O comando **rg-reprovision** deve ser utilizado sempre quando for necessário que a OLT realize o reprovisionamento do perfil de Residencial Gateway na ONU. Situações em que o cliente realize uma configuração errada na ONU ou um reset para as configurações padrões são exemplos de situações em que este comando deve ser utilizado, recuperando as funcionalidades padrões da ONU.

As ONUs que foram configuradas antes da ativação do **rg-one-shot-prov** apresentam o campo de status **RG One Shot Provision** com a informação **Not provisioned**, ou seja, as configurações realizadas pela interface WEB serão perdidas quando a ONU for reiniciada. O exemplo a seguir apresenta um exemplo desta informação:

```
show interface gpon 1/1/12 onu 4
Last updated      : 2019-09-27 12:05:54 UTC-3
ID                : 4
Serial Number     : DACM00009C5C
Password         :
Uptime           : 4 min
Last Seen Online  : N/A
Vendor ID        : DACM
Equipment ID     : DM984-422
Name             :
Operational state : Up
Primary status    : Active
Distance         : 0 [km]
IPv4 mode        : DHCP
IPv4 address     : 172.24.1.157/24
```

```

IPv4 default gateway : 172.24.1.12
IPv4 VLAN            : 1505
IPv4 CoS             : 0
Line Profile         : Triple-Play-42X-veip
Service Profile      : DM984-42X
RG Profile           : 1-1-12-ONU-4
RG One Shot Provision : Not provisioned
SNMP                 : Disabled
Allocated bandwidth : 2048 fixed, 22144 assured+fixed [kbit/s]
Upstream-FEC         : Enabled
Anti Rogue ONU isolate : Disabled
Version              : 800.5156.12
Active FW             : v4.1.6-8-g943a valid, committed
Standby FW           : v4.1.6-7-g5f87 valid, not committed
Software Download State : None
Rx Optical Power [dBm] : -8.00
Tx Optical Power [dBm] : Not supported

```

Após aplicar o comando **rg-reprovision** ou realizar um reset na ONU, o campo **RG One Shot Provision** é preenchido com a informação do timestamp de quando foi realizado o provisionamento da ONU através do perfil de Residencial Gateway, como pode ser observado no exemplo:

```

show interface gpon 1/1/12 onu 4
Last updated          : 2019-09-27 12:07:27 UTC-3
ID                   : 4
Serial Number        : DACM00009C5C
Password             :
Uptime               : 1 min
Last Seen Online     : N/A
Vendor ID            : DACM
Equipment ID         : DM984-422
Name                 :
Operational state    : Up
Primary status       : Active
Distance             : 0 [km]
IPv4 mode             : DHCP
IPv4 address         : 172.24.1.157/24
IPv4 default gateway : 172.24.1.12
IPv4 VLAN            : 1505
IPv4 CoS             : 0
Line Profile         : Triple-Play-42X-veip
Service Profile      : DM984-42X
RG Profile           : 1-1-12-ONU-4
RG One Shot Provision : Provisioned on 2019-09-27 12:07:21 UTC-3
SNMP                 : Disabled
Allocated bandwidth : 2048 fixed, 22144 assured+fixed [kbit/s]
Upstream-FEC         : Enabled
Anti Rogue ONU isolate : Disabled
Version              : 800.5156.12
Active FW             : v4.1.6-8-g943a valid, committed
Standby FW           : v4.1.6-7-g5f87 valid, not committed
Software Download State : None
Rx Optical Power [dBm] : -7.99
Tx Optical Power [dBm] : Not supported

```



Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificando os perfis GPON](#).

7.2.9 TR-069 ACS Profile

O serviço de configuração automática através de um servidor (ACS - Auto Configuration Server) permite realizar provisionamentos de serviços de forma automática através do protocolo TR-069. Para que uma ONU possa utilizar os serviços disponíveis no ACS, ela precisa ter suporte ao protocolo TR-069 e o servidor precisa estar previamente configurado com os parâmetros a serem provisionados. Uma vez que a estrutura para o TR-069 esteja preparada, a ONU precisa receber da OLT a informação de como chegar até o ACS, esta configuração na ONU é realizada pela OLT através do perfil

tr069-acis-profile, o qual precisa ser configurado com a URL do servidor, usuário e senha de acesso.

- **URL:** É o endereço pelo qual o servidor TR-069 responde.
- **Username:** É o usuário de acesso ao servidor TR-069.
- **Password:** É a senha de acesso para o usuário utilizado.

Para realizar a criação do perfil do ACS os seguintes comandos devem ser utilizados:

```
config
profile gpon tr069-acis-profile <ACS_PROFILE_NAME>
url <ACS-URL>
username <ACS-USERNAME>
password <ACS-PASSWORD>
!
commit
```

Uma vez definido o perfil do ACS, ele deve ser aplicado às ONUs que devem fazer uso deste método de provisionamento. Os comandos a seguir exemplificam o processo de criação de um perfil para provisionamento via TR-069 e aplicação à ONU desejada:

```
config
profile gpon tr069-acis-profile TR-069
url http://tr-069-server.internal:17000
username datacom
password datacom1234
!
interface gpon 1/1/1 onu 0
tr069-acis-profile TR-069
!
commit
```



É mandatório que a ONU possua suporte à configuração via protocolo TR-069. Antes de utilizar esta funcionalidade, verifique na documentação do produto se a solução de configuração via TR-069 está disponível para o modelo utilizado.



Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificando os perfis GPON](#).

7.2.10 Verificando os perfis GPON

Abaixo os principais comandos disponíveis para realizar a verificação da funcionalidade. O usuário deve usar a palavra-chave **do** antes do comando caso estiver no modo de configuração.



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

```
show running-config profile gpon
```

7.3 Tipos de Serviço GPON

É possível configurar várias aplicações GPON entre a OLT e as ONU. O DmOS suporta três principais tipos de serviços:

7.3.1 Service VLAN N:1

- **N:1:** Esse tipo de serviço geralmente é implantado para fornecer acesso a Internet a clientes residenciais, uma vez que apenas uma VLAN é usada para transportar o serviço de internet em toda a rede.

O comando a seguir configurará a VLAN para o tipo de serviço N:1. Isso significa que os clientes (N) na mesma VLAN não poderão se comunicar entre si.

```
config
service vlan 100 type n:1
commit
```

7.3.2 Service VLAN 1:1

- **1:1:** Esse tipo de serviço geralmente é implantado para fornecer aplicações corporativas ou acesso à internet residencial, uma vez que uma VLAN diferente é usada para transportar o serviço de cada cliente através da rede. Cada classe de tráfego do mesmo assinante deve ter a mesma VLAN.

O comando a seguir configurará a VLAN para o tipo de serviço 1:1. Isso significa que os clientes na mesma VLAN não poderão se comunicar entre si.

```
config
service vlan 100 type 1:1
commit
```

7.3.3 Service VLAN TLS

- **TLS:** Esse tipo de serviço geralmente é implantado para fornecer aplicações corporativas, uma vez que uma VLAN distinta é usada para transportar o serviço de cada cliente através da rede. Cada classe de tráfego do mesmo assinante pode ter a mesma ou diferente VLAN. Este serviço quando utilizado em conjunto com o Hairpin possibilita o oferecimento de serviços LAN-to-LAN sem necessidade de equipamentos adicionais (roteadores, por exemplo).

O comando a seguir configurará a VLAN para o tipo de serviço TLS. Isso significa que os clientes na mesma VLAN poderão se comunicar entre si.

```
config
service vlan 100 type tls
commit
```

7.4 Mapeando o Service Port

Uma porta de serviço é usada para estabelecer uma relação entre o tráfego da porta GEM e a VLAN de serviço.

Exemplos de aplicações com Service Port:

7.4.1 Service Port - Transparent

No exemplo abaixo o tráfego oriundo da VLAN ID 100 nas ONUs será encaminhado de forma transparente através do seguinte comando:

```
config
service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 100
commit
```

7.4.2 Service Port - Replace

Por exemplo, o tráfego oriundo da VLAN ID 100 nas ONUs será mapeado para a Service VLAN 200 através do seguinte comando:

```
config
service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 200
commit
```

7.4.3 Service Port - Add

Por exemplo, o tráfego oriundo da VLAN ID 100 nas ONUs receberá uma nova tag de VLAN 1000 através do seguinte comando:

```
config
service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 100 action vlan add vlan-id 1000
commit
```



Um service-port que utiliza uma service VLAN do tipo N:1 suporta apenas a operação replace.

7.5 Configurando Aplicações GPON

Para configurar uma aplicação GPON com ONU (bridge/router) é necessário seguir os passos abaixo:

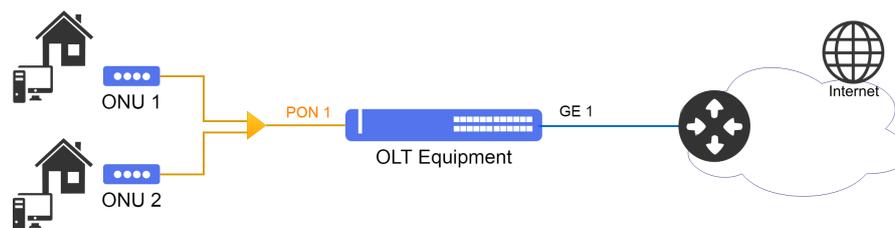
- **Configurar VLAN**
- **Configurar Service VLAN**
- **Habilitar a interface GPON**

- **Verificar a descoberta de ONU**
- **Configurar o perfil de banda (bandwidth-profile)**
- **Configurar o perfil de linha (line-profile)**
- **Configurar o RG Profile (apenas para ONU router)**
- **Provisionar a ONU**
- **Configurar o Service Port**

7.5.1 Configurando uma Aplicação N:1 com ONU bridge

Suponha que o usuário deseje configurar dois clientes com mesmo perfil de banda. Para este exemplo, o tipo de serviço N:1 será configurado exemplificando o fornecimento de acesso a Internet para clientes residenciais. A VLAN 100 será utilizada como VLAN de serviço. A configuração de **native vlan** na ONU será utilizada para entrega do serviço sem tag de VLAN na Ethernet da ONU.

O cenário abaixo será usado para demonstrar a configuração do serviço usando a interface ethernet das ONUs.



Cenário para Serviço de Acesso a Internet usando a Service-VLAN N:1

Abaixo a configuração completa para a aplicação N:1 com ONU bridge:

```
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1
!
service vlan 100 type n:1
!
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
traffic type-4 max-bw 1106944
!
profile gpon line-profile DEFAULT-LINE
upstream-fec
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
gem 1
tcont 1 priority 0
map ethernet
ethernet 1 vlan 100 cos any
!
!
interface gpon 1/1/1
no shutdown
onu 1
name CLIENTE-1
serial-number DACM00000001
line-profile DEFAULT-LINE
ethernet 1
negotiation
no shutdown
native vlan vlan-id 100
!
onu 2
```

```

name CLIENTE-2
serial-number DACM00000002
line-profile DEFAULT-LINE
ethernet 1
negotiation
no shutdown
native vlan vlan-id 100
!
!
service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 100
service-port 2 gpon 1/1/1 onu 2 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 100
!
commit

```

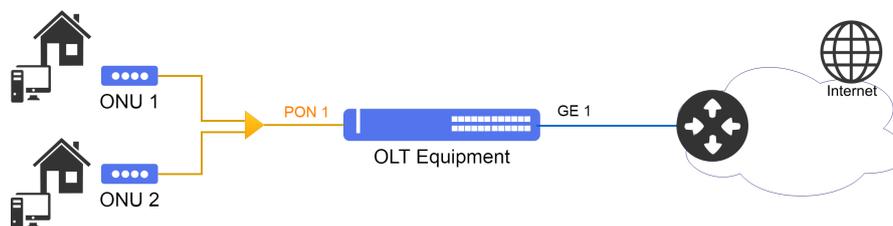


Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificando aplicações GPON](#).

7.5.2 Configurando uma Aplicação 1:1 com ONU bridge

Suponha que o usuário deseje configurar dois clientes com mesmo perfil de banda. Para este exemplo, o tipo de serviço 1:1 será configurado exemplificando o fornecimento de acesso a Internet para clientes corporativos. A VLAN 100 será utilizada como VLAN de serviço da ONU 1 e a VLAN 200 como VLAN de serviço da ONU 2. A entrega do serviço ocorre com tag de VLAN na Ethernet da ONU.

O cenário abaixo será usado para demonstrar a configuração do serviço usando a interface ethernet das ONUs.



Cenário para Serviço de Acesso a Internet usando a Service-VLAN 1:1

Abaixo a configuração completa para a aplicação 1:1 com ONU bridge:

```

config
dot1q
vlan 100,200
interface gigabit-ethernet-1/1/1
!
!
service vlan 100 type 1:1
!
service vlan 200 type 1:1
!
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
traffic type-4 max-bw 1106944
!
profile gpon line-profile LINE-1
upstream-fec
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
gem 1
tcont 1 priority 0
map ethernet
ethernet 1 vlan 100 cos any
!
!
profile gpon line-profile LINE-2
upstream-fec
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH

```

```

gem 1
  tcont 1 priority 0
  map ethernet
    ethernet 1 vlan 200 cos any
  !
!
interface gpon 1/1/1
  no shutdown
  onu 1
    name CLIENTE-1
    serial-number DACM00000001
    line-profile LINE-1
    ethernet 1
      negotiation
      no shutdown
    !
  !
  onu 2
    name CLIENTE-2
    serial-number DACM00000002
    line-profile LINE-2
    ethernet 1
      negotiation
      no shutdown
    !
  !
!
service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 100
service-port 2 gpon 1/1/1 onu 2 gem 1 match vlan vlan-id 200 action vlan replace vlan-id 200
!
commit

```

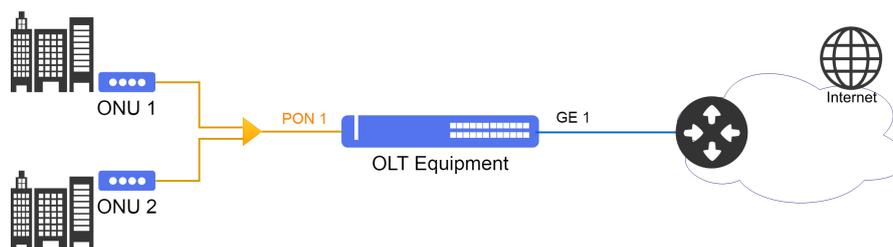


Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificando aplicações GPON](#).

7.5.3 Configurando uma Aplicação TLS com ONU router

Suponha que o usuário deseje configurar uma aplicação LAN-to-LAN para transparência de protocolos e possibilidade dos clientes se comunicarem. Para este exemplo, o tipo de serviço TLS será configurado exemplificando o fornecimento de aplicações corporativas. A VLAN 100 será utilizada como VLAN de serviço.

O cenário abaixo será usado para demonstrar a configuração do serviço usando a interface VEIP das ONUs DATACOM modelo DM98x.



Cenário para Serviço Corporativo usando a Service-VLAN TLS



É necessário configurar um RG Profile para que as configurações sejam enviadas para ONU DM98x.

A principal alteração em relação a configuração para ONU bridge é no tipo de interface configurada que passa de **ethernet** para **veip**.

Abaixo a configuração completa para a aplicação TLS com ONU router modelo DM98x:

```

config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1
!
!
service vlan 100 type tls
!
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
traffic type-4 max-bw 1106944
!
profile gpon line-profile DEFAULT-LINE
upstream-fec
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
gem 1
tcont 1 priority 0
map veip
veip 1 vlan 100 cos any
!
!
profile gpon rg-profile RG-DM98x
wan-bridge-connection VLAN-100
vlan-mux vlan 100
no multicast-source igmp
itf-grouping
igmp-snooping
ports eth1 vlan 100
!
!
interface gpon 1/1/1
no shutdown
onu 1
name CLIENTE-1
serial-number DACM00000001
rg-profile RG-DM98x
line-profile DEFAULT-LINE
veip 1
!
!
onu 2
name CLIENTE-2
serial-number DACM00000002
rg-profile RG-DM98x
line-profile DEFAULT-LINE
veip 1
!
!
service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 100
service-port 2 gpon 1/1/1 onu 2 gem 1 match vlan vlan-id 100 action vlan replace vlan-id 100
!
commit

```



Os comandos disponíveis para troubleshooting podem ser encontrados no tópico [Verificando aplicações GPON](#).

7.5.4 Configurando uma aplicação GPON com MPLS

Para configurar essa aplicação, consultar o tópico [MPLS com acesso GPON](#).

7.5.5 Verificando aplicações GPON

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



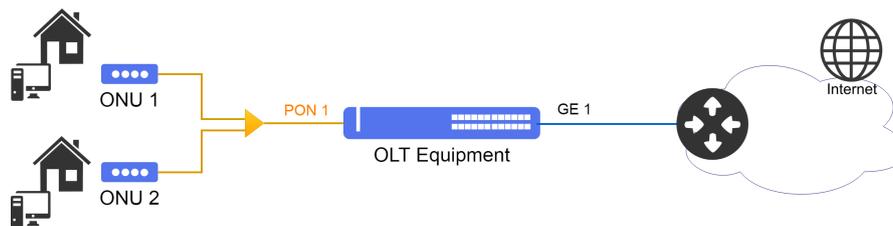
Para maiores detalhes sobre as saídas dos comandos, consultar o **Command Reference**.

```
show interface gpon <chassis/slot/port> statistics
show interface gpon onu
show interface gpon <chassis/slot/port> onu <id>
show interface gpon <chassis/slot/port> onu <id> gem <id> statistics
show mac-address-table
```

7.6 Provisionamento Automático de ONUs

A ferramenta de autoprovisionamento é utilizada para configurar de forma automática todas as ONUs descobertas na OLT baseado em um conjunto de perfis pré-determinados. A configuração é realizada de forma global e vai aplicar a configuração definida no autoprovisionamento para todas as ONUs descobertas.

Devem ser incluídos no autoprovisionamento os perfis criados do GPON, assim como também é possível utilizar os perfis default carregados.



Cenário para Serviço de Acesso a Internet usando a Service-VLAN N:1

Suponha que o usuário deseje que todas as ONUs que forem descobertas no ramo PON sejam automaticamente configuradas com os perfis previamente configurados.

O procedimento a seguir apresenta a configuração necessária para ativar o provisionamento automático.

```
config
gpon 1/1
onu-auto-provisioning
enable
line-profile <DEFAULT-LINE>
ethernet 1
veip 1
service-port 1 gem 1 match vlan vlan-id <VLAND-ID> action vlan add vlan-id <VLAND-ID>
!
commit
```

Alternativamente, caso seja necessário configurar o provisionamento automático para apenas uma interface GPON, os seguintes comandos devem ser utilizados:

```
config
interface gpon 1/1/1
onu-auto-provisioning
enable
line-profile <DEFAULT-LINE>
ethernet 1
veip 1
```

```

    service-port 1 gem 1 match vlan vlan-id <VLAN-ID> action vlan add vlan-id <VLAN-ID>
    !
    !
    !
    commit

```



A configuração de provisionamento automático por PONLINK tem precedência sobre a Global. Ambas podem coexistir no mesmo equipamento, porém a global só será utilizada na interface quando não houver configuração desta funcionalidade para esta interface.



A porta de serviço (service-port) deve ser criada para cada GEM que o usuário queira configurar. É possível configurar até 16 service-ports no autoprovisionamento, os quais serão aplicados em todas as ONUs descobertas.

Abaixo a configuração completa para a aplicação com provisionamento automático de forma Global:

```

config
dot1q
vlan 100
    interface gigabit-ethernet-1/1/1
    !
    !
    service vlan 100 type n:1
    !
    profile gpon bandwidth-profile DEFAULT-BANDWIDTH
    traffic type-4 max-bw 1106944
    !
    profile gpon line-profile DEFAULT-LINE
    upstream-fec
    tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
    gem 1
        tcont 1 priority 0
        map any-ethernet
            ethernet any vlan any cos any
        !
        map any-veip
            veip 1 vlan 100 cos any
        !
    gem 2
        tcont 1 priority 0
        map any-iphost
            iphost vlan any cos any
    !
    !
    profile gpon snmp-profile DEFAULT-SNMP
    if-type
    if-descr
    if-oper-status
    if-onu-power-rx
    statistics-in-bw-usage
    statistics-out-bw-usage
    !
    interface gpon 1/1/1
    no shutdown
    !
    gpon 1/1
    onu-auto-provisioning
        enable
        line-profile DEFAULT-LINE
        snmp-profile DEFAULT-SNMP
        ethernet 1
        veip 1
        service-port 1 gem 1 match vlan vlan-id 100 action vlan add vlan-id 100
    !
    !
    commit

```

7.6.1 Verificando o provisionamento automático

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



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

```
show running gpon
show interface gpon onu
show interface gpon <chassis/slot/port> onu <id>
```

8 Switching

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) por um identificador de 1 a 4094.

Este capítulo contém as seguintes seções:

- Configuração da Tabela MAC
- Configuração de VLAN
- Configuração do RSTP
- Configuração do MSTP
- Configuração do EAPS
- Configuração do ERPS
- Configuração do L2CP
- Configuração do Loopback Detection
- Configuração do DHCP Relay L2

8.1 Configuração da Tabela MAC

8.1.1 Configurando o tempo de Aging

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. O valor padrão do aging time é 600 segundos.

Os próximos passos irão demonstrar como configurar o aging time para o valor de **300** segundos.

```
config
mac-address-table aging-time 300
commit
```



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

8.1.2 Desativando o aprendizado de endereços MAC

Por padrão, o aprendizado de endereço MAC está ativado em todas as interfaces dos switches DmOS. O usuário pode controlar o aprendizado de endereços MAC em uma interface, controlando qual interface pode aprender os endereços MAC.



Desativar o aprendizado de endereços MAC em uma interface pode fazer com que sejam gerados floods na rede, fazendo com que pacotes sejam encaminhados desnecessariamente.

Os comando a seguir irão exemplificar como desabilitar o aprendizado do endereço MAC na interface gigabit-ethernet 1/1/6 de um switch DmOS.

```
config
mac-address-table interface gigabit-ethernet-1/1/6 learning disabled
commit
```



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

8.1.3 Verificando a tabela MAC

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



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

```
show mac-address-table
show mac-address-table interface <INTERFACE>
show mac-address-table mac-address <MAC_ADDRESS>
show mac-address-table type <STATIC/DYNAMIC>
show mac-address-table vlan <VLAN_ID>
show running-config mac-address-table interface learning
```

8.2 Configuração de VLAN

8.2.1 Configurando VLANs 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 1/1/1 e Gigabit Ethernet 1/1/2 usando modo tagged.

```
config
dot1q
vlan 200
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
```



Por padrão, caso o usuário não especifique o modo da interface na VLAN, o modo utilizado será o **tagged**.

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 ten-gigabit-ethernet 1/1/1 em modo tagged.

```
config
dot1q
vlan 1500-2000
name TRAFEGO
interface ten-gigabit-ethernet-1/1/1 tagged
commit
```



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

8.2.2 Configurando VLANs 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 através da configuração de switchport.

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

```

config
dot1q
vlan 200
interface gigabit-ethernet-1/1/1 untagged
interface gigabit-ethernet-1/1/2 untagged
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 200
!
!
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 200
commit

```

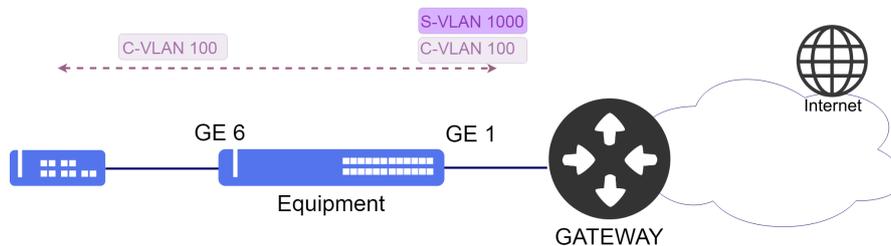


Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando a configuração de VLAN](#).

8.2.3 Configurando 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.



Implementando o QinQ

Os próximos passos irão demonstrar como configurar o QinQ para transportar um cliente conectado a interface Gigabit-Ethernet-1/1/6. O cliente possui uma **VLAN (C-VLAN) 100** e será transportado através da rede do provedor de serviço com a **VLAN (S-VLAN) 1000**.



Para configurar o QinQ é necessário configurar a interface de forma untagged e ativando a opção QinQ através da configuração de switchport.

```

config
dot1q
vlan 1000
interface gigabit-ethernet-1/1/1 tagged

```

```

interface gigabit-ethernet-1/1/6 untagged
!
switchport
interface gigabit-ethernet-1/1/6
  qinq
  native-vlan vland-id 1000
commit

```

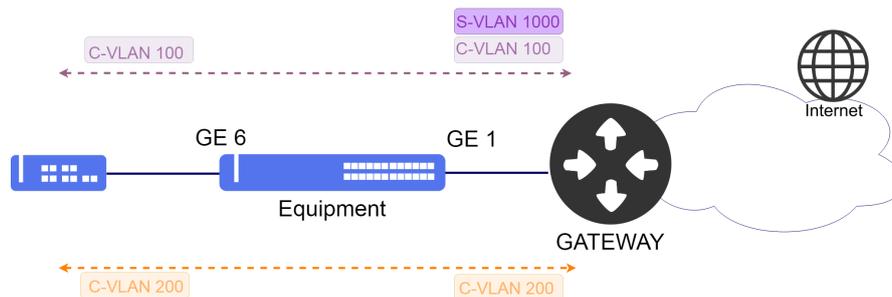


Não há comandos de troubleshooting para esta funcionalidade.

8.2.4 Configurando QinQ Seletivo

O QinQ seletivo possui a mesma lógica do QinQ padrão, porém, adiciona uma nova VLAN no tráfego que entra em uma interface apenas para as VLAN de clientes especificadas (C-VLANs). Esta funcionalidade tem por objetivo criar VLANs de serviços (S-VLANs) para separar clientes (C-VLANs) que divergem no tipo de serviço contratado como, por exemplo, o QoS.

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



Implementação do QinQ Seletivo

Suponha que o usuário queira configurar dois diferentes clientes. Ambos conectados a interface gigabit-ethernet-1/1/6, porém, o cliente com a VLAN 100 (C-VLAN) será transportado de forma transparente dentro da rede do provedor de serviços através da VLAN 1000 (S-VLAN) e o segundo cliente terá a VLAN 200 (C-VLAN) mantida. Os próximos passos irão demonstrar como configurar o QinQ seletivo.



A configuração do QinQ Seletivo se dá através da funcionalidade de mapeamento de VLANs (vlan-mapping), utilizando a action **add**.

```

config
dot1q
vlan 200
  interface gigabit-ethernet-1/1/1 tagged
  interface gigabit-ethernet-1/1/6 tagged
!
vlan 1000
  interface gigabit-ethernet-1/1/1 tagged
  interface gigabit-ethernet-1/1/6 untagged
!
vlan-mapping
  interface gigabit-ethernet-1/1/6

```


8.2.6 Verificando a configuração de VLAN

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



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

```
show vlan brief
show vlan detail
show vlan membership detail
```

8.3 Configuração do RSTP

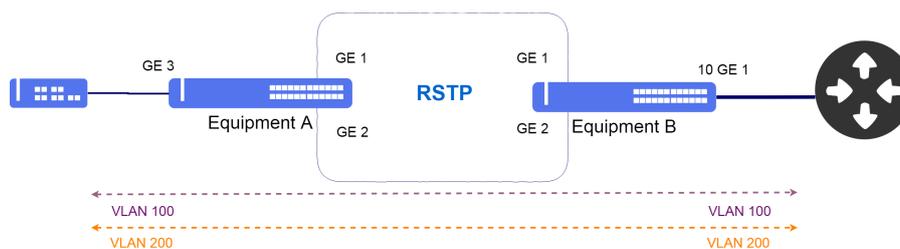
O protocolo RSTP (Rapid Spanning Tree Protocol) definido pela norma IEEE 802.1w é utilizado para fornecer um caminho único na rede, eliminando loops entre os equipamentos.



As BPDU do RSTP são encaminhadas sem a presença de VLAN (untagged).

8.3.1 Configurando um RSTP Básico

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



Implementação do RSTP

Suponha que o usuário queira realizar as seguintes configurações:

- **Equipment A:** VLAN ID 100 e 200 para tráfego com a interface gigabit-ethernet-1/1/3 como interface de acesso.
- **Equipment B:** VLAN ID 100 e 200 para tráfego com a interface ten-gigabit-ethernet-1/1/1 como interface de uplink.

```
!Equipment A
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
interface gigabit-ethernet-1/1/3 tagged
!
```

```
vlan 200
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
interface gigabit-ethernet-1/1/3 tagged
!
!
spanning-tree
interface gigabit-ethernet-1/1/1
interface gigabit-ethernet-1/1/2
commit
```

```
!Equipment B
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
interface ten-gigabit-ethernet-1/1/1 tagged
!
vlan 200
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
interface ten-gigabit-ethernet-1/1/1 tagged
!
!
spanning-tree
interface gigabit-ethernet-1/1/1
interface gigabit-ethernet-1/1/2
commit
```

8.3.2 Aplicando os parâmetros do RSTP

Caso necessário, o usuário pode alterar parâmetros default do Spanning Tree ou habilitar parâmetros que não estão disponíveis na configuração padrão do Spanning Tree.

Abaixo a lista de parâmetros que podem ser modificados nas interfaces do Spanning Tree:

- **auto-edge:** Caso não receba BPDUs, a interface entrará automaticamente para o estado edge port e não transmitirá BPDUs.
- **edge-port:** Quando configurado, a interface não transmitirá BPDUs. O valor padrão é auto-edge.
- **bpdu-guard:** A interface entrará no estado de encaminhamento mas não transmitirá BPDUs, a menos que uma BPDU seja recebida por essa interface. Este comando se aplica somente para interfaces que já foram configuradas como edge-port.
- **cost:** Permite alterar o custo do caminho da interface para cálculos do STP. Por padrão, esse valor está associado à velocidade do link.
- **link-type:** Configura a interface para informar se o segmento de LAN é ponto a ponto ou ponto multiponto. O valor padrão é auto.
- **port-priority:** Configura a prioridade da interface para alterar a probabilidade de se tornar uma Root Port. O valor padrão é 128.
- **restricted-role:** Configura a interface para não ser selecionada como Root Port de uma topologia STP.
- **restricted-tcn:** Configura a interface para não propagar as notificações recebidas de alteração da topologia STP.

Os próximos passos irão demonstrar como configurar a interface gigabit-ethernet-1/1/1 como edge-port.



Para configurar os demais parâmetros listados acima, o procedimento é o mesmo utilizado no exemplo abaixo.

```
config
spanning-tree
interface gigabit-ethernet-1/1/1 edge-port
commit
```



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

8.3.3 Verificando o RSTP

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



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

```
show spanning-tree
show spanning-tree brief
show spanning-tree detail
show spanning-tree extensive
```

8.4 Configuração do MSTP

O protocolo MSTP (Multiple Spanning Tree Protocol) definido pela norma IEEE 802.1s é utilizado para fornecer um caminho único na rede, eliminando loops entre os equipamentos. O protocolo tem a vantagem em relação ao RSTP de proporcionar um balanceamento do tráfego através das múltiplas instâncias MSTI ajustando os custos das portas para que o balanceamento do tráfego seja eficiente.



O grupo de VLANs protegido em uma MSTI somente poderá ter overlap com o grupo de VLANs protegido pelos protocolos EAPS e ERPS se as VLANs forem exatamente as mesmas.



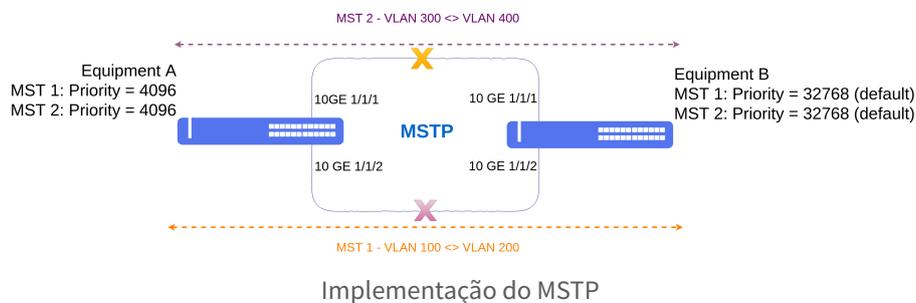
Não pode ter overlap de VLANs entre as MSTIs.



As VLANs de controle do ERPS e EAPS não podem fazer parte de uma MSTI.

8.4.1 Configurando o MSTP para balanceamento do tráfego

O cenário abaixo será usado para demonstrar a configuração do MSTP para que o balanceamento do tráfego seja eficiente.



Suponha que o usuário queira realizar as seguintes configurações:

Equipment A

- **MST 1:** Priority 4096 e VLAN ID 100 até 200. Port-priority = 32 na ten-gigabit-ethernet-1/1/2.
- **MST 2:** Priority 4096 e VLAN ID 300 até 400.

Equipment B

- **MST 1:** Priority 32768 (default) e VLAN ID 100 até 200.
- **MST 2:** Priority 32768 (default) e VLAN ID 300 até 400.

Ambos os equipamentos usam as interfaces ten-gigabit-ethernet 1/1/1 e ten-gigabit-ethernet 1/1/2 para formar a topologia MSTP com os seguintes parâmetros: **name = datacom** e **revision = 12345**.



Os parâmetros **name** e **revision** devem ser os mesmos em todos os equipamentos que participam da topologia MSTP.



As interfaces presentes na CIST são necessárias nas instâncias MSTI apenas se houver necessidade de configurar os parâmetros específicos como **cost** e **port-priority**.

```
!Equipment A
config
dot1q
vlan 100-200,300-400
  interface ten-gigabit-ethernet-1/1/1
  !
  interface ten-gigabit-ethernet-1/1/2
  !
!
spanning-tree
mode mstp
name datacom
revision 12345
interface ten-gigabit-ethernet-1/1/1
  auto-edge
!
interface ten-gigabit-ethernet-1/1/2
  auto-edge
!
mst 1
  priority 4096
  vlan 100-200
  interface ten-gigabit-ethernet-1/1/2
    port-priority 32
!
mst 2
  priority 4096
  vlan 300-400
commit
```

```
!Equipment B
config
dot1q
vlan 100-200,300-400
  interface ten-gigabit-ethernet-1/1/1
  !
  interface ten-gigabit-ethernet-1/1/2
  !
!
spanning-tree
mode mstp
name datacom
revision 12345
interface ten-gigabit-ethernet-1/1/1
  auto-edge
!
interface ten-gigabit-ethernet-1/1/2
  auto-edge
!
mst 1
  vlan 100-200
!
mst 2
  vlan 300-400
commit
```



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

8.4.2 Verificando o MSTP

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



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

```
show spanning-tree
show spanning-tree brief
show spanning-tree detail
show spanning-tree extensive
```

8.5 Configuração do 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.



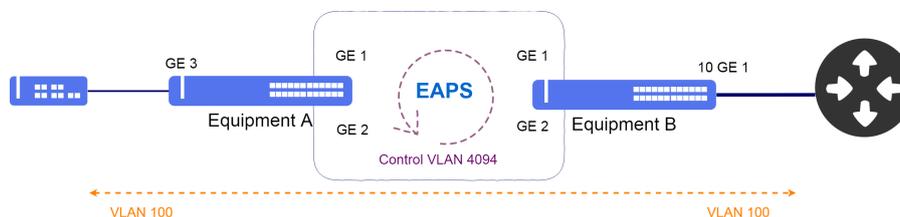
O protocolo EAPS funciona adequadamente apenas em topologias em anel.



O grupo de VLANs protegido em uma instância EAPS somente poderá ter overlap com o grupo de VLANs protegido pelos protocolos MSTP e ERPS se as VLANs forem exatamente as mesmas.

8.5.1 Configurando um Anel EAPS Básico

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



Implementação do EAPS

Suponha que o usuário queira realizar as seguintes configurações:

- **Equipment A:** VLAN 100 para tráfego com a interface gigabit-ethernet-1/1/3 como interface de acesso e a VLAN 4094 para VLAN de controle do EAPS em modo transit através das interfaces gigabit-ethernet-1/1/1 e 1/1/2.
- **Equipment B:** VLAN 100 para tráfego com a interface tem-gigabit-ethernet-1/1/1 como interface de uplink e a VLAN 4094 para VLAN de controle do EAPS em modo master através das interfaces gigabit-ethernet-1/1/1 e 1/1/2.

```
!Equipment A
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
interface gigabit-ethernet-1/1/3 tagged
!
vlan 4094
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 tagged
!!
```

```
!
eaps 0
control-vlan 4094
protected-vlans 100
port
  primary gigabit-ethernet-1/1/1
  secondary gigabit-ethernet-1/1/2
!
!
mode transit
commit
```

```
!Equipment B
config
dot1q
vlan 100
  interface gigabit-ethernet-1/1/1 tagged
  interface gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/1 tagged
!
vlan 4094
  interface gigabit-ethernet-1/1/1 tagged
  interface gigabit-ethernet-1/1/2 tagged
!
!
!
eaps 0
control-vlan 4094
protected-vlans 100
port
  primary gigabit-ethernet-1/1/1
  secondary gigabit-ethernet-1/1/2
!
!
mode master
commit
```



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

8.5.2 Verificando o EAPS

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



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

```
show eaps
show eaps brief
show eaps detail
```

8.6 Configuração do ERPS

O protocolo ERPS (Ethernet Ring Protection Switching) definido pela norma ITU-U G.8032 é utilizado para fornecer um caminho único na rede, evitando e eliminando loops entre os equipamentos.

A inibição de loop em um anel Ethernet é realizada assegurando que um segmento fique sem passar tráfego, ou seja,

bloqueado. O protocolo ERPS utiliza uma porta denominada RPL Owner responsável por bloquear todo o tráfego, exceto os pacotes de controle do protocolo.



É recomendado usar a interface adjacente interligada ao RPL Owner como RPL Neighbor. Esta configuração é opcional, porém, auxilia a RPL Owner no bloqueio do tráfego do link.



É obrigatório configurar "ring-id 1" caso seja necessário interoperar com outros produtos DATACOM e outros vendors que possuam ERPSv1.



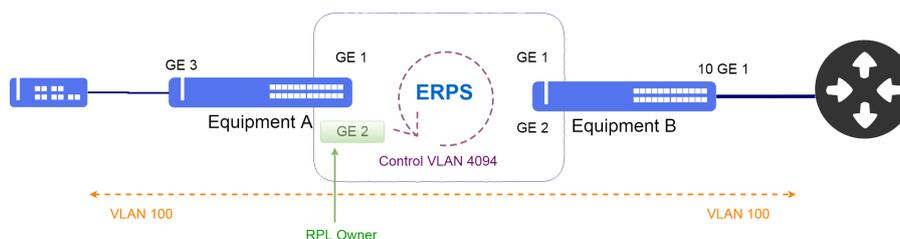
O grupo de VLANs protegido em uma instância ERPS somente poderá ter overlap com o grupo de VLANs protegido pelos protocolos MSTP e EAPS se as VLANs forem exatamente as mesmas.



Em cenários que tenha DWDM, SDH ou outra tecnologia de transporte dados que não propague a queda do link, é necessário utilizar o Ethernet OAM ou CFM com MEP DOWN para que ocorra a convergência do ERPS em caso de falha da tecnologia usada.

8.6.1 Configurando o ERPS Single Ring

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



Implementação do ERPS Single Ring

Suponha que o usuário queira realizar as seguintes configurações:

- **Equipment A:** VLAN 100 para tráfego com a interface gigabit-ethernet-1/1/3 como interface de acesso e a VLAN 4094 para VLAN de controle do ERPS e a interfaces gigabit-ethernet-1/1/2 como RPL-Owner.
- **Equipment B:** VLAN 100 para tráfego com a interface ten-gigabit-ethernet-1/1/1 como interface de uplink e a VLAN 4094 para VLAN de controle do ERPS.

```
!Equipment A
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1 tagged
```




Os equipamentos de interconexão dos anéis deverão ser configurados na instância do sub-ring como nó de interconexão através do comando **node interconnection** e precisam indicar qual o anel ERPS é o seu anel principal através do comando **parent-ring**.



O canal virtual deverá ter sua própria VLAN de controle.

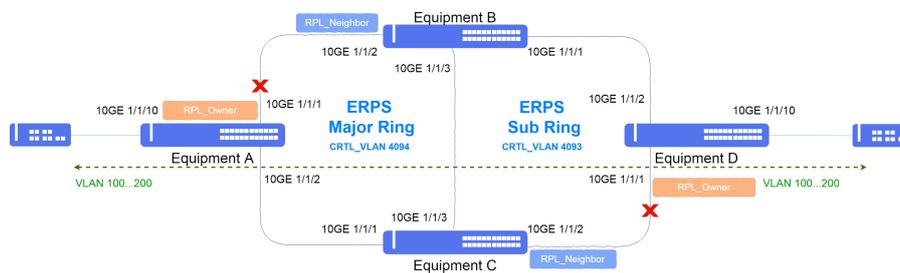


Nesta versão do DmOS, a VLAN de controle do canal virtual não poderá ser igual a VLAN de controle do sub-ring.



Nesta versão do DmOS, é necessário realizar o mapeamento da VLAN de controle dos sub-rings nos equipamentos de interconexão que realizam o canal virtual através do **vlan-mapping**.

O cenário abaixo será usado para demonstrar a configuração do ERPS utilizando topologia com múltiplos anéis.



Implementação do ERPS Multi-Ring

Suponha que o usuário queira proteger o grupo de VLANs 100 a 200 com o uso de um anel principal (Major Ring) utilizando a VLAN de controle 4094 e um anel secundário (Sub-ring) utilizando a VLAN de controle 4093. Um canal virtual (Virtual Channel) será configurado com o uso da VLAN de controle 4000 e será protegida no anel principal.

- **Equipment A:** Grupo de VLANs 100 a 200 serão protegidas para o tráfego de dados. A interface ten-gigabit-ethernet-1/1/10 será utilizada como interface de acesso. As interfaces ten-gigabit-ethernet-1/1/1 e ten-gigabit-ethernet-1/1/2 serão utilizadas no anel principal, onde a interface ten-gigabit-ethernet-1/1/1 será utilizada como RPL Onwer.
- **Equipment B:** Grupo de VLANs 100 a 200 serão protegidas para o tráfego de dados. As interfaces ten-gigabit-ethernet-1/1/2 e ten-gigabit-ethernet-1/1/3 serão utilizadas no anel principal e a interface ten-gigabit-ethernet-1/1/1 será utilizada no sub anel. O canal virtual será uma VLAN protegida no anel principal, ou seja, entre os equipamentos A, B e C.
- **Equipment C:** Grupo de VLANs 100 a 200 serão protegidas para o tráfego de dados. As interfaces ten-gigabit-

ethernet-1/1/1 e ten-gigabit-ethernet-1/1/3 serão utilizadas no anel principal e a interface ten-gigabit-ethernet-1/1/2 será utilizada no sub anel. O canal virtual será uma VLAN protegida no anel principal, ou seja, entre os equipamentos A, B e C.

- **Equipment D:** Grupo de VLANs 100 a 200 serão protegidas para o tráfego de dados. A interface ten-gigabit-ethernet-1/1/10 será utilizada como interface de acesso. As interfaces ten-gigabit-ethernet-1/1/1 e ten-gigabit-ethernet-1/1/2 serão utilizadas no sub anel, onde a interface ten-gigabit-ethernet-1/1/1 será utilizada como RPL Owner.

```

!Equipment A
config
dot1q
vlan 100-200
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/10 tagged
!
vlan 4000
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
!
vlan 4094
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
!
!
!
erps
ring ERPS-MAJOR
  ring-id 1
  control-vlan 4094
  protected-vlans 100-200,4000
  port0
    interface ten-gigabit-ethernet-1/1/1 rpl-role owner
  !
  port1
    interface ten-gigabit-ethernet-1/1/2
  !
!
!
commit

```

```

!Equipment B
config
dot1q
vlan 100-200
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/3 tagged
!
vlan 4000
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/3 tagged
!
vlan 4093
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/3 tagged
!
vlan 4094
  interface ten-gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/3 tagged
!
!
vlan-mapping
interface ten-gigabit-ethernet-1/1/1
  egress
    rule ERPS-rule-1
      match vlan vlan-id 4000
      action replace vlan vlan-id 4093 pcp 0
    !
  !
!
interface ten-gigabit-ethernet-1/1/2
  egress
    rule ERPS-rule-2
      match vlan vlan-id 4093
      action replace vlan vlan-id 4000 pcp 0
    !
  !
!

```



```

ring-id 1
control-vlan 4094
protected-vlans 100-200,4000
port0
  interface ten-gigabit-ethernet-1/1/1
  !
port1
  interface ten-gigabit-ethernet-1/1/3
  !
!
ring ERPS-SUBRING
ring-id 1
control-vlan 4093
protected-vlans 100-200,4000
type sub-ring
node interconnection
parent-ring ERPS-MAJOR
port0
  interface ten-gigabit-ethernet-1/1/2 neighbor
  !
port1
  virtual-channel control-vlan 4000
  !
!!
!
commit

```

```

!Equipment D
config
dot1q
vlan 100-200
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
  interface ten-gigabit-ethernet-1/1/10 tagged
  !
vlan 4093
  interface ten-gigabit-ethernet-1/1/1 tagged
  interface ten-gigabit-ethernet-1/1/2 tagged
  !
!
!
erps
ring ERPS-SUBRING
ring-id 1
control-vlan 4093
protected-vlans 100-200
type sub-ring
port0
  interface ten-gigabit-ethernet-1/1/2
  !
port1
  interface ten-gigabit-ethernet-1/1/1 rpl owner
  !
!!
!
commit

```



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

8.6.3 Verificando o ERPS

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



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

```
show erps
show erps brief
```

8.7 Configuração do L2CP

O protocolo L2CP (Layer 2 Control Protocol) é utilizado para fornecer serviços LAN-to-LAN de forma transparente através de uma rede de tal forma que equipamentos centrais da rede não processem as PDUs.



O protocolo L2CP somente é suportado nos Switches.



O DmOS suporta o **L2CP** no modo de configuração **extended** e através protocolos **CDP, Dot1x, EAPS, ERPS, GVRP, LACP, LLDP, Marker, OAM, PAgP, PVST, STP, UDLD e VTP**.



O modo de configuração extended é proprietário, para interoperabilidade utilizar o L2CP por protocolo.



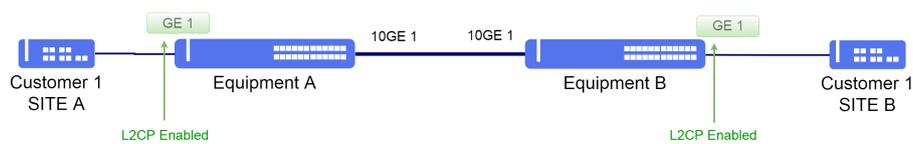
O modo de configuração por protocolo tem precedência sobre o modo estendido.

8.7.1 Configurando o L2CP no modo extended

O modo estendido do L2CP compreende o seguintes endereços MAC:

Tipo da PDU	MAC Address
IEEE	01:80:C2:00:00:0X e 01:80:C2:00:00:2X
EAPS	00:E0:2B:00:00:04
RRPP	00:0F:E2:07:82:XX
Protocolos Cisco	01:00:0C:CC:XX:XX e 01:00:0C:CD:XX:XX

O cenário abaixo será usado para demonstrar a configuração do protocolo L2CP no modo extended. Esta configuração é utilizada quando duas redes privadas de um mesmo cliente estão conectadas pela rede do ISP e este cliente necessita que os protocolos L2 rodem como uma única rede entre as redes privadas.



Implementação do L2CP

Suponha que o usuário queira utilizar as seguintes configurações em ambos os equipamentos:

- VLAN ID 100 para Customer 1 com interface gigabit-ethernet-1/1/1 como interface de acesso e interface ten-gigabit-ethernet-1/1/1 como interface de uplink. O L2CP é ativado na interface de acesso.

```
config
dot1q
vlan 100
interface ten-gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/1 untagged
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 100
!
!
layer2-control-protocol
interface gigabit-ethernet-1/1/1
extended action tunnel
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o L2CP](#).

8.7.2 Configurando o L2CP por protocolo específico

Utilizando o cenário [Configuring L2CP in extended mode](#) como base é possível alterar a configuração do L2CP por protocolo invés do modo extended em ambos os equipamentos.

```
config
layer2-control-protocol interface gigabit-ethernet-1/1/1 cdp action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 dot1x action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 eaps action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 erps action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 gvrp action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 lacp action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 lldp action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 marker action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 oam action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 pagp action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 pvst action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 stp action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 udld action tunnel
layer2-control-protocol interface gigabit-ethernet-1/1/1 vtp action tunnel
commit
```

Caso seja necessário interoperabilidade com outro fabricante que utiliza o MAC de destino (01:00:0C:CD:CD:D0) no L2CP utilizar o comando abaixo.

```
config
layer2-control-protocol tunnel-mac interop
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o L2CP](#).

8.7.3 Configurando a transparência de PDUs

É possível habilitar a transparência de PDUs utilizando a funcionalidade L2CP usando o comando abaixo. Esta funcionalidade encaminha as PDUs sem alterar as informações da PDU, por este motivo todos os switches do caminho devem suportar a transparência de PDUs.



É necessário configurar a transparência de PDU em todos equipamentos do caminho.

Utilizando o cenário [Configuring L2CP in extended mode](#) como base é possível alterar a configuração do L2CP para utilizar transparência de PDUs invés de tunelamento pelo modo extended.

```
config
layer2-control-protocol interface gigabit-ethernet-1/1/1 extended action forward
layer2-control-protocol interface ten-gigabit-ethernet-1/1/1 extended action forward
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o L2CP](#).

8.7.4 Verificando o L2CP

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



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

```
show running-config layer2-control-protocol
debug enable l2cp-tunneling
```

8.7.5 Comportamento default das PDUs nas OLTs



Nas plataformas DM461x com suporte a tecnologia GPON a transparência de PDUs L2 em serviços TLS (service vlan type TLS) está ativada sem a possibilidade de alterar este comportamento. Já para serviços 1:1 e N:1 (service vlan type 1:1 ou n:1) a transparência de PDUs L2 está desativada sem a possibilidade de alterar este comportamento.

A tabela abaixo resume o comportamento da transparência de PDUs L2 nas plataformas DM461x para cada tipo de serviço GPON.

Tipo da PDU	MAC Address	Serviço TLS	Serviço N:1 ou 1:1
IEEE	01:80:C2:00:00:0X e 01:80:C2:00:00:2X	Encaminhar	Bloquear
EAPS	00:E0:2B:00:00:04	Encaminhar	Encaminhar
ERPS	01:19:A7:<ring-id>	Encaminhar	Encaminhar
RRPP	00:0F:E2:07:82:XX	Encaminhar	Encaminhar
Protocolos Cisco	01:00:0C:CC:XX:XX e 01:00:0C:CD:XX:XX	Encaminhar	Encaminhar

8.7.6 Comportamento default das PDUs nos Switches

Para as demais plataformas, as actions **tunnel** e **forward** são suportadas. A tabela abaixo resume o comportamento padrão do tratamento das PDUs caso o L2CP não esteja configurado.

Tipo da PDU	MAC Address	Ação Padrão
IEEE	01:80:C2:00:00:0X e 01:80:C2:00:00:2X	Bloquear
EAPS	00:E0:2B:00:00:04	Encaminhar
ERPS	01:19:A7:<ring-id>	Encaminhar
RRPP	00:0F:E2:07:82:XX	Encaminhar
Protocolos Cisco	01:00:0C:CC:XX:XX e 01:00:0C:CD:XX:XX	Encaminhar

8.8 Configuração do Loopback Detection

O Loopback Detection (LBD) detecta loop enviando periodicamente PDUs em uma interface verificando se estas PDUs são recebidas na mesma interface. Caso o loop for detectado, as seguintes ações irão ocorrer:

- A interface é bloqueada.
- Um alarme é ativado.

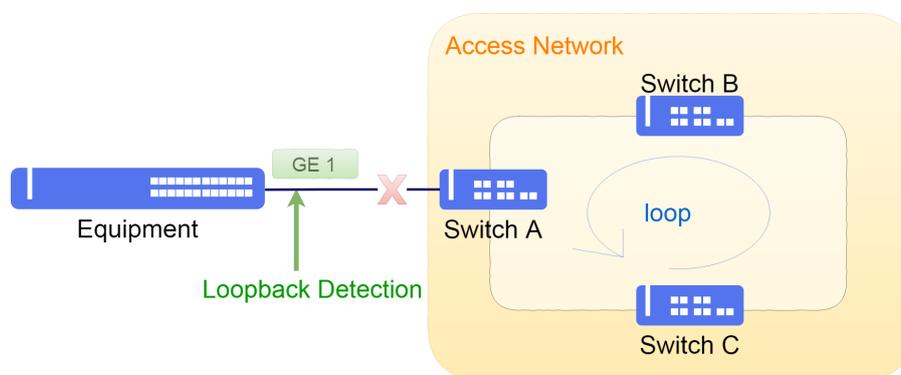
- Um log é registrado.
- Uma trap SNMP é enviada para o servidor SNMP configurado.



A configuração de Loopback Detection não é suportada em portas membro do LAG.

8.8.1 Configurando Loopback Detection para a rede de acesso

No cenário abaixo, conforme mostrado, ocorre um loop na rede de acesso conectada ao equipamento. Os pacotes enviados de uma interface são enviados de volta para essa interface.



Cenário com loop

Os próximos passos irão demonstrar como habilitar a detecção de loopback em uma interface.

```
config
loopback-detection
interface gigabit-ethernet-1/1/1
commit
```



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

8.8.2 Verificando o Loopback Detection

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



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

```
debug enable loopback-detection
show alarm
```

8.9 Configuração do DHCP Relay L2

O DHCP Relay L2 realiza o snooping de pacotes DHCP para fins de segurança e gerenciamento de assinantes, mantendo o controle dos IP atribuídos por um servidor DHCP confiável aos dispositivos de rede não confiáveis. A opção DHCP option 82 anexada pelo agente de retransmissão pode ser usada para manter a rastreabilidade do usuário e fornecer a configuração de rede com base na localização de clientes de rede.



A configuração padrão tem o DHCP desativado.



Atualmente, a funcionalidade DHCP Relay somente está disponível nas plataformas DM461x com suporte a tecnologia GPON.

Para habilitar o DHCP Relay na VLAN 20 o usuário deverá realizar o seguinte procedimento:

```
config
dhcp l2-relay vlan 20
commit
```



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

8.9.1 Verificando o DHCP Relay

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



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

```
show allowed-ip entry-type dhcp
```

9 Serviços IP

Este capítulo demonstra como realizar configurações básicas de interfaces L3, endereços IPv4 e IPv6. Também aborda a configuração de serviços IP.

Este capítulo contém as seguintes seções:

- Configuração de Endereços IP
- Configuração do IPv6 SLAAC
- Configuração do DHCP Relay L3

9.1 Configuração de Endereços IP

O usuário pode configurar endereços IPv4 e IPv6 manualmente nas interfaces de gerência, L3 e loopback.

9.1.1 Configurando endereços IPv4

Os passos a seguir demonstram como configurar o endereço IPv4 **10.10.0.1/30** em uma interface L3 associada à VLAN 2.

```
config
dot1q
vlan 2
  interface gigabit-ethernet-1/1/1 untagged
  !
  !
switchport
interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 2
  !
  !
interface l3 VLAN2
  ipv4 address 10.10.0.1/30
  lower-layer-if vlan 2
commit
```



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

9.1.2 Configurando endereços IPv6

Os passos a seguir demonstram como configurar o endereço IPv6 **2001::a0a:1/126** em uma interface L3 associada à VLAN 2.

```
config
dot1q
vlan 2
  interface gigabit-ethernet-1/1/1 untagged
  !
  !
switchport
interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 2
```

```
!
!
interface l3 VLAN2
  lower-layer-if vlan 2
  ipv6 enable
  ipv6 address 2001::a0a:1/126
commit
```



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

9.1.3 Verificando os endereços IP

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



Para maiores detalhes sobre as saídas dos comandos, consultar o [Command Reference](#).

```
show ip interface brief
show ipv6 interface brief
```

9.1.4 Configurando MTU em interfaces L3

Também é possível configurar MTU em interfaces L3. Neste caso, a restrição de MTU irá ocorrer apenas para pacotes no plano de controle, ou seja, pacotes direcionados à CPU do equipamento

No exemplo abaixo, é configurado MTU de 2000 bytes na interface VLAN2.

```
config
interface l3 VLAN2
  ip-mtu 2000
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

9.2 Configuração do IPv6 SLAAC

O SLAAC (IPv6 Stateless Address Autoconfiguration) permite que uma ou mais interfaces do equipamento forneçam informações de prefixos IPv6 a hosts conectados a estas interfaces sem necessidade de utilizar um servidor DHCPv6 ou configurar o endereço manualmente.

Sua operação é baseada na troca de mensagens do tipo **RA (Router Advertisement)** e **RS (Router Solicitation)**, permitindo que os clientes usem as informações recebidas nestas mensagens para configurarem de forma automática os seus próprios endereços IPv6.



O SLAAC está disponível para interfaces L3 e interface MGMT.



Por padrão, o **lifetime** das mensagens RA é de **1800** segundos. Caso a interface do equipamento não deva ser utilizada como rota default, o lifetime deve ser configurado como 0. O **lifetime** não está disponível para a interface MGMT, pois ela não pode ser utilizada como rota default.

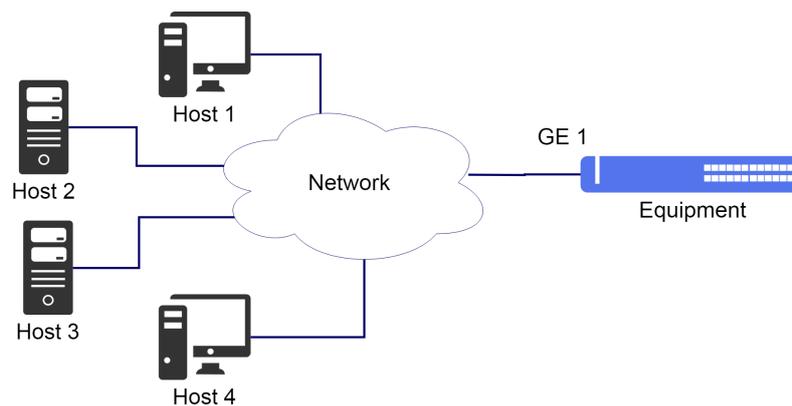


Por padrão, uma vez que o comando "ipv6 enable" for configurado em uma interface, as mensagens de RA passarão a ser enviadas para todos os clientes que pertencem ao domínio de broadcast conectado a esta interface. A informação de prefixo de rede somente será preenchida nas mensagens de RA após a configuração do "ipv6 address <x:x:x::y/64>" ou do "ipv6 nd ra prefix <x:x:x::/64>".



Para funcionamento com SLAAC, é necessário que o endereço IPv6 tenha prefixo /64.

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



Implementação do SLAAC

Suponha que o usuário deseje utilizar o prefixo **2222::/64** em um domínio de rede específico. Para isso, o SLAAC pode ser ativado para propagar este prefixo de rede para todos os hosts conectados neste domínio através da interface L3 **SLAAC-1**. Os próximos passos irão mostrar como realizar a configuração.

```
config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1 untagged
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 10
!
!
interface l3 SLAAC-1
lower-layer-if vlan 10
ipv6 enable
ipv6 nd ra prefix 2222::/64
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o IPv6 SLAAC](#).

9.2.1 Verificando o IPv6 SLAAC

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



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

```
debug enable ipv6-nd-rx
debug enable ipv6-nd-tx
```

9.3 Configuração do DHCP Relay L3

É possível realizar o encaminhamento de mensagens de DHCP entre dois domínios broadcast por intermédio de um DHCP Relay. As mensagens de broadcast geradas pelo cliente (DHCP Discovery e Request) são recebidas pelo switch encarregado de realizar o relay. Essas mensagens são convertidas de broadcast para unicast e encaminhadas diretamente ao servidor DHCP. O funcionamento do serviço de DHCP relay depende da rede local estar configurada com uma VLAN e endereço IP, assim como a rede pela qual o switch irá alcançar o servidor DHCP, conforme demonstrado em [Configuração de Endereços IP](#).

O DHCP possui algumas configurações adicionais que fornecem uma maior segurança na alocação de endereços. Estas opções podem ser configuradas de forma global no relay ou separadamente por interface.

- **information option:** Insere a Option 82 ao frame referente à interface na qual foi recebido;
- **information trust-all:** Aceita frames que já chegam com marcação de Option 82;

- **information policy keep:** Mantém a marcação da Option 82 recebida quando já vem com essa marcação.



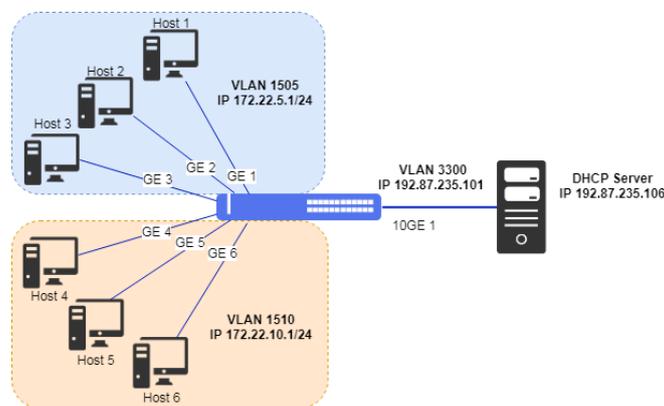
Caso seja configurado a Option 82 de forma global e na interface, as configurações da interface tem preferência.



Para maiores detalhes sobre outros parâmetros da Option 82, consultar o **Command Reference**.

9.3.1 Configurando o DHCP Relay L3

A topologia abaixo exemplifica uma aplicação para o serviço de DHCP relay:



Cenário do DHCP Relay L3

Os passos a seguir demonstram como configurar o serviço de DHCP relay L3 para os clientes da VLAN 1505 e da VLAN 1510 com destino a um servidor DHCP na VLAN 3300:

```
config
dot1q
vlan 1505
interface gigabit-ethernet-1/1/1
untagged
interface gigabit-ethernet-1/1/2
untagged
interface gigabit-ethernet-1/1/3
untagged
!
vlan 1510
interface gigabit-ethernet-1/1/4
untagged
interface gigabit-ethernet-1/1/5
untagged
interface gigabit-ethernet-1/1/6
untagged
!
vlan 3300
interface ten-gigabit-ethernet-1/1/1
!
!
!
switchport interface gigabit-ethernet-1/1/1 native-vlan vlan-id 1505
!
switchport interface gigabit-ethernet-1/1/2 native-vlan vlan-id 1505
!
switchport interface gigabit-ethernet-1/1/3 native-vlan vlan-id 1505
```

```
!
switchport interface gigabit-ethernet-1/1/4 native-vlan vlan-id 1510
!
switchport interface gigabit-ethernet-1/1/5 native-vlan vlan-id 1510
!
switchport interface gigabit-ethernet-1/1/6 native-vlan vlan-id 1510
!
interface l3 vl-1505
 lower-layer-if vlan 1505
 ipv4 address 172.22.5.1/24
!
interface l3 vl-1510
 lower-layer-if vlan 1510
 ipv4 address 172.22.10.1/24
!
interface l3 vl-3300
 lower-layer-if vlan 3300
 ipv4 address 192.87.235.101/24
!
!
dhcp relay DHCP-RELAY-L3
 server ipv4 192.87.235.106
 interface l3-vl-1505
!
 interface l3-vl-1510
!
!
commit
```

9.3.2 Configurando o DHCP Option globalmente

Baseado no exemplo anterior, será adicionado de forma global a ação para a Option 82 no DHCP Relay.

No exemplo a seguir, os frames DHCP que chegarem sem a marcação de Option 82 serão marcados antes de serem enviados ao servidor, porém caso já exista essa marcação ela será mantida para ser enviada ao servidor. A Option 82 inserida pelo switch é composta pelos campos Circuit ID e Remote ID, exemplo: **10ge-1/1/1:1505**.

```
config
dhcp relay DHCP-RELAY-L3
 information option
 information trust-all
 information policy keep
 server ipv4 192.87.235.106
!
 interface l3-vl-1505
!
 interface l3-vl-1510
!
!
commit
```

9.3.3 Configurando o DHCP Option por interface

Baseado no exemplo inicial do DHCP, será adicionado o DHCP Option em uma interface específica.

A configuração do serviço de DHCP relay por interface possibilita configurar a Option 82 de forma diferente por interface em vez de utilizar as configurações da Option 82 global da instância.

Os passos a seguir demonstram como configurar o serviço de DHCP relay para inserir a Option 82 somente nos pacotes DHCP do cliente que está na interface gigabit-ethernet-1/1/1, as outras interfaces não terão a inserção da Option 82. Os pacotes DHCP dos clientes são encaminhados ao servidor DHCP 192.87.235.106:

```
config
dhcp relay DHCP-RELAY-L3
server ipv4 192.87.235.106
interface l3-vl-1505
!
interface l3-vl-1510
!
if-option gigabit-ethernet-1/1/1
information option
!
!
commit
```

10 Roteamento

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.

Este capítulo contém as seguintes seções:

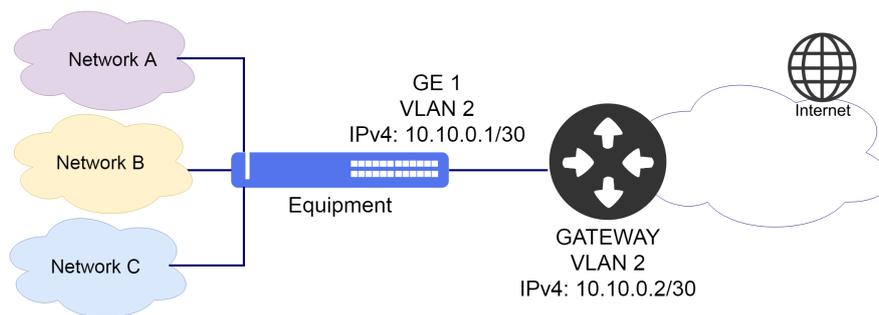
- Configuração de Rotas Estáticas
- Configuração de Rotas Black Hole
- Configuração do VLAN Routing
- Configuração da VRF
- Configuração do PBR
- Configuração do OSPFv2
- Configuração do OSPFv3
- Configuração do BGP
- Configuração do VRRP
- Configuração do BFD

10.1 Configuração de Rotas Estáticas

O roteamento estático tem por objetivo encaminhar pacotes entre redes distintas com a configuração das rotas de forma manual pelos administradores de rede.

10.1.1 Configurando uma Rota Estática Padrão

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



Implementação do roteamento estático

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

```
config
dot1q
vlan 2
interface gigabit-ethernet-1/1/1 tagged
!
!
interface l3 DEFAULT ROUTE-VLAN2
ipv4 address 10.10.0.1/30
lower-layer-if vlan 2
!
!
router static address-family ipv4 0.0.0.0/0 next-hop 10.10.0.2
commit
```



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

10.1.2 Verificando as Rotas Estáticas

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



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

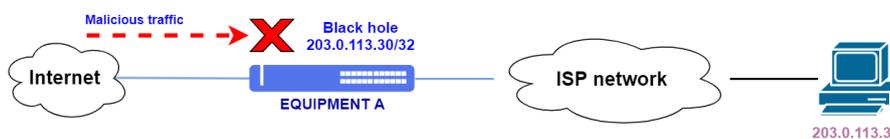
```
show ip route
show ip route static
show ip rib
show ip rib static
show ip interface brief
```

10.2 Configuração de rotas black hole

Todo o tráfego destinado a uma rota *black hole* é descartado. Em uma situação de ataque, em que uma grande quantidade de tráfego está sendo encaminhada a um determinado destino, uma rota black hole pode ser configurada para descartar este tráfego e evitar que sature links na rede do ISP (Internet Service Provider).

10.2.1 Configurando rotas black hole IPv4

No exemplo abaixo, o endereço **203.0.113.30/32** está sendo o destino de um ataque que pode saturar os links do ISP e afetar outros clientes. Para evitar que este tráfego afete outros clientes, foi configurada uma rota black hole e este tráfego é descartado assim que entra na rede do ISP.

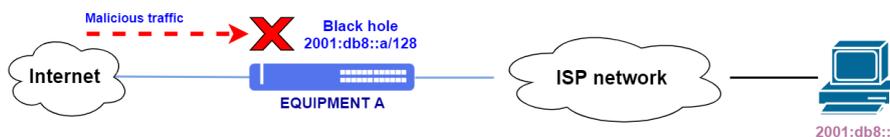


Rota black hole IPv4

```
config
router static
address-family ipv4
 203.0.113.30/32 blackhole
!
commit
```

10.2.2 Configurando rotas black hole IPv6

No exemplo abaixo, o endereço **2001:db8::a/128** está sendo o destino de um ataque que pode saturar os links do ISP e afetar outros clientes. Para evitar que este tráfego afete outros clientes, foi configurada uma rota black hole e este tráfego é descartado assim que entra na rede do ISP.



Rota black hole IPv6

```
config
router static
address-family ipv6
 2001:db8::a/128 blackhole
!
commit
```

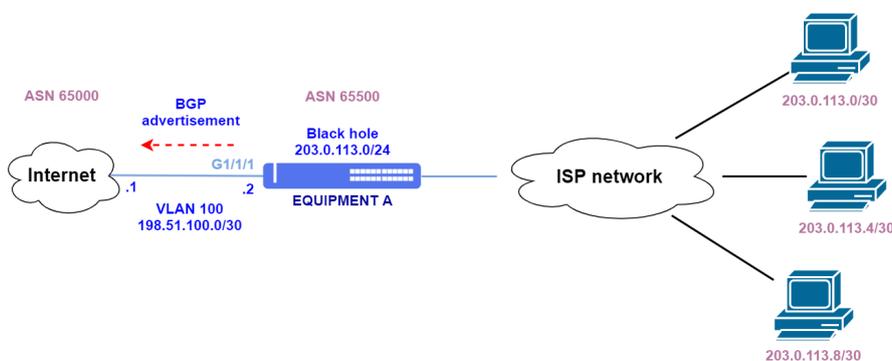
10.2.3 Sumarização com rotas black hole

No cenário a seguir, o ISP possui uma rede 203.0.113.0/24 distribuída em diversas redes menores /30 nos seus clientes. Estas rotas /30 não podem ser redistribuídas para o BGP no seu link de trânsito de Internet, que aceita apenas rotas /24 ou menos específicas.

Uma forma de sumarizar estas rotas e anunciar somente a rota /24 é a utilização de uma rota black hole. No exemplo abaixo, é configurada uma rota estática 203.0.113.0/24 black hole e ela é redistribuída para o neighbor BGP.

Ao ser anunciada pelo eBGP, o next-hop da rota é alterado para o endereço do parâmetro **update-source-address** do neighbor BGP. Desta forma, a rota black hole torna-se uma rota com next-hop válido ao ser anunciada.

Pacotes com destino aos endereços dos clientes não serão descartados pela rota black hole, pois, para estes destinos, existem rotas /30 mais específicas, que tem preferência à rota black hole /24.



Sumarização de rotas com black hole

```
!Equipment A
config
dot1q
vlan 100
  interface gigabit-ethernet-1/1/1
  !
!
!
interface l3 VLAN100
  lower-layer-if vlan 100
  ipv4 address 198.51.100.2/30
!
interface loopback 0
  ipv4 address 203.0.113.254/32
!
router bgp 65500
  router-id 203.0.113.254
  address-family ipv4 unicast
  !
  redistribute static address-family ipv4
  match-address 203.0.113.0/24
  !
  neighbor 198.51.100.1
  update-source-address 198.51.100.2
  remote-as 65000
  address-family ipv4 unicast
  !
!
router static
  address-family ipv4
  203.0.113.0/24 blackhole
!
!
commit
```



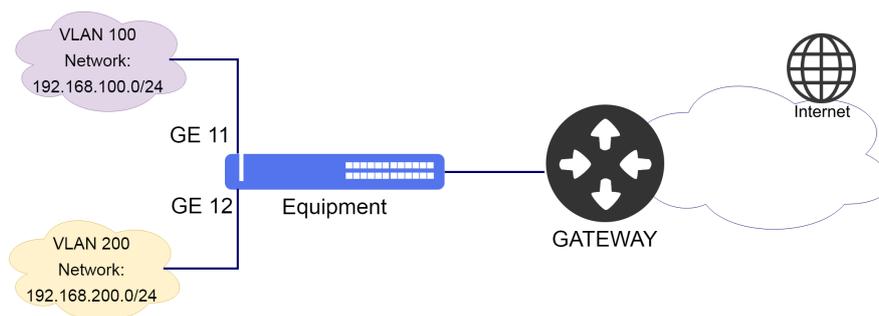
A sumarização de rotas através da redistribuição de rotas estáticas black hole também pode ser realizada com IPv6.

10.3 Configuração do VLAN Routing

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.

10.3.1 Configurando um Roteamento Básico entre VLANs

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



Implementação do roteamento entre VLANs

Suponha que o usuário deseje configurar o roteamento entre a VLAN 100 que possui a interface L3 com endereço 192.168.100.1/24 e a VLAN 200 que possui a interface L3 com endereço 192.168.200.1/24.



É possível configurar endereço IPv4 secundário nas interfaces L3. Endereço IPv6 secundário não é suportado.

```
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/11 tagged
!
!
vlan 200
interface gigabit-ethernet-1/1/12 tagged
!
!
interface l3 L3-VLAN100
ipv4 address 192.168.100.1/24
lower-layer-if vlan 100
!
!
interface l3 L3-VLAN200
ipv4 address 192.168.200.1/24
```

```
lower-layer-if vlan 200
!
!
commit
```



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

10.3.2 Verificando as Rotas

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



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

```
show ip route
show ip route connected
show ip interface brief
```

10.4 Configuração da VRF

O VRF (Virtual Routing and Forwarding) é uma funcionalidade que permite a existência de diversas instâncias de roteamento isoladas em um mesmo equipamento.

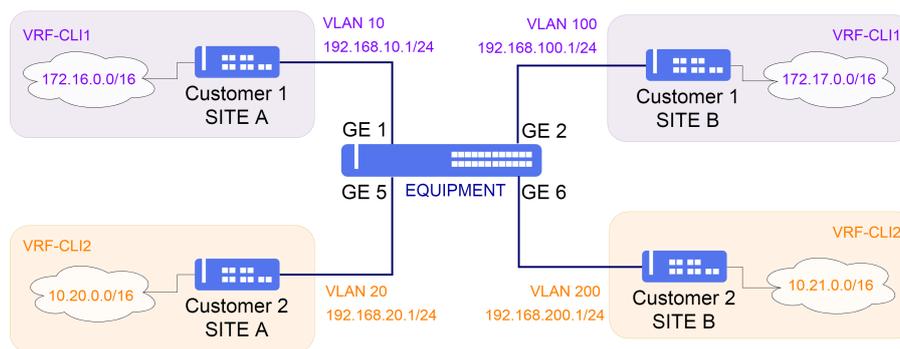
Por padrão, o DmOS utiliza duas tabelas de roteamento, global e management. É possível criar outras tabelas de roteamento através de outras instâncias de VRF.



Para configurar uma **VRF mgmt** (VRF exclusiva para gerenciamento do equipamento), é necessário configurar apenas a interface mgmt e uma rota default na VRF mgmt. Por padrão, a VRF mgmt já está criada no DmOS.

10.4.1 Configurando a VRF Lite

A VRF lite é uma versão mais básica do VRF, sem suporte a sinalização por MPLS. O cenário abaixo será usado para demonstrar a configuração de duas VRFs lite.



Implementação do VRF Lite

Não deve haver comunicação entre os clientes 1 e 2. Portanto, duas VRFs serão configuradas para isolar as tabelas de roteamento e o tráfego entre ambos. Serão utilizadas as seguintes especificações:

- **VRF-CLI1:**
Interface na VLAN 10 com endereço IPv4 192.168.10.1/24
Interface na VLAN 100 com endereço IPv4 192.168.100.1/24
- **VRF-CLI2:**
Interface na VLAN 20 com endereço IPv4 192.168.20.1/24
Interface na VLAN 200 com endereço IPv4 192.168.200.1/24

Para criar as duas VRFs, basta seguir as configurações abaixo.

```
config
vrf VRF-CLI1
description CLIENT1
!
vrf VRF-CLI2
description CLIENT2
!
commit
```

Em seguida, são configuradas as interfaces e rotas associadas a estas VRFs.

```
config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1 tagged
!
!
vlan 20
interface gigabit-ethernet-1/1/5 tagged
!
!
vlan 100
interface gigabit-ethernet-1/1/2 tagged
!
!
vlan 200
interface gigabit-ethernet-1/1/6 tagged
!
!
!
interface l3 CLI1-VLAN10
vrf VRF-CLI1
ipv4 address 192.168.10.1/24
lower-layer-if vlan 10
!
interface l3 CLI1-VLAN100
vrf VRF-CLI1
ipv4 address 192.168.100.1/24
lower-layer-if vlan 100
!
interface l3 CLI2-VLAN20
vrf VRF-CLI2
```

```

ipv4 address 192.168.20.1/24
lower-layer-if vlan 20
!
interface l3 CLI2-VLAN200
vrf VRF-CLI2
ipv4 address 192.168.200.1/24
lower-layer-if vlan 200
!
router static
vrf VRF-CLI1
address-family ipv4
172.16.0.0/16 next-hop 192.168.10.2
172.17.0.0/16 next-hop 192.168.100.2
!
!
!
vrf VRF-CLI2
address-family ipv4
10.20.0.0/16 next-hop 192.168.20.2
10.21.0.0/16 next-hop 192.168.200.2
!
!
!
commit

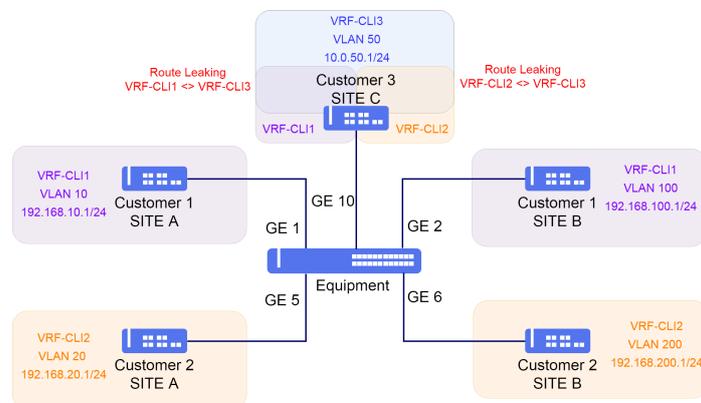
```



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

10.4.2 Habilitando o Route Leaking entre VRFs

Utilizando o cenário anterior como base, será incluído um terceiro cliente.



Route leaking entre VRFs

O Client 3 possui as seguintes especificações:

- **VRF-CLI3:**
Interface na VLAN 50 com endereço IPv4 10.1.50.1/24

Como os três clientes estão em VRFs diferentes, não há comunicação entre eles. Porém, considerando que é requisito que os clientes 1 e 2 consigam acessar o cliente 3, é necessário utilizar route leaking entre as VRFs.

Cada VRF deve ter um identificador único chamado de route distinguisher (RD). O RD irá dizer à qual VRF cada rota pertence, permitindo assim que possa haver overlapping (sobreposição) de endereços IP em VRFs diferentes.

- **VRF-CLI1:** rd 1:10

- **VRF-CLI2:** rd 2:20
- **VRF-CLI3:** rd 3:50

Para que ocorra o leaking, são utilizados route-targets (RT). Assim como o RD, RTs são identificadores adicionados às rotas para permitir que um roteador saiba quais rotas devem ser inseridas em quais VRFs. Podem ter o mesmo formato do RD. Rotas exportadas com um determinado RT serão importadas em VRFs que possuem este RT configurado como import. Será feito leaking entre VRF-CLI1 e VRF-CLI3 e entre VRF-CLI2 e VRF-CLI3. Desta forma, haverá comunicação entre Cliente 1 e Cliente 3, Cliente 2 e Cliente 3. Não haverá comunicação entre Cliente 1 e Cliente 2 pois ambos não estão configurados para importar as rotas entre eles.



O route leaking entre VRFs pode ser configurado com a redistribuição de rotas estáticas e a redistribuição de rotas diretamente conectadas.

```

config
dot1q
  vlan 50
  interface gigabit-ethernet-1/1/10 tagged
  !
  !
  !
interface l3 CLI3-VLAN50
vrf VRF-CLI3
  ipv4 address 10.1.50.1/24
  lower-layer-if vlan 50
  !
vrf VRF-CLI1
  rd 1:10
  address-family ipv4 unicast
  route-target import 3:50
  !
  route-target export 1:10
  !
  !
vrf VRF-CLI2
  rd 2:20
  address-family ipv4 unicast
  route-target import 3:50
  !
  route-target export 2:20
  !
  !
vrf VRF-CLI3
  rd 3:50
  address-family ipv4 unicast
  route-target import 1:10
  !
  route-target import 2:20
  !
  route-target export 3:50
  !
  !
router static
vrf VRF-CLI3
  address-family ipv4
  0.0.0.0/0 next-hop 10.1.50.2
  !
  !
  !
router bgp 65500
  address-family ipv4 unicast
  !
  vrf VRF-CLI1
  address-family ipv4 unicast
  redistribute static
  !
  exit-address-family
  !
  !
  vrf VRF-CLI2
  address-family ipv4 unicast
  redistribute static

```

```
!
exit-address-family
!
!
vrf VRF-CLI3
address-family ipv4 unicast
redistribute static
!
exit-address-family
!
!
commit
```



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

10.4.3 Verificando as VRFs

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



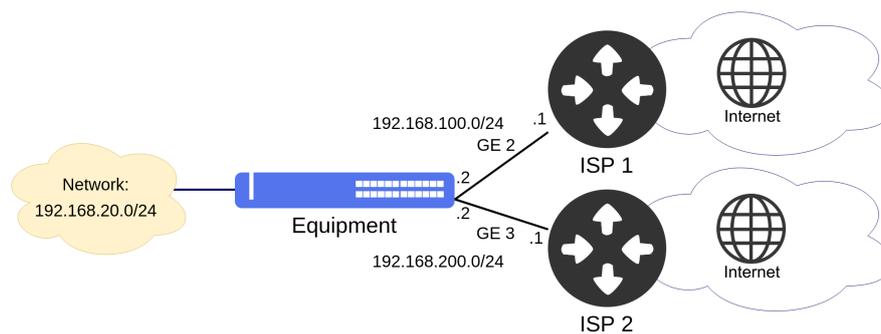
Para maiores detalhes sobre as saídas dos comandos, consultar o [Command Reference](#).

```
show ip route vrf <VRF_NAME>
show ip fib vrf <VRF_NAME>
```

10.5 Configuração do PBR

O roteamento baseado em políticas (Policy-based routing PBR) permite ao usuário usar regras para classificar o tráfego com base em alguns dos seus atributos e encaminhar seletivamente os pacotes para um próximo hop alternativo. Todos os pacotes recebidos que correspondem às regras são considerados para o roteamento baseado em políticas. Todos os pacotes que não correspondem a nenhuma regra configurada são encaminhados seguindo a tabela de roteamento do sistema. As políticas PBR podem ser aplicadas apenas às interfaces Ethernet do data plane para tráfego de entrada, no entanto o usuário não pode aplicar políticas PBR a pacotes gerados localmente.

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



Cenário do PBR

Suponha que o usuário deseja configurar uma política PBR para que o tráfego do host 192.168.20.1 seja encaminhado pelo próximo salto 192.168.200.1 que é alcançável via interface Gigabit Ethernet 3, e para que o tráfego originado dos demais hosts da rede 192.168.20.0/24 sejam encaminhados pela tabela de roteamento do sistema.

Os próximos passos irão mostrar como realizar estas configurações.

```

config
dot1q
vlan 100
interface gigabit-ethernet-1/1/2
untagged
!
vlan 200
interface gigabit-ethernet-1/1/3
untagged
!
!
switchport
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 100
!
interface gigabit-ethernet-1/1/3
native-vlan
vlan-id 200
!
!
interface l3 ISP_1
lower-layer-if vlan 100
ipv4 address 192.168.100.2/24
!
interface l3 ISP_2
lower-layer-if vlan 200
ipv4 address 192.168.200.2/24
!
!
router static
address-family ipv4
0.0.0.0/0 next-hop 192.168.100.1
!
!
router pbr 1
priority 7
match source ipv4-address 192.168.20.1/32
action next-hop 192.168.200.1
!
router pbr 2
priority 10
match source ipv4-address 192.168.20.0/24
action l3-routing
!
commit

```



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

10.5.1 Verificando o PBR

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



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

```
show router pbr
show router pbr <rule_id>
```

10.6 Configuração do OSPFv2

O OSPFv2 (Open Shortest Path First version 2) é o Interior Gateway Protocol (IGP) descrito pela RFC 2328 (versão 2) para roteamento de endereços IPv4. Como é um IGP, é utilizado para roteamento dentro de um mesmo AS (Autonomous System). É baseado no algoritmo de Dijkstra, que calcula o caminho mais curto para cada destino com base nos custos de cada link.

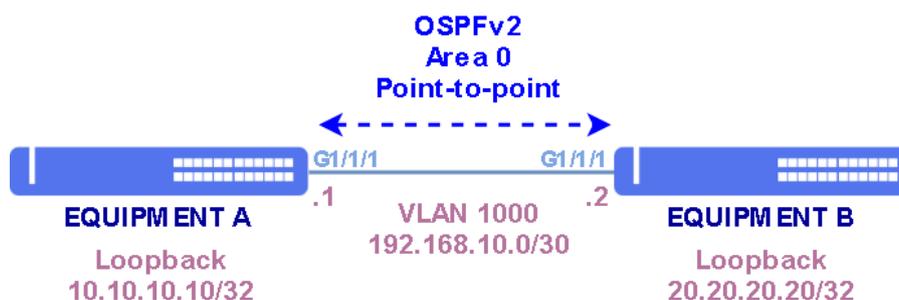


Atualmente, o DmOS suporta o OSPFv2 para redes do tipo Ponto-a-Ponto e Broadcast.

- **Ponto-a-Ponto:** Tipo de rede onde somente uma única adjacência pode ser formada sobre o link. Não há eleição de DR (Designated Router) ou BDR (Backup Designated Router).
- **Broadcast:** Um roteador é eleito como DR (Designated Router) e outro é eleito como BDR (Backup Designated Router). Esta eleição é baseada nas prioridades do OSPF e são utilizadas para limitar a quantidade de adjacências formadas na rede. Portanto, cada roteador da rede OSPF só formará adjacências com estes dois roteadores, o DR e o BDR.

10.6.1 Configurando o OSPFv2 em rede Ponto a Ponto

O cenário abaixo será usado para demonstrar a configuração do OSPFv2 em rede tipo Ponto a Ponto.



Implementação Ponto a Ponto do protocolo OSPFv2

Para realizar a configuração de uma sessão OSPF na área 0 com network-type do tipo ponto-a-ponto, as seguintes configurações podem ser utilizadas:

- **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.

```
!Equipment A
config
dot1q
vlan 1000
interface gigabit-ethernet-1/1/1
untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 1000
!
!
interface l3 OSPF
lower-layer-if vlan 1000
ipv4 address 192.168.10.1/30
!
interface loopback 0
ipv4 address 10.10.10.10/32
!
router ospf 1
router-id 10.10.10.10
area 0
interface l3-OSPF
network-type point-to-point
!
interface loopback-0
!
!
!
commit
```

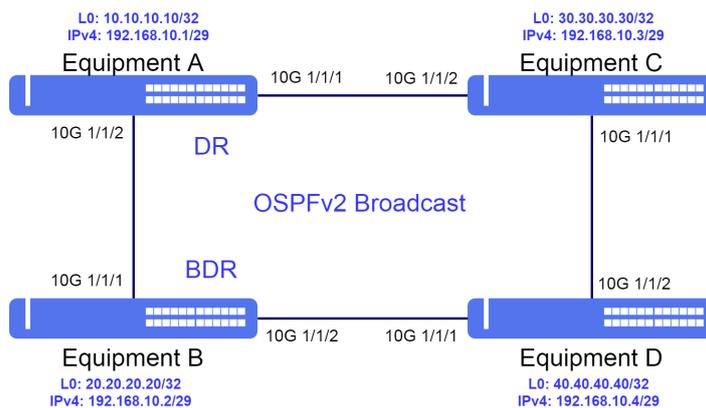
```
!Equipment B
config
dot1q
vlan 1000
interface gigabit-ethernet-1/1/1
untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 1000
!
!
!
interface l3 OSPF
lower-layer-if vlan 1000
ipv4 address 192.168.10.2/30
!
interface loopback 0
ipv4 address 20.20.20.20/32
!
router ospf 1
router-id 20.20.20.20
area 0
interface l3-OSPF
network-type point-to-point
interface loopback-0
!
!
!
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.2 Configurando o OSPFv2 em rede Broadcast

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



Implementação Broadcast do protocolo OSPFv2

Para realizar a configuração de uma sessão OSPF na área 0 com network-type do tipo broadcast, as seguintes configurações podem ser utilizadas:

- **Equipment A:** Interface L3 na VLAN 1000 com endereço IPv4 192.168.10.1/29 e interface loopback com IPv4 10.10.10.10/32 sendo utilizada como router-id na área 0. A prioridade OSPF configurada será 250.
- **Equipment B:** Interface L3 na VLAN 1000 com endereço IPv4 192.168.10.2/29 e interface loopback com IPv4 20.20.20.20/32 sendo utilizada como router-id na área 0. A prioridade OSPF configurada será 200.
- **Equipment C:** Interface L3 na VLAN 1000 com endereço IPv4 192.168.10.3/29 e interface loopback com IPv4 30.30.30.30/32 sendo utilizada como router-id na área 0. A prioridade OSPF configurada será 150.
- **Equipment D:** Interface L3 na VLAN 1000 com endereço IPv4 192.168.10.4/29 e interface loopback com IPv4 40.40.40.40/32 sendo utilizada como router-id na área 0. A prioridade OSPF configurada será 100.



Devido as prioridades do OSPF serem maiores nos EQUIPMENT A e B, estes serão eleitos o DR e o BDR, respectivamente.

```
!Equipment A
config
dot1q
vlan 1000
interface ten-gigabit-ethernet-1/1/1
untagged
interface ten-gigabit-ethernet-1/1/2
untagged
!
```

```

!
switchport
interface ten-gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 1000
interface ten-gigabit-ethernet-1/1/2
  native-vlan
  vlan-id 1000
!
!
interface l3 OSPF
  lower-layer-if vlan 1000
  ipv4 address 192.168.10.1/29
!
interface loopback 0
  ipv4 address 10.10.10.10/32
!
router ospf 1
  router-id 10.10.10.10
  area 0
    interface l3-OSPF
      network-type broadcast
      router-priority 250
    !
  !
  interface loopback-0
!
!
!
commit

```

```

!Equipment B
config
dot1q
vlan 1000
  interface ten-gigabit-ethernet-1/1/1
    untagged
  interface ten-gigabit-ethernet-1/1/2
    untagged
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 1000
interface ten-gigabit-ethernet-1/1/2
  native-vlan
  vlan-id 1000
!
!
interface l3 OSPF
  lower-layer-if vlan 1000
  ipv4 address 192.168.10.2/29
!
interface loopback 0
  ipv4 address 20.20.20.20/32
!
router ospf 1
  router-id 20.20.20.20
  area 0
    interface l3-OSPF
      network-type broadcast
      router-priority 200
    !
  !
  interface loopback-0
!
!
!
commit

```

```

!Equipment C
config
dot1q
vlan 1000
  interface ten-gigabit-ethernet-1/1/1
    untagged
  interface ten-gigabit-ethernet-1/1/2
    untagged
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
  native-vlan

```

```

vlan-id 1000
interface ten-gigabit-ethernet-1/1/2
 native-vlan
   vlan-id 1000
!
!
interface l3 OSPF
 lower-layer-if vlan 1000
 ipv4 address 192.168.10.3/29
!
interface loopback 0
 ipv4 address 30.30.30.30/32
!
router ospf 1
 router-id 30.30.30.30
 area 0
   interface l3-OSPF
     network-type broadcast
     router-priority 150
   !
   interface loopback-0
!
!
!
commit

```

```

!Equipment D
config
dot1q
vlan 1000
 interface ten-gigabit-ethernet-1/1/1
   untagged
 interface ten-gigabit-ethernet-1/1/2
   untagged
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
 native-vlan
   vlan-id 1000
interface ten-gigabit-ethernet-1/1/2
 native-vlan
   vlan-id 1000
!
!
interface l3 OSPF
 lower-layer-if vlan 1000
 ipv4 address 192.168.10.4/29
!
interface loopback 0
 ipv4 address 40.40.40.40/32
!
router ospf 1
 router-id 40.40.40.40
 area 0
   interface l3-OSPF
     network-type broadcast
     router-priority 100
   !
   interface loopback-0
!
!
!
commit

```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.3 Configurando a área no OSPFv2

É possível configurar diferentes tipos de área no OSPFv2. Os tipos de áreas disponíveis são: **normal**, **stub**, **stub no-summary**, **nssa**, **nssa no-summary** e **nssa suppress-external**.



É possível configurar a área NSSA com no-summary e suppress-external juntas.



Não é possível configurar o tipo para a area 0. Esta área sempre será do tipo NORMAL por ser considerada a área backbone da rede OSPF.

No exemplo abaixo, a área 10 será configurada como uma área stub.

```
config
router ospf 1
router-id 10.10.10.10
area 10
 stub
 !
 !
 !
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.4 Filtrando rotas recebidas no OSPFv2

Pode ser necessário restringir a quantidade de rotas instaladas em alguns equipamentos, devido a limitações na capacidade de hardware.

No exemplo abaixo, foi configurado um prefix-list chamado *allowed-prefixes* permitindo apenas rotas 203.0.113.0 com máscara entre /24 e /32. Ao aplicar este prefixo na configuração do protocolo OSPF, somente rotas neste intervalo serão instaladas. Outros prefixos recebidos serão mantidos na database do OSPF, porém não serão instalados na RIB.

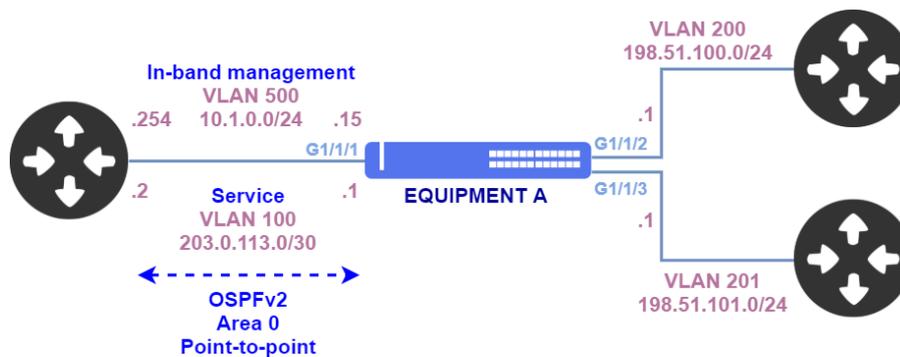
```
prefix-list allowed-prefixes
seq 10
 action permit
 address 203.0.113.0/24
 le 32
 !
 !
router ospf 1
 import-prefix-list allowed-prefixes
 !
 !
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.5 Filtrando rotas redistribuídas no OSPFv2

No cenário abaixo, o **EQUIPMENT A** é um CPE com gerência *in-band* (VLAN 500) e com adjacência OSPF com o ISP na rede de serviço (VLAN 100). Este equipamento possui duas interfaces L3 com endereços **198.51.100.1/24** e **198.51.101.1/24**. Estas rotas precisam ser redistribuídas no OSPFv2, porém, ao configurar **redistribute connected** no OSPF, a rota de gerência também é redistribuída na rede de serviço, o que não é desejável.



Filtrando rotas redistribuídas no OSPFv2

Para que somente as redes das VLANs 200 e 201 sejam redistribuídas, pode ser configurada uma regra **export-prefix-list** no OSPF. À esta regra é associado o prefix list **mgmt-network**, que filtra a rede 10.1.0.0/24, evitando que seja anunciada ao neighbor OSPF. As rotas 198.51.100.0/24 e 198.51.101.0/24 são redistribuídas normalmente.

```
!Equipment A
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/1
!
vlan 200
interface gigabit-ethernet-1/1/2
!
vlan 201
interface gigabit-ethernet-1/1/3
!
vlan 500
interface gigabit-ethernet-1/1/1
!
!
interface l3 VLAN100
lower-layer-if vlan 100
ipv4 address 203.0.113.1/30
!
interface l3 VLAN200
lower-layer-if vlan 200
ipv4 address 198.51.100.1/24
!
interface l3 VLAN201
lower-layer-if vlan 201
ipv4 address 198.51.101.1/24
!
interface l3 MGMT
lower-layer-if vlan 500
ipv4 address 10.1.0.15/24
!
router static
address-family ipv4
0.0.0.0/0 next-hop 10.1.0.254
!
router ospf 1
export-prefix-list mgmt-network
redistribute connected
area 0
interface l3-VLAN100
```

```

network-type point-to-point
!
!
prefix-list mgmt-network
seq 10
action deny
address 10.1.0.0/24
!
!
commit

```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.6 Habilitando ECMP no OSPFv2

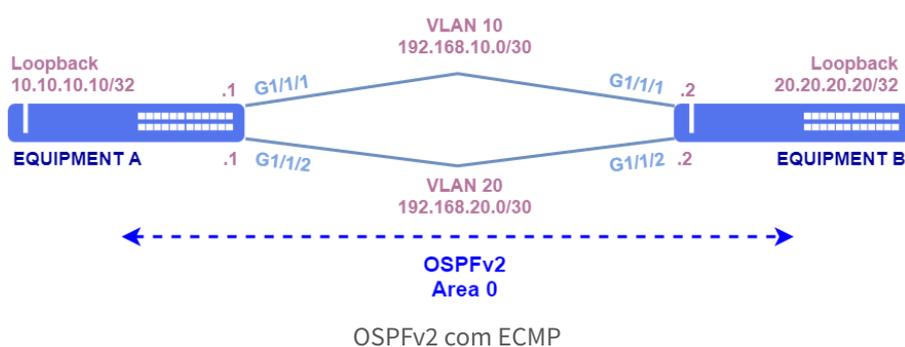
O comportamento padrão do OSPFv2 é a instalação de apenas uma rota para um mesmo destino. Caso exista mais de uma rota válida com mesmo custo, apenas uma será selecionada. Habilitando o ECMP (Equal-Cost Multi-Path), fará com que o OSPFv2 instale mais de uma rota para um mesmo destino e faça balanceamento de tráfego entre os caminhos disponíveis.

O balanceamento é realizada de forma semelhante ao feito em LAGs. É gerado um hash com base em parâmetros do pacote (endereços IP, porta UDP/TCP e VLAN). O valor do hash irá definir por qual link os pacotes de um fluxo específico serão encaminhados.

No cenário abaixo, há dois caminhos de igual custo entre os equipamentos A e B. Inserindo a configuração **maximum paths 2** no OSPF, ambos os caminhos serão instalados na tabela de roteamento.



É possível habilitar o ECMP para utilizar até 16 caminhos diferentes, caso estejam disponíveis.



```

!Equipment A
config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1
!
!
vlan 20
interface gigabit-ethernet-1/1/2
!
!
!

```

```
interface l3 VLAN10
  lower-layer-if vlan 10
  ipv4 address 192.168.10.1/30
!
interface l3 VLAN20
  lower-layer-if vlan 10
  ipv4 address 192.168.20.1/30
!
interface loopback 0
  ipv4 address 10.10.10.10/32
!
router ospf 1
  maximum paths 2
  area 0
    interface l3-VLAN10
      network-type point-to-point
    !
    interface l3-VLAN20
      network-type point-to-point
    !
    interface loopback-0
    !
  !
!
!
commit
```

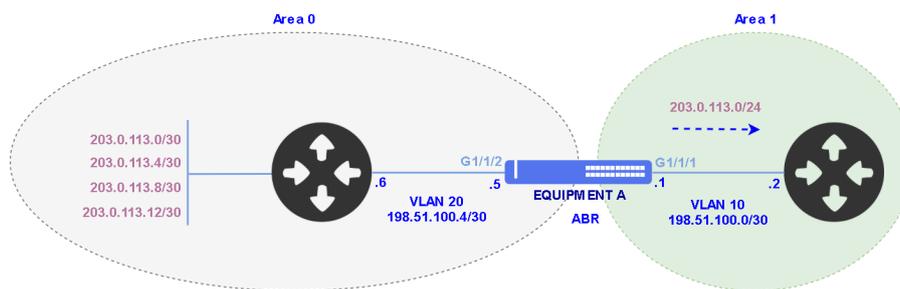
```
!Equipment B
config
dot1q
vlan 10
  interface gigabit-ethernet-1/1/1
  !
vlan 20
  interface gigabit-ethernet-1/1/2
  !
!
!
interface l3 VLAN10
  lower-layer-if vlan 10
  ipv4 address 192.168.10.2/30
!
interface l3 VLAN20
  lower-layer-if vlan 10
  ipv4 address 192.168.20.2/30
!
interface loopback 0
  ipv4 address 20.20.20.20/32
!
router ospf 1
  maximum paths 2
  area 0
    interface l3-VLAN10
      network-type point-to-point
    !
    interface l3-VLAN20
      network-type point-to-point
    !
    interface loopback-0
    !
  !
!
!
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.7 Sumarização de rotas no OSPFv2

O cenário abaixo será utilizado para demonstrar a sumarização de rotas no OSPFv2.



Sumarização de rotas no OSPFv2

Na área 0, a rede 203.0.113.0/24 está dividida em diversas subredes. O **EQUIPMENT A** irá anunciar todas estas rotas à área 1. Para diminuir o número de rotas na área 1, pode-se configurar no OSPF a sumarização para que apenas a rede 203.0.113.0/24 seja anunciada.

No OSPF, a sumarização de rotas pode ocorrer somente entre áreas. Neste caso, é realizada no EQUIPMENT A, que é um **ABR (Area Border Router)**, pois possui conexões tanto na área 0 como na área 1.

Como demonstrado na configuração abaixo, o comando **range 203.0.113.0 255.255.255.0**, configurado na área 0, instrui o OSPF a anunciar para as outras áreas somente a rede 203.0.113.0/24 e não as subredes contidas nela.

Recomenda-se a configuração de uma rota *black hole* no EQUIPMENT A, evitando que pacotes com destino a subredes inexistentes sejam encaminhados. Por exemplo, no cenário apresentado, caso um pacote com destino ao endereço 203.0.113.100 seja encaminhado para dentro da área 0, este não encontrará uma rota mais específica e poderia entrar em loop. A rota *black hole* descarta estes pacotes, evitando que sejam encaminhados desnecessariamente.



Para mais detalhe sobre configuração de rotas *black hole*, consultar o tópico [Configuração de rotas black hole](#)

```
!Equipment A
config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1
untagged
!
vlan 20
interface gigabit-ethernet-1/1/2
untagged
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 10
!
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 20
!
!
interface l3 VLAN10
lower-layer-if vlan 10
ipv4 address 198.51.100.1/30
!
interface l3 VLAN20
lower-layer-if vlan 20
ipv4 address 198.51.100.5/30
```

```
!  
router static  
  address-family ipv4  
    203.0.113.0/24 black-hole  
!  
!  
router ospf 1  
  area 0  
    interface l3-VLAN10  
      network-type point-to-point  
    !  
    range 203.0.113.0 255.255.255.0 advertise  
  !  
  area 1  
    interface l3-VLAN20  
      network-type point-to-point  
  !  
!  
!  
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv2](#).

10.6.8 Verificando o OSPFv2

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



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

```
show ip ospf  
show ip ospf neighbor  
show ip ospf database  
show ip ospf interface  
show ip ospf detail  
show ip ospf extensive  
show ip ospf brief  
show ip ospf database external  
show ip route ospf  
show ip rib ospf
```

10.7 Configuração do OSPFv3

O OSPFv3 (Open Shortest Path First version 3) é o Interior Gateway Protocol (IGP) descrito pela RFC 2740 para roteamento de endereços IPv6. Como este protocolo é um IGP, é utilizado dentro de um mesmo AS (Autonomous System). É baseado no algoritmo de Dijkstra, que calcula o caminho mais curto para cada destino com base nos custos dos links.



Atualmente, o OSPFv3 suporta apenas redes do tipo ponto-a-ponto.


```

switchport
interface ten-gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 1000
!
!
!
interface l3 OSPFv3
  lower-layer-if vlan 1000
  ipv6 enable
  ipv6 address 2600::c0a8:a02/64
!
!
interface loopback 0
  ipv4 address 20.20.20.20/32
  ipv6 enable
  ipv6 address 2700::1414:1415/64
!
!
router ospfv3 1
  router-id 20.20.20.20
  area 0
    interface l3-OSPFv3
      network-type point-to-point
    interface loopback-0
!
!
!
commit

```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv3](#).

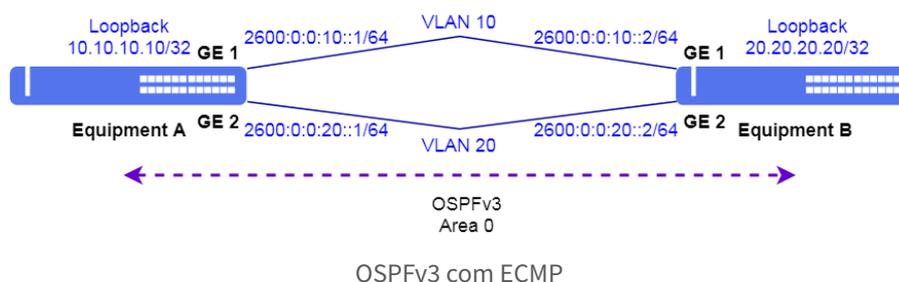
10.7.2 Habilitando ECMP no OSPFv3

O comportamento padrão do OSPFv3 é a instalação de apenas uma rota para um mesmo destino. Caso exista mais de uma rota válida com mesmo custo, apenas uma será selecionada. Habilitando o ECMP (Equal-Cost Multi-Path), fará com que o OSPFv3 instale mais de uma rota para um mesmo destino e faça balanceamento de tráfego entre os caminhos disponíveis.

No cenário abaixo, há dois caminhos de igual custo entre os equipamentos A e B. Inserindo a configuração **maximum paths 2** no OSPF, ambos os caminhos serão instalados na tabela de roteamento.



É possível habilitar o ECMP para utilizar até 16 caminhos diferentes, caso estejam disponíveis.



```

!Equipment A
config
dot1q
vlan 10

```

```
interface gigabit-ethernet-1/1/1
!
!
vlan 20
interface gigabit-ethernet-1/1/2
!
!
!
interface l3 VLAN10
lower-layer-if vlan 10
ipv6 enable
ipv6 address 2600:0:0:10::1/64
!
interface l3 VLAN20
lower-layer-if vlan 10
ipv6 enable
ipv6 address 2600:0:0:20::1/64
!
interface loopback 0
ipv4 address 10.10.10.10/32
!
!
router ospfv3 1
maximum paths 2
area 0
interface l3-VLAN10
network-type point-to-point
!
interface l3-VLAN20
network-type point-to-point
!
interface loopback-0
!
!
!
commit
```

```
!Equipment B
config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1
!
!
vlan 20
interface gigabit-ethernet-1/1/2
!
!
!
interface l3 VLAN10
lower-layer-if vlan 10
ipv6 enable
ipv6 address 2600:0:0:10::2/64
!
!
interface l3 VLAN20
lower-layer-if vlan 10
ipv6 enable
ipv6 address 2600:0:0:20::2/64
!
!
interface loopback 0
ipv4 address 20.20.20.20/32
!
!
router ospfv3 1
maximum paths 2
area 0
interface l3-VLAN10
network-type point-to-point
!
interface l3-VLAN20
network-type point-to-point
!
interface loopback-0
!
!
!
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser verificados no tópico [Verificando o OSPFv3](#).

10.7.3 Verificando o OSPFv3

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



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

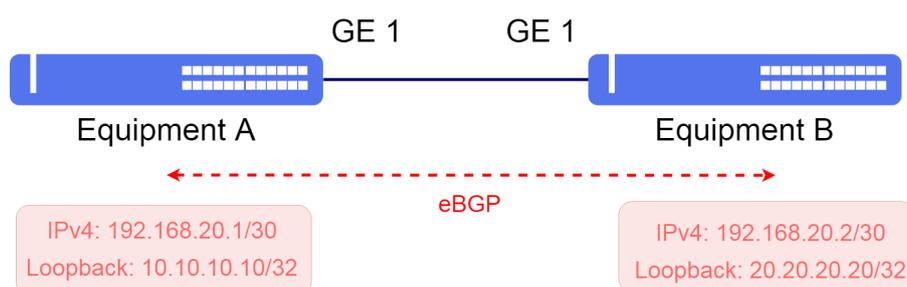
```
show ipv6 ospf
show ipv6 ospf neighbor
show ipv6 ospf database
show ipv6 ospf brief
show ipv6 ospf database external
show ipv6 route ospf
show ipv6 rib ospf
```

10.8 Configuração do BGP

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 diferente AS, o BGP é chamado de **eBGP** (external BGP) enquanto que, quando a vizinhança é estabelecida entre roteadores do mesmo AS, o BGP é chamado de **iBGP** (internal BGP).

10.8.1 Configurando uma sessão eBGP IPv4 Single Homed

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



Implementação básica protocolo BGP IPv4

Suponha que o usuário queira realizar as seguintes configurações:

- **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 recomendado utilizar os endereços das interfaces físicas ao invés da loopback.

```
!Equipment A
config
dot1q
vlan 2000
  interface gigabit-ethernet-1/1/1
    untagged
  !
  !
  !
switchport
interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 2000
  !
  !
interface l3 BGP
  lower-layer-if vlan 2000
  ipv4 address 192.168.20.1/30
  !
  !
interface loopback 0
  ipv4 address 10.10.10.10/32
  !
  !
router bgp 20000
  router-id 10.10.10.10
  address-family ipv4 unicast
  !
  neighbor 192.168.20.2
  update-source-address 192.168.20.1
  remote-as 40000
  ebgp-multihop 1
  address-family ipv4 unicast
  !
  !
  !
commit
```

```
!Equipment B
config
dot1q
vlan 2000
  interface gigabit-ethernet-1/1/1
    untagged
  !
  !
  !
switchport
interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 2000
  !
  !
interface l3 BGP
  lower-layer-if vlan 2000
  ipv4 address 192.168.20.2/30
  !
  !
interface loopback 0
  ipv4 address 20.20.20.20/32
  !
  !
router bgp 40000
  router-id 20.20.20.20
  address-family ipv4 unicast
  !
  neighbor 192.168.20.1
  update-source-address 192.168.20.2
```

```
remote-as 20000
ebgp-multihop 1
address-family ipv4 unicast
!
commit
```



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

10.8.2 Configurando route-maps e prefix-lists IPv4

A configuração anterior irá anunciar todas as rotas válidas presentes na BGP RIB e aceitar qualquer rota recebida do vizinho. Em alguns casos, pode ser necessário filtrar os prefixos para evitar enviar ou receber rotas não desejadas.

A configuração de export (advertise-filter) a seguir irá:

- Rejeitar rotas privadas
- Rejeitar rotas com máscara maior que /24
- Anunciar rotas com máscara entre /16 e /18 realizando prepend
- Anunciar o restante das rotas que não se enquadram nas regras anteriores

A configuração de import (receive-filter) a seguir irá:

- Rejeitar rotas privadas
- Rejeitar rotas com máscara maior que /24
- Rejeitar rotas originadas no AS 5678
- Aceitar o restante das rotas que não se enquadram nas regras anteriores



O parâmetro **match-as-path** recebe uma expressão regular. No exemplo a seguir, para que ocorra match em AS paths iniciando em 5678, a expressão regular utilizada é `[^0-9]5678$`. O `[^0-9]` indica que naquela posição não deve haver um número, ocorrendo match apenas em 5678 e não em 15678, por exemplo.

```
!Equipment A
config
prefix-list ipv4-private-networks
seq 10
action permit
address 10.0.0.0/8
ge 8
seq 20
action permit
address 192.168.0.0/16
ge 16
seq 30
action permit
address 172.16.0.0/12
ge 12
!
prefix-list ipv4-more-specific-24
```

```
seq 10
  action permit
  address 0.0.0.0/0
  ge 25
!
prefix-list ipv4-between-16-18
seq 10
  action permit
  address 0.0.0.0/0
  ge 16
  le 18
!
router bgp 20000
route-map advertise-filter 10
  action deny
  match-ip nlri prefix-list ipv4-private-networks
!
route-map advertise-filter 30
  action deny
  match-ip nlri prefix-list ipv4-more-specific-24
!
route-map advertise-filter 40
  action permit
  match-ip nlri prefix-list ipv4-between-16-18
  set-prepend-local-as 1
!
route-map advertise-filter 50
  action permit
!
route-map receive-filter 10
  action deny
  match-ip nlri prefix-list ipv4-private-networks
!
route-map receive-filter 30
  action deny
  match-ip nlri prefix-list ipv4-more-specific-24
!
route-map receive-filter 40
  action deny
  match-as-path [^0-9]5678$
!
route-map receive-filter 50
  action permit
!
route-policy neighbor-as4000-policy
  import-route-map receive-filter
  export-route-map advertise-filter
!
neighbor 192.168.20.2
  route-policy neighbor-as4000-policy
!
commit
```



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

10.8.3 Configurando uma sessão iBGP IPv6 Single Homed

O cenário abaixo será usado para demonstrar a configuração do protocolo BGP com endereçamento IPv6 no mesmo AS, ou seja, iBGP.


```
router static
 address-family ipv6
  2500::/64 next-hop 2800::c0a8:1402
commit
```

```
!Equipment B
config
dot1q
vlan 2000
 interface gigabit-ethernet-1/1/1
  untagged
  !
  !
  !
switchport
 interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 2000
  !
  !
  !
interface l3 BGP
 lower-layer-if vlan 2000
 ipv6 enable
 ipv6 address 2800::c0a8:1402/64
  !
  !
interface loopback 0
 ipv4 address 20.20.20.20/32
 ipv6 enable
 ipv6 address 2500::1414:1414/64
  !
  !
router bgp 20000
 router-id 20.20.20.20
 address-family ipv6 unicast
  !
 neighbor 2700::a0a:a0a
  update-source-address 2500::1414:1414
  remote-as 20000
  ebgp-multihop 255
  address-family ipv6 unicast
  !
  !
router static
 address-family ipv6
  2700::/64 next-hop 2800::c0a8:1401
commit
```



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

10.8.4 Configurando route-maps e prefix-lists IPv6

A configuração anterior irá anunciar todas as rotas válidas presentes na BGP RIB e aceitar qualquer rota recebida do vizinho. Em alguns casos, pode ser necessário filtrar os prefixos para evitar enviar ou receber rotas não desejadas.

A configuração a seguir irá evitar que o EQUIPMENT A envie ou receba rotas privadas e rotas com máscara maior que /48. O EQUIPMENT A também irá rejeitar rotas originadas no AS 5678.

```
!Equipment A
config
prefix-list ipv6-private-networks
 seq 10
```

```
    action permit
    address fc00::/7
    ge 8
    !
prefix-list ipv6-more-specific-48
seq 10
    action permit
    address ::/0
    ge 49
    !
router bgp 20000
route-map advertise-filter 10
    action deny
    match-ip nlri prefix-list ipv6-private-networks
    !
route-map advertise-filter 30
    action deny
    match-ip nlri prefix-list ipv6-more-specific-48
    !
route-map advertise-filter 40
    action permit
    !
route-map receive-filter 10
    action deny
    match-ip nlri prefix-list ipv6-private-networks
    !
route-map receive-filter 30
    action deny
    match-ip nlri prefix-list ipv6-more-specific-48
    !
route-map receive-filter 40
    match-as-path [^0-9]5678$
    action deny
    !
route-map receive-filter 50
    action permit
    !
route-policy neighbor-as2000-policy
import-route-map receive-filter
export-route-map advertise-filter
    !
neighbor 2500::1414:1414
    route-policy neighbor-as2000-policy
    !
!
commit
```



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

10.8.5 Configurando BGP Communities

Communities BGP são parâmetros que podem ser incluídos em rotas anunciadas pelo BGP. Estes parâmetros podem ser usados para tomar ações sobre estas rotas, como rejeitá-las ou alterar suas características.

O cenário abaixo será usado para demonstrar a configuração de communities no protocolo BGP.



Configurando communities

```

!Equipment A
config
dot1q
vlan 100
  interface gigabit-ethernet-1/1/1
  !
vlan 200
  interface gigabit-ethernet-1/1/2
  !
!
interface l3 VLAN100
  lower-layer-if vlan 100
  ipv4 address 192.168.84.1/30
  !
interface l3 VLAN200
  lower-layer-if vlan 200
  ipv4 address 192.168.84.5/30
  !
router bgp 27686
  router-id 192.168.0.1
  address-family ipv4 unicast
  !
  neighbor 192.168.84.2
    update-source-address 192.168.84.1
    remote-as 3549
    ebgp-multihop 1
    address-family ipv4 unicast
  !
  neighbor 192.168.84.6
    update-source-address 192.168.84.5
    remote-as 262318
    ebgp-multihop 1
    address-family ipv4 unicast
  !
!
commit

```

Dentre os prefixos recebidos do ASN 3549, o prefixo 203.0.0.0/24 deve ser marcado com a community 3549:1000 antes de ser reanunciado.

Dentre os prefixos recebidos do ASN 262318, o prefixo 198.51.100.0/24 é recebido com a community 27686:501. Prefixos recebidos com esta community devem ser anunciados com prepend de 2 ASNs.

```

!Equipment A
config
prefix-list prefix-203_0_0
  seq 10
  action permit
  address 203.0.0.0/24
  !
router bgp 27686
  route-map import-from-asn3549 10

```

```
action permit
set-community 3549:1000
match-ip nlrp prefix-list prefix-203_0_0
route-map import-from-asn3549 20
action permit
!
route-map export-to-asn3549 10
action permit
match-community 27686:501
set-prepend-local-as 2
route-map export-to-asn3549 20
action permit
!
route-policy asn3549-policy
import-route-map import-from-asn3549
export-route-map export-to-asn3549
!
neighbor 192.168.84.2
route-policy asn3549-policy
!
!
```



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

10.8.6 Verificando o BGP

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



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

```
show ip bgp
show ip bgp neighbor
show ip bgp prefixes
show ip bgp summary
show ip bgp community
show ip route bgp
show ip rib bgp
show ipv6 route bgp
show ipv6 rib bgp
```

10.9 Configuração do VRRP

O VRRP (Virtual Router Redundancy Protocol) tem por objetivo eliminar o ponto único de falha disponibilizando um ou mais equipamentos para serem gateways de uma LAN caso o gateway principal fique indisponível. O protocolo controla os endereços IP associados a um roteador virtual, no qual um dos equipamentos é eleito o Master e os demais são eleitos Backup.



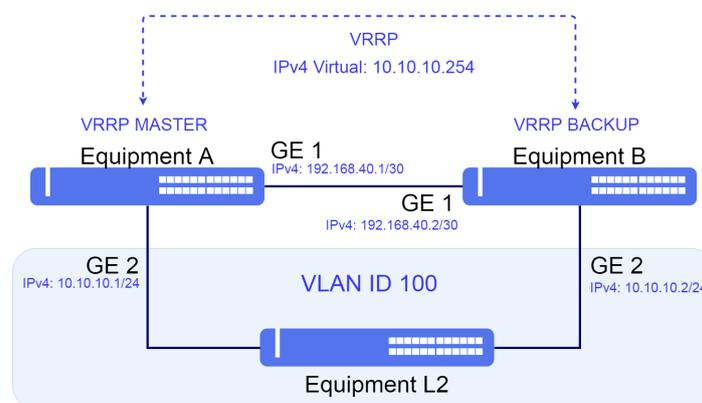
São suportadas as versões **VRRPv2** (com suporte a endereçamento IPv4, descrito pela RFC 3768) e **VRRPv3** (com suporte a endereçamentos IPv4 e IPv6, descrito pela RFC 5798).



Uma conexão direta entre os roteadores do VRRP é recomendada para aumentar a resiliência em caso de falhas individuais dos links. Nestas conexões diretas deve-se evitar o uso do RSTP ou outros protocolos de controle L2.

10.9.1 Configurando o VRRPv2 para fornecer Alta Disponibilidade

O cenário abaixo será usado para demonstrar a configuração do protocolo VRRPv2 para fornecer Alta Disponibilidade.



Implementação básica do protocolo VRRP

Suponha que o usuário queira realizar as seguintes configurações:

- **Equipment A:** Interface L3 para gateway da rede L2 na VLAN 100 com endereço IPv4 10.10.10.1/24. VRRP na versão 2 com IP do Roteador Virtual 10.10.10.254, prioridade 250 e autenticação com senha password. Conexão direta entre os roteadores (A e B) através da Interface L3 na VLAN 4000 com endereço IPv4 192.168.40.1/30
- **Equipment B:** Interface L3 para gateway da rede L2 na VLAN 100 com endereço IPv4 10.10.10.2/24. VRRP na versão 2 com IP do Roteador Virtual 10.10.10.254, prioridade 200 e autenticação com senha password. Conexão direta entre os roteadores (A e B) através da Interface L3 na VLAN 4000 com endereço IPv4 192.168.40.2/30

```
!Equipment A
config
dot1q
vlan 100
interface gigabit-ethernet-1/1/2
untagged
!
!
vlan 4000
interface gigabit-ethernet-1/1/1
!
!
switchport
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 100
```

```
!
!
!
interface l3 EQUIP-A-to-EQUIP-B
  lower-layer-if vlan 4000
  ipv4 address 192.168.40.1/30
!
!
interface l3 VRRP
  lower-layer-if vlan 100
  ipv4 address 10.10.10.1/24
!
!
router vrrp
  interface l3-VRRP
    address-family ipv4
      vr-id 1
      version v2
      priority 250
      authentication simple-text "password"
      address 10.10.10.254
commit
```

```
!Equipment B
config
dot1q
vlan 100
  interface gigabit-ethernet-1/1/2
    untagged
  !
!
vlan 4000
  interface gigabit-ethernet-1/1/1
  !
!
switchport
  interface gigabit-ethernet-1/1/2
    native-vlan
      vlan-id 100
  !
!
!
interface l3 EQUIP-B-to-EQUIP-A
  lower-layer-if vlan 4000
  ipv4 address 192.168.40.2/30
!
!
interface l3 VRRP
  lower-layer-if vlan 100
  ipv4 address 10.10.10.2/24
!
!
router vrrp
  interface l3-VRRP
    address-family ipv4
      vr-id 1
      version v2
      priority 200
      authentication simple-text "password"
      address 10.10.10.254
commit
```



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

10.9.2 Verificando o VRRP

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



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

```
show router vrrp brief
```

10.10 Configuração do BFD

O protocolo BFD (Bidirectional Forwarding Detection) é definido pela RFC 5880. É utilizado para detectar falhas de forma rápida em um link entre dois equipamentos.



O protocolo BFD é suportado apenas no OSPFv2.



Os intervalos de TX e RX são fixos em 300ms e o multiplicador está fixo em 3. Não é possível alterá-los através de configuração, porém estes valores podem ser modificados através de negociação com o vizinho.

Caso ocorra uma falha de comunicação no link entre dois equipamentos e as interfaces permaneçam up, o protocolo de roteamento entre eles não irá detectar a falha imediatamente, sendo necessário ocorrer timeout. Este timeout pode ser de vários segundos, dependendo da configuração do protocolo de roteamento. Enquanto isto, o tráfego continuará sendo enviado pelo link e, conseqüentemente, será descartado.

Caso o BFD esteja habilitado na interface deste protocolo de roteamento, ele irá detectar a falha muito rapidamente e irá sinalizar a queda para que o protocolo de roteamento convirja imediatamente, evitando que pacotes continuem sendo encaminhados para o link mesmo estando com problema.

10.10.1 Configurando o BFD no OSPFv2

No cenário abaixo, há uma sessão OSPF entre os equipamentos A e B. A configuração a seguir demonstra como configurar o BFD nesta interface com OSPF habilitado.



```
!Equipment A
config
dot1q
vlan 10
  interface gigabit-ethernet-1/1/1
  untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/1
  native vlan
  vlan-id 10
!
!
!
interface l3 VLAN10
  lower-layer-if vlan 10
  ipv4 address 192.168.10.1/30
!
interface loopback 0
  ipv4 address 10.10.10.10/32
!
router ospf 1
  area 0
  interface loopback 0
  !
  interface l3-VLAN10
  bfd
  session-type desired
  !
  network-type point-to-point
!
!
!
commit
```

```
!Equipment B
config
dot1q
vlan 10
  interface gigabit-ethernet-1/1/1
  untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/1
  native vlan
  vlan-id 10
!
!
!
interface l3 VLAN10
  lower-layer-if vlan 10
  ipv4 address 192.168.10.2/30
!
interface loopback 0
  ipv4 address 20.20.20.20/32
!
router ospf 1
  area 0
  interface loopback 0
  !
  interface l3-VLAN10
  bfd
  session-type desired
  !
  network-type point-to-point
!
!
!
commit
```

10.10.2 Verificando o BFD

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



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

```
show bfd session
```

11 MPLS

O MPLS (Multi-Protocol Label Switching), definido pela RFC 3031, é baseado no encaminhamento de pacotes por rótulos ou *labels*. Com o MPLS, pode-se implementar engenharia de tráfego e VPNs (Virtual Private Networks - Redes Virtuais Privadas). Neste capítulo, será abordada a configuração de L2VPNs e L3VPNs.

Este capítulo contém as seguintes seções:

- Configurando o LDP
- Configurando o RSVP
- Configuração de VPWS
- Configuração de VPLS
- Habilitando FAT em uma L2VPN
- Verificando L2VPNs
- Configuração de L3VPNs

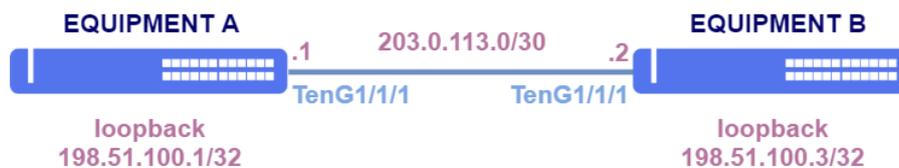
11.1 Configurando o LDP

O protocolo LDP (Label Distribution Protocol) é utilizado para distribuição de labels entre os equipamentos.



Uma licença é necessária para a operação do MPLS. Para mais detalhes de como ativá-la, verifique o tópico [Configuração das Licenças](#).

A topologia a seguir será utilizada como demonstração para configuração do LDP.



Configuração do protocolo LDP

```
!Equipment A
config
dot1q
vlan 10
interface ten-gigabit-ethernet-1/1/1
untagged
!
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
native-vlan
vlan-id 10
!
!
!
interface l3 VLAN10
ipv4 address 203.0.113.1/30
lower-layer-if vlan 10
```

```
!!
interface loopback 0
  ipv4 address 198.51.100.1/32
!!
router ospf 1
  router-id 198.51.100.1
  area 0
    interface l3-VLAN10
      network-type point-to-point
    !
    interface loopback-0
    !
  !
mpls ldp
  lsr-id loopback-0
  interface l3-VLAN10
  !
!
commit
```

```
!Equipment B
config
dot1q
vlan 10
  interface ten-gigabit-ethernet-1/1/1
    untagged
  !
!
switchport
  interface ten-gigabit-ethernet-1/1/1
    native-vlan
      vlan-id 10
  !
!
interface l3 VLAN10
  ipv4 address 203.0.113.2/30
  lower-layer-if vlan 10
  !
!
interface loopback 0
  ipv4 address 198.51.100.2/32
  !
!
router ospf 1
  router-id 198.51.100.2
  area 0
    interface l3-VLAN10
      network-type point-to-point
    !
    interface loopback-0
    !
  !
mpls ldp
  lsr-id loopback-0
  interface l3-VLAN10
  !
!
commit
```

11.2 Configurando o RSVP

O protocolo **RSVP** é utilizado para o estabelecimento de túneis entre os equipamentos. Diferentemente do LDP, que utiliza o melhor caminho escolhido pelo IGP para chegar ao destino, o caminho dos túneis é configurado pelo operador.



Uma licença é necessária para a operação do MPLS. Para mais detalhes de como ativá-la, verifique o tópico [Configuração das Licenças](#).

Para a definição de qual caminho um túnel deve utilizar, o DmOS utiliza atributos chamados *affinity* configurados nas interfaces. No valor utilizado neste atributo, cada bit corresponde a uma característica do link.

No exemplo abaixo, existem três características possíveis. Para cada característica, é utilizado um bit específico. Este valor é representado em hexadecimal no DmOS.

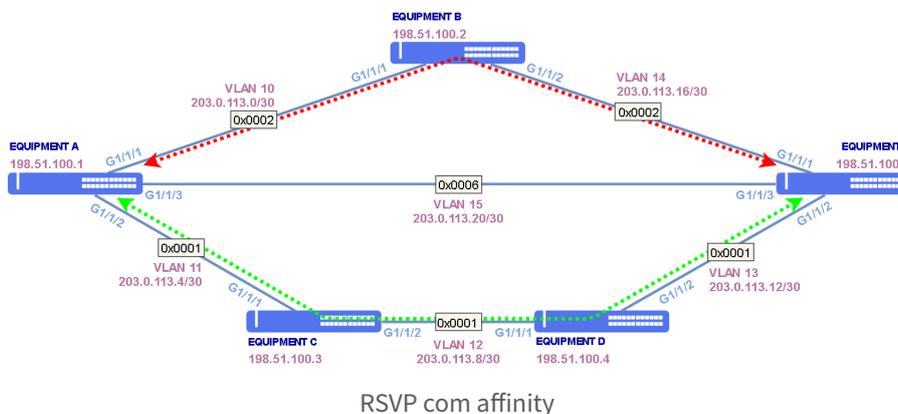
Característica	Binário	Hexadecimal
Link de alta capacidade	00000001	0x1
Link de baixa capacidade	00000010	0x2
Link com alta latência	00000100	0x4

Um link pode possuir duas ou mais características simultaneamente. Por exemplo, um link pode ser de baixa capacidade e possuir alta latência ao mesmo tempo. Neste caso, o seu atributo será a soma de 0x2 e 0x4, sendo seu valor final 0x6.

Túneis são unidirecionais, ou seja, é necessário configurar um túnel com origem no EQUIPMENT A com destino ao EQUIPMENT E e outro túnel com origem no EQUIPMENT E e com destino ao EQUIPMENT A.

Os túneis serão associados a dois caminhos. O caminho primário irá passar somente pelos links com atributo 0x1 (alta capacidade). Caso ocorra uma falha no caminho primário, o túnel subirá pelo caminho secundário, que pode passar por links com atributo 0x2 (baixa capacidade). Ambos os caminhos não podem passar por links com atributo 0x4 (alta latência), então os caminhos serão configurados para excluir estes links.

No cenário, o caminho de menor custo é através da VLAN 15, porém este link possui alta latência então foi excluído.



Primeiramente, será realizada a configuração das interfaces e do OSPF.

```

!Equipment A
config
dot1q
vlan 10
  interface gigabit-ethernet-1/1/1
  untagged
!
!
vlan 11
  interface gigabit-ethernet-1/1/2
  untagged
!
!
vlan 15
    
```

```

interface gigabit-ethernet-1/1/3
  untagged
  !
  !
  !
switchport
interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 10
  !
interface gigabit-ethernet-1/1/2
  native-vlan
  vlan-id 11
  !
interface gigabit-ethernet-1/1/3
  native-vlan
  vlan-id 15
  !
  !
interface loopback 0
  ipv4 address 198.51.100.1/32
  !
interface l3 VLAN10
  lower-layer-if vlan 10
  ipv4 address 203.0.113.1/30
  !
interface l3 VLAN11
  lower-layer-if vlan 11
  ipv4 address 203.0.113.5/30
  !
interface l3 VLAN15
  lower-layer-if vlan 15
  ipv4 address 203.0.113.21/30
  !
router ospf 1 vrf global
  area 0
  interface l3-VLAN10
    network-type point-to-point
  !
  interface l3-VLAN11
    network-type point-to-point
  !
  interface l3-VLAN15
    network-type point-to-point
  !
  interface loopback-0
  !
  !
  !
commit

```

```

!Equipment B
config
dot1q
vlan 10
  interface gigabit-ethernet-1/1/1
    untagged
  !
  !
vlan 14
  interface gigabit-ethernet-1/1/2
    untagged
  !
  !
switchport
interface gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 10
  !
interface gigabit-ethernet-1/1/2
  native-vlan
  vlan-id 14
  !
  !
interface loopback 0
  ipv4 address 198.51.100.2/32
  !
interface l3 VLAN10
  lower-layer-if vlan 10
  ipv4 address 203.0.113.2/30
  !
interface l3 VLAN14
  lower-layer-if vlan 14
  ipv4 address 203.0.113.17/30
  !
  !

```

```

router ospf 1 vrf global
area 0
interface l3-VLAN10
network-type point-to-point
!
interface l3-VLAN14
network-type point-to-point
!
interface loopback-0
!
!
!
commit

```

```

!Equipment C
config
dot1q
vlan 11
interface gigabit-ethernet-1/1/1
untagged
!
!
vlan 12
interface gigabit-ethernet-1/1/2
untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 11
!
!
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 12
!
!
!
interface loopback 0
ipv4 address 198.51.100.3/32
!
!
interface l3 VLAN11
lower-layer-if vlan 11
ipv4 address 203.0.113.6/30
!
interface l3 VLAN12
lower-layer-if vlan 12
ipv4 address 203.0.113.9/30
!
router ospf 1 vrf global
area 0
interface l3-VLAN11
network-type point-to-point
!
!
interface l3-VLAN12
network-type point-to-point
!
interface loopback-0
!
!
!
commit

```

```

!Equipment D
config
dot1q
vlan 12
interface gigabit-ethernet-1/1/1
untagged
!
!
vlan 13
interface gigabit-ethernet-1/1/2
untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/1
native-vlan
vlan-id 12
!
!
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 13

```

```

!
!
interface loopback 0
  ipv4 address 198.51.100.4/32
!
interface l3 VLAN12
  lower-layer-if vlan 12
  ipv4 address 203.0.113.10/30
!
interface l3 VLAN13
  lower-layer-if vlan 13
  ipv4 address 203.0.113.13/30
!
router ospf 1 vrf global
  area 0
    interface l3-VLAN12
      network-type point-to-point
    !
    interface l3-VLAN13
      network-type point-to-point
    !
    interface loopback-0
  !
!
!
commit

```

```

!Equipment E
config
dot1q
  vlan 13
    interface gigabit-ethernet-1/1/2
      untagged
    !
  !
  vlan 14
    interface gigabit-ethernet-1/1/1
      untagged
    !
  !
  vlan 15
    interface gigabit-ethernet-1/1/3
      untagged
    !
  !
!
switchport
  interface gigabit-ethernet-1/1/1
    native-vlan
      vlan-id 14
    !
  !
  interface gigabit-ethernet-1/1/2
    native-vlan
      vlan-id 13
    !
  !
  interface gigabit-ethernet-1/1/3
    native-vlan
      vlan-id 15
    !
  !
!
!
interface loopback 0
  ipv4 address 198.51.100.5/32
!
interface l3 VLAN13
  lower-layer-if vlan 13
  ipv4 address 203.0.113.14/30
!
interface l3 VLAN14
  lower-layer-if vlan 14
  ipv4 address 203.0.113.18/30
!
interface l3 VLAN15
  lower-layer-if vlan 15
  ipv4 address 203.0.113.22/30
!
router ospf 1 vrf global
  area 0
    interface l3-VLAN13
      network-type point-to-point
    !
    interface l3-VLAN14
      network-type point-to-point
    !
    interface l3-VLAN15
      network-type point-to-point
    !
!
!

```

```
interface loopback-0
!
!
commit
```

Em seguida, é necessário habilitar o RSVP nas interfaces e no OSPF.

As informações dos atributos de cada link são divulgadas através do OSPF. O protocolo RSVP define um caminho e sinaliza o túnel com base nas informações do OSPF.

```
!Equipment A
config
router ospf 1 vrf global
 mpls-te router-id loopback-0
!
mpls rsvp
 interface l3-VLAN10
!
 interface l3-VLAN11
!
 interface l3-VLAN15
!
!
commit
```

```
!Equipment B
config
router ospf 1 vrf global
 mpls-te router-id loopback-0
!
mpls rsvp
 interface l3-VLAN10
!
 interface l3-VLAN14
!
!
commit
```

```
!Equipment C
config
router ospf 1 vrf global
 mpls-te router-id loopback-0
!
mpls rsvp
 interface l3-VLAN11
!
 interface l3-VLAN12
!
!
commit
```

```
!Equipment D
config
router ospf 1 vrf global
 mpls-te router-id loopback-0
!
mpls rsvp
 interface l3-VLAN12
!
 interface l3-VLAN13
!
!
commit
```

```
!Equipment E
config
router ospf 1 vrf global
 mpls-te router-id loopback-0
!
mpls rsvp
 interface l3-VLAN13
!
 interface l3-VLAN14
!
 interface l3-VLAN15
```

```
!  
commit
```

O próximo passo é a configuração dos atributos nas interfaces.

```
!Equipment A  
config  
mpls traffic-eng  
interface l3-VLAN10  
affinity-flags 0x2  
!  
interface l3-VLAN11  
affinity-flags 0x1  
!  
interface l3-VLAN15  
affinity-flags 0x6  
!  
!  
commit
```

```
!Equipment B  
config  
mpls traffic-eng  
interface l3-VLAN10  
affinity-flags 0x2  
!  
interface l3-VLAN14  
affinity-flags 0x2  
!  
!  
commit
```

```
!Equipment C  
config  
mpls traffic-eng  
interface l3-VLAN11  
affinity-flags 0x1  
!  
interface l3-VLAN12  
affinity-flags 0x1  
!  
!  
commit
```

```
!Equipment D  
config  
mpls traffic-eng  
interface l3-VLAN12  
affinity-flags 0x1  
!  
interface l3-VLAN13  
affinity-flags 0x1  
!  
!  
commit
```

```
!Equipment E  
config  
mpls traffic-eng  
interface l3-VLAN13  
affinity-flags 0x1  
!  
interface l3-VLAN14  
affinity-flags 0x2  
!  
interface l3-VLAN15  
affinity-flags 0x6  
!  
!  
commit
```

Após habilitado o RSVP e os atributos *affinity* configurados, é possível subir os túneis. A configuração do túnel precisa ser feita somente no equipamento de origem.

Existem três formas de selecionar o caminho utilizando *affinity*. Links que não obedecem às regras configuradas na definição do caminho (*path-option*) não são considerados para estabelecimento do túnel.

- **include-any** - Deve ocorrer match em pelo menos um bit do valor do link. Caso o valor do parâmetro **include-any** for 0, o link é aceito independentemente do valor do seu atributo **affinity**.
- **include-all** - Todos os bits configurados no parâmetro devem também estar configurados no link. Caso o valor do parâmetro **include-all** for 0, o link é aceito independentemente do valor do seu atributo **affinity**.
- **exclude-any** - Links que possuam qualquer um dos bits especificados são excluídos.

Para estes túneis, foram definidos dois caminhos. O caminho primário **HIGH-CAPACITY-LOW-DELAY** será estabelecido somente por links que possuam atributo referente a alta capacidade (**include-any 0x1**) e não possuam o atributo referente a alta latência (**exclude-any 0x4**).

O caminho **LOW-CAPACITY-LOW-DELAY** pode ser estabelecido somente por links com atributo referente a baixa capacidade (**include-any 0x2**) e não possuam o atributo referente a alta latência (**exclude-any 0x4**).

A ordem de prioridade dos caminhos é definida por um número ao associar o caminho ao túnel. Na configuração abaixo, o *path 10* tem prioridade sobre o *path 20*.

```
!Equipment A
config
mpls traffic-eng
attribute-set
  path-option HIGH-CAPACITY-LOW-DELAY
  affinity-flags exclude-any 0x4
  affinity-flags include-any 0x1
!
  path-option LOW-CAPACITY-LOW-DELAY
  affinity-flags exclude-any 0x4
  affinity-flags include-any 0x2
!
!
interface tunnel-te 1
destination 198.51.100.5
  path 10 dynamic attribute-set HIGH-CAPACITY-LOW-DELAY
  path 20 dynamic attribute-set LOW-CAPACITY-LOW-DELAY
!
commit
```

```
!Equipment E
config
mpls traffic-eng
attribute-set
  path-option HIGH-CAPACITY-LOW-DELAY
  affinity-flags exclude-any 0x4
  affinity-flags include-any 0x1
!
  path-option LOW-CAPACITY-LOW-DELAY
  affinity-flags exclude-any 0x4
  affinity-flags include-any 0x2
!
!
interface tunnel-te 1
destination 198.51.100.1
  path 10 dynamic attribute-set HIGH-CAPACITY-LOW-DELAY
  path 20 dynamic attribute-set LOW-CAPACITY-LOW-DELAY
!
commit
```

Para exemplos de associação de túnel com L2VPNs, consultar as sessões [VPWS com RSVP](#) ou [VPLS com RSVP](#).

Abaixo os principais comandos disponíveis para realizar o Troubleshooting. Caso o usuário esteja no nível de configuração,

é necessário utilizar a palavra-chave **do** antes do comando.



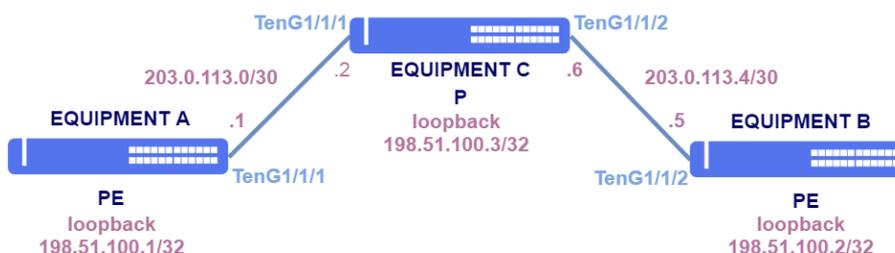
Para maiores detalhes sobre as saídas dos comandos, consulte o **Command Reference**.

```
show mpls traffic-eng tunnel-te brief
show mpls traffic-eng tunnel-te id <tunnel-te-id>
show mpls traffic-eng tunnel-te name <lsp_name>
show mpls forwarding-table
show ip ospf database opaque-area
```

11.3 Configuração de VPWS

Uma VPWS (Virtual Private Wire Service) permite a emulação de serviços Ethernet ponto-a-ponto em uma rede MPLS.

A topologia abaixo será utilizada como base para os exemplos desta sessão.



Topologia base para VPWS

Loopbacks:

Equipamento	Loopback
EQUIPMENT A	198.51.100.1/32
EQUIPMENT B	198.51.100.2/32
EQUIPMENT C	198.51.100.3/32

Endereçamento entre os PEs e o P:

PE	Intf PE	Endereço PE	P	Intf P	Endereço P	VLAN
EQUIP A	TenG1/1/1	203.0.113.1/30	EQUIP C	TenG1/1/2	203.0.113.2/30	10
EQUIP B	TenG1/1/2	203.0.113.5/30	EQUIP C	TenG1/1/1	203.0.113.6/30	20

```
!Equipment A
config
dot1q
vlan 10
```



```

!Equipment C
config
dot1q
vlan 10
interface ten-gigabit-ethernet-1/1/1
untagged
!
!
!
vlan 20
interface ten-gigabit-ethernet-1/1/2
untagged
!
!
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
native-vlan
vlan-id 10
!
!
interface ten-gigabit-ethernet-1/1/2
native-vlan
vlan-id 20
!
!
!
!
interface l3 VLAN10
ipv4 address 203.0.113.2/30
lower-layer-if vlan 10
!
!
interface l3 VLAN20
ipv4 address 203.0.113.6/30
lower-layer-if vlan 20
!
!
!
interface loopback 0
ipv4 address 198.51.100.3/32
!
!
router ospf 1
router-id 198.51.100.3
area 0
interface l3-VLAN10
network-type point-to-point
!
interface l3-VLAN20
network-type point-to-point
!
interface loopback-0
!
!
!
!
mpls ldp
lsr-id loopback-0
interface l3-VLAN10
interface l3-VLAN20
!
!
!
commit

```

11.3.1 VPWS com LDP

A sinalização de VPNs pode ser feita através do protocolo LDP. Para que isto ocorra, é necessário estabelecer uma sessão LDP targeted entre os PEs, conforme demonstrado a seguir.

```

!Equipment A
config
mpls ldp
lsr-id loopback-0
neighbor targeted 198.51.100.2
!
!
!
commit

```

```

!Equipment B
config
mpls ldp
  lsr-id loopback-0
  neighbor targeted 198.51.100.1
!
!
!
commit

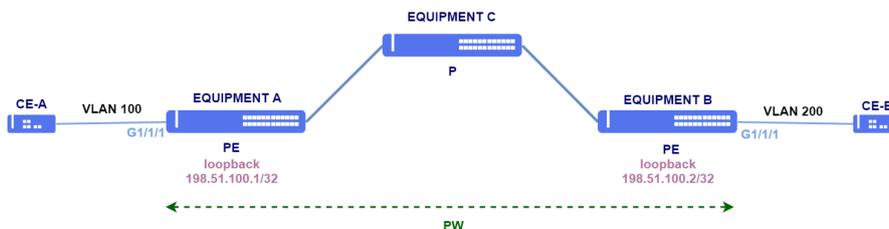
```



O MTU configurado no PW é utilizado exclusivamente para sinalização e deve ser igual entre os neighbors da VPN. Caso não seja especificado o valor do pw-mtu, o valor considerado será o especificado na AC (access-interface), que, por padrão, utiliza 9198 bytes.

Configurando uma VPWS com PW type VLAN - Caso 1

Na topologia abaixo, há uma VPN com PW do tipo VLAN com interfaces de acesso com dot1q configurado. A tag de VLAN utilizada nas pontas da VPN é diferente.



Configuração de VPNs com PW type VLAN

Ambas as interfaces de acesso são do tipo *tagged*, ou seja, irá permitir que somente frames com a VLAN configurada sejam encapsulados e transportados.

Neste cenário, a ponta A da VPN recebe a VLAN 100 e a ponta B, a VLAN 200. O frame recebido com a VLAN 100 do CE-A é encaminhado à ponta B (EQUIPMENT B), porém terá o tag substituído pelo tag 200 antes de ser enviado ao CE-B. O frame recebido com tag 200 do CE-B é encaminhado à ponta A (EQUIPMENT A), porém tem o tag substituído por 100 antes de ser enviado ao CE-A. Desta forma, é possível a comunicação entre VLANs diferentes.

```

!Equipment A
config
mpls l2vpn
vpws-group CUSTOMER1
  vpn VPN1
  neighbor 198.51.100.2
  pw-type vlan
  pw-id 100
!
!
!
access-interface gigabit-ethernet-1/1/1
  dot1q 100
!
!
!
commit

```

```

!Equipment B
config
mpls l2vpn
vpws-group CUSTOMER1

```

```

vpn VPN1
 neighbor 198.51.100.1
  pw-type vlan
  pw-id 100
  !
  !
 access-interface gigabit-ethernet-1/1/1
  dot1q 200
  !
  !
 !
 !
commit

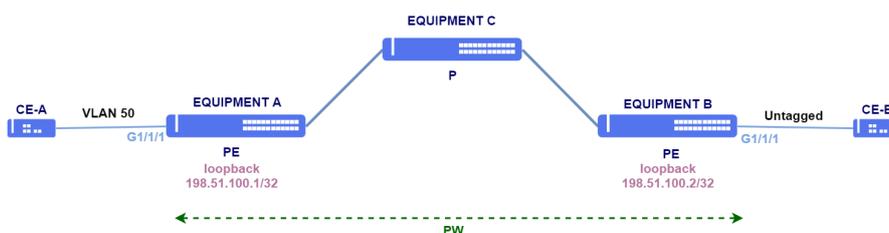
```



Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L2VPNs](#).

Configurando uma VPWS com PW type VLAN - Caso 2

Na topologia abaixo, há uma VPN com PW do tipo VLAN com interface de acesso com dot1q no site A e interface de acesso untagged no site B.



Configuração de VPNs com PW type VLAN

A sinalização das VPNs é feita através do protocolo LDP. Para que isto ocorra, é necessário estabelecer uma sessão LDP targeted entre os PEs, conforme demonstrado a seguir.

```

!Equipment A
config
 mpls ldp
  lsr-id loopback-0
  neighbor targeted 198.51.100.2
  !
  !
 !
 !
commit

```

```

!Equipment B
config
 mpls ldp
  lsr-id loopback-0
  neighbor targeted 198.51.100.1
  !
  !
 !
 !
commit

```

A interface de acesso do lado A é do tipo *tagged* e irá permitir que somente a VLAN 50 seja encapsulada. No lado B, a interface é untagged.

O frame recebido com VLAN 50 do CE-A é encaminhado à ponta B (EQUIPMENT B), porém terá o tag removido antes de ser


```

!
access-interface gigabit-ethernet-1/1/1
!
!
!
commit

```

```

!Equipment B
config
mpls l2vpn
vpws-group CUSTOMER1
vpn VPN4
neighbor 198.51.100.1
pw-type ethernet
pw-id 103
!
!
access-interface gigabit-ethernet-1/1/1
dot1q 500
!
!
!
commit

```

```

!Equipment D
config
dot1q
vlan 500
interface gigabit-ethernet-1/1/5
!
interface gigabit-ethernet-1/1/20
untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/20
native-vlan
vlan-id 500
!
qinq
!
!
commit

```

11.3.2 VPWS com RSVP

VPWS podem ser configuradas para trafegarem sobre túneis RSVP. A configuração da VPN é semelhante aos exemplos já demonstrados na sessão [VPWS com LDP](#). A única diferença é a associação do neighbor a um túnel.



A sinalização de L2VPNs ainda ocorre por uma sessão LDP targeted. Somente o tráfego de L2VPNs é encaminhado através de túneis.

No exemplo abaixo, foi associado o túnel 10 ao neighbor 198.51.100.2. O tráfego com destino a este neighbor será encaminhado através do túnel.

```

config
mpls l2vpn
vpws-group CUSTOMER1
vpn VPN1
neighbor 198.51.100.2
pw-type vlan
pw-id 100
tunnel-interface tunnel-te-10
!

```


MPLS com acesso GPON

A configuração para o serviço GPON que será utilizada como base para o MPLS esta disponível a seguir:

Profile GPON

```
config
!
profile gpon bandwidth-profile 100Mbps
  traffic type-4 max-bw 100032
!
profile gpon line-profile MPLS
  upstream-fec
  tcont 1 bandwidth-profile 100Mbps
  gem 1
    tcont 1 priority 0
    map 1
      ethernet 1 vlan 2282 cos any
  !
  gem 2
    tcont 1 priority 0
    map 2
      ethernet 1 vlan 2292 cos any
!
commit
```

Provisionamento de ONU

```
config
!
interface gpon 1/1/1
  onu 1
    serial-number DACM000BBB01
    line-profile MPLS
    ethernet 1
      negotiation
      no shutdown
  !
  onu 2
    serial-number DACM000BBB02
    line-profile MPLS
    ethernet 1
      negotiation
      no shutdown
!
commit
```

Para mais detalhes na configuração de GPON, consultar a sessão [Configurando Aplicações GPON](#).

Infraestrutura MPLS

A configuração para a infraestrutura MPLS que será utilizada nos casos de uso desta sessão, estão disponíveis a seguir. As configurações disponíveis são apenas para os equipamentos A e B (PE).

```
!Equipment A
config
!
dot1q
  vlan 100
  interface ten-gigabit-ethernet-1/1/1 untagged
!
switchport interface ten-gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 100
!
interface l3 MPLS-GPON
  lower-layer-if vlan 100
  ipv4 address 10.10.10.1/30
!
interface loopback 0
  ipv4 address 172.30.5.250/32
!
router ospf 1
```

```
area 0
 interface l3-MPLS-GPON
   network-type point-to-point
 !
 interface loopback-0
 !
 !
mpls ldp
 lsr-id loopback-0
 interface l3-MPLS-GPON
   neighbor targeted 172.30.6.4
 !
 !
commit
```

```
!Equipment B
config
 !
 !
dot1q
 vlan 100
   interface ten-gigabit-ethernet-1/1/1 untagged
 !
switchport interface ten-gigabit-ethernet-1/1/1
 native-vlan
   vlan-id 100
 !
interface l3 MPLS-GPON
 lower-layer-if vlan 100
 ipv4 address 10.10.10.2/30
 !
interface loopback 0
 ipv4 address 172.30.6.4/32
 !
router ospf 1
 area 0
   interface l3-MPLS-GPON
     network-type point-to-point
 !
 interface loopback-0
 !
 !
mpls ldp
 lsr-id loopback-0
 interface l3-MPLS-GPON
   neighbor targeted 172.30.5.250
 !
 !
commit
```

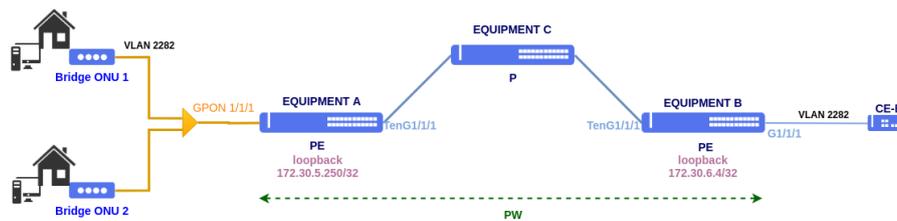
Após realizar as configurações acima, deve-se verificar se existe comunicação entre os neighbors LDP. Para mais informações sobre o protocolo LDP, consultar o tópico [Configuração do LDP](#).



Mais detalhes sobre a configuração da infraestrutura MPLS com VPWS, consultar o tópico [Configuração do VPWS](#).

Configurando uma VPWS com PW type VLAN e acesso service-port - Caso 1

Para este caso de uso, a service-port de cada ONU será a interface de acesso para uma VPWS que é estabelecida com a rede MPLS. Estas service-ports podem coexistir com as demais service-ports utilizadas para outros serviços, como por exemplo, acesso à internet, tráfego Multicast/IGMP para tráfego de vídeo ou ainda telefonia VOIP. Vale salientar que a service-port utilizada na VPN pode ser criada na ativação de uma nova ONU ou ser utilizada em adição aos serviços em operação. Para tanto, os perfis utilizados na ONU devem ser editados a fim de contemplar todos os serviços.



VPWS com acesso service-port

Para realizar esta configuração a L2VPN deve ser configurada com PW type VLAN e modo VLAN Based usando a service-port como interface de acesso. Somente o tráfego da VLAN 2282 mapeada no service-port através do gem 1 é encapsulado na L2VPN.

Service port

```
!Equipment A
config
service-port 2282 gpon 1/1/1 onu 1 gem 1
commit
```

É importante notar que nos casos onde as service-ports serão utilizadas como interface de acesso para o MPLS, não será necessária a indicação de VLAN, como é demonstrado no exemplo para a service-port 2282.

```
!Equipment A
config
mpls l2vpn
vpws-group GPON_VPWS
vpn 2282
description VPWS_VLAN_BASED_SP
neighbor 172.30.6.4
pw-type vlan
pw-id 2282
pw-mtu 2000
!
access-interface service-port 2282
dot1q 2282
mtu 2000
!
commit
```

No exemplo é configurado **MTU de 2000 bytes** tanto no PW quanto no acesso devido ao limite máximo de MTU suportado pela ONU. Esse valor pode ser alterado conforme necessário, respeitando o limite de cada equipamento.

```
!Equipment B
config
mpls l2vpn
vpws-group GPON_VPWS
vpn 2282
description VPWS_VLAN_BASED_SP
neighbor 172.30.5.250
pw-type vlan
pw-id 2282
pw-mtu 2000
!
access-interface gigabit-ethernet 1/1/1
dot1q 2282
mtu 2000
!
commit
```

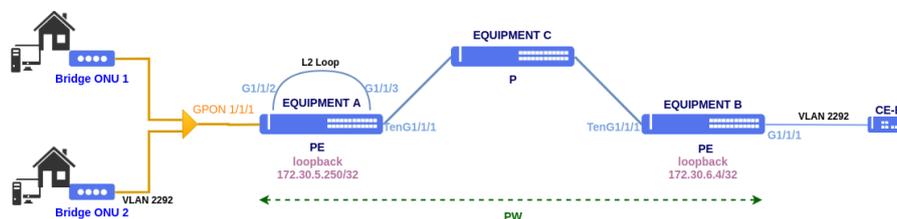


Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L2VPNs](#).

Configurando uma VPWS com PW type VLAN e acesso Ethernet - Caso 2

Para o serviço aqui proposto, a interface GbE-1/1/2 será utilizada como Uplink da OLT para os serviços GPON, sendo a configuração dos serviços GPON realizada de maneira convencional, como se a interface GbE-1/1/2 fosse de fato a interface de Uplink da OLT, sem levar em consideração a parte MPLS.

Após configurada a OLT, a interface GbE-1/1/2 será conectada fisicamente à interface GbE-1/1/3 criando um loop físico entre elas, a interface GbE-1/1/3 será a interface de acesso para uma VPWS que será interligada com a rede MPLS.



VPN acesso GPON com Ethernet loop

Para esse cenário é necessário mapear na OLT a **interface gigabit-ethernet-1/1/2 na VLAN 2292** e criar o service-port para o mapeamento da VLAN 2292 na ONU.

VLAN de serviço

```
!Equipment A
config
!
dot1q
vlan 2292
interface gigabit-ethernet-1/1/2
!
service vlan 2292
type tlv
!
!
commit
```

Service port

```
!Equipment A
config
!
service-port 2292
gpon 1/1/1 onu 2 gem 2 match vlan vlan-id 2292 action vlan replace vlan-id 2292
!
!
commit
```

Para os casos onde o acesso MPLS utiliza interface Ethernet a service-port utilizada para o MPLS realiza match em VLAN, como é demonstrado no exemplo para a **service-port 2292**.

```
!Equipment A
config
mpls l2vpn
vpn 2292
description VPWS_VLAN_BASED_ETH
neighbor 172.30.6.4
pw-type vlan
pw-id 2292
pw-mtu 2000
!
access-interface gigabit-ethernet-1/1/3
dot1q 2292
mtu 2000
!
!
commit
```

No exemplo é configurado **MTU de 2000 bytes** tanto no PW quanto no acesso devido ao limite máximo de MTU suportado pela ONU. Esse valor pode ser alterado conforme necessário, respeitando o limite de cada equipamento.

```
!Equipment B
config
mpls l2vpn
vpws-group GPON_VPWS
vpn 2292
description VPWS_VLAN_BASED_ETH
neighbor 172.30.5.250
pw-type vlan
pw-id 2292
pw-mtu 2000
!
access-interface gigabit-ethernet 1/1/1
dot1q 2292
mtu 2000
!
!
commit
```

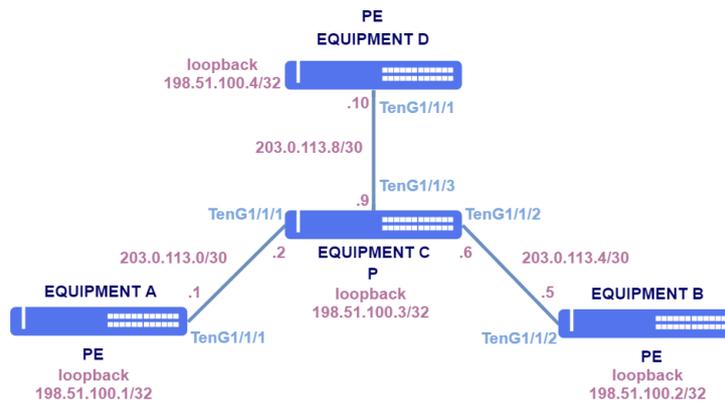


Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L2VPNs](#).

11.4 Configuração de VPLS

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 domínio de broadcast, emulando um serviço Ethernet ponto-multiponto.

A topologia abaixo será utilizada como base para os exemplos de VPLS nesta sessão.



Topologia para VPLS

Loopbacks:

Equipamento	Loopback
EQUIPMENT A	198.51.100.1/32
EQUIPMENT B	198.51.100.2/32
EQUIPMENT C	198.51.100.3/32
EQUIPMENT D	198.51.100.4/32

Endereçamento entre PEs e o P:

PE	Intf PE	Endereço PE	P	Intf P	Endereço P	VLAN
EQUIP A	TenG1/1/1	203.0.113.1/30	EQUIP C	TenG1/1/2	203.0.113.2/30	10
EQUIP B	TenG1/1/2	203.0.113.5/30	EQUIP C	TenG1/1/1	203.0.113.6/30	20
EQUIP D	TenG1/1/1	203.0.113.9/30	EQUIP C	TenG1/1/3	203.0.113.10/30	30

```

!Equipment A
config
dot1q
vlan 10
interface ten-gigabit-ethernet-1/1/1
untagged
!
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
native-vlan
vlan-id 10
!
!
interface l3 VLAN10
ipv4 address 203.0.113.1/30
lower-layer-if vlan 10
!
!
interface loopback 0
ipv4 address 198.51.100.1/32
    
```

```

!
router ospf 1
router-id 198.51.100.1
area 0
interface l3-VLAN10
network-type point-to-point
!
interface loopback-0
!
!
!
mpls ldp
lsr-id loopback-0
interface l3-VLAN10
!
!
!
commit

```

```

!Equipment B
config
dot1q
vlan 20
interface ten-gigabit-ethernet-1/1/2
untagged
!
!
!
!
switchport
interface ten-gigabit-ethernet-1/1/2
native-vlan
vlan-id 20
!
!
!
interface l3 VLAN20
ipv4 address 203.0.113.5/30
lower-layer-if vlan 20
!
!
interface loopback 0
ipv4 address 198.51.100.2/32
!
!
router ospf 1
router-id 198.51.100.2
area 0
interface l3-VLAN20
network-type point-to-point
!
interface loopback-0
!
!
!
mpls ldp
lsr-id loopback-0
interface l3-VLAN20
!
!
!
commit

```

```

!Equipment C
config
dot1q
vlan 10
interface ten-gigabit-ethernet-1/1/1
untagged
!
!
!
vlan 20
interface ten-gigabit-ethernet-1/1/2
untagged
!
!
!
vlan 30
interface ten-gigabit-ethernet-1/1/3
untagged
!
!
!
!
switchport
interface ten-gigabit-ethernet-1/1/1

```

```

native-vlan
  vlan-id 10
  !
!
interface ten-gigabit-ethernet-1/1/2
  native-vlan
  vlan-id 20
  !
!
interface ten-gigabit-ethernet-1/1/3
  native-vlan
  vlan-id 30
  !
!
interface l3 VLAN10
  ipv4 address 203.0.113.2/30
  lower-layer-if vlan 10
  !
!
interface l3 VLAN20
  ipv4 address 203.0.113.6/30
  lower-layer-if vlan 20
  !
!
interface l3 VLAN30
  ipv4 address 203.0.113.10/30
  lower-layer-if vlan 30
  !
!
interface loopback 0
  ipv4 address 198.51.100.3/32
  !
!
router ospf 1
  router-id 198.51.100.3
  area 0
  interface l3-VLAN10
  network-type point-to-point
  !
  interface l3-VLAN20
  network-type point-to-point
  !
  interface l3-VLAN30
  network-type point-to-point
  !
  interface loopback-0
  !
!
!
mpls ldp
  lsr-id loopback-0
  interface l3-VLAN10
  !
  interface l3-VLAN20
  !
  interface l3-VLAN30
  !
!
!
commit

```

```

!Equipment D
config
dot1q
  vlan 30
  interface ten-gigabit-ethernet-1/1/1
  untagged
  !
!
!
switchport
interface ten-gigabit-ethernet-1/1/1
  native-vlan
  vlan-id 30
  !
!
!
interface l3 VLAN30
  ipv4 address 203.0.113.9/30
  lower-layer-if vlan 30
  !
!
!
interface loopback 0
  ipv4 address 198.51.100.4/32
  !
!
!

```

```
router ospf 1
router-id 198.51.100.4
area 0
interface l3-VLAN30
network-type point-to-point
!
interface loopback-0
!
!
mpls ldp
lsr-id loopback-0
interface l3-VLAN30
!
!
commit
```

11.4.1 VPLS com LDP

A sinalização das VPNs pode ser feita através do protocolo LDP. Para que isto ocorra, é necessário estabelecer uma sessão LDP targeted entre os PEs, conforme demonstrado a seguir.

```
!Equipment A
config
mpls ldp
lsr-id loopback-0
neighbor targeted 198.51.100.2
!
neighbor targeted 198.51.100.4
!
!
commit
```

```
!Equipment B
config
mpls ldp
lsr-id loopback-0
neighbor targeted 198.51.100.1
!
neighbor targeted 198.51.100.4
!
!
commit
```

```
!Equipment D
config
mpls ldp
lsr-id loopback-0
neighbor targeted 198.51.100.1
!
neighbor targeted 198.51.100.2
!
!
commit
```



O MTU configurado no PW é utilizado exclusivamente para sinalização e deve ser igual entre os neighbors da VPN. Caso não seja especificado o valor do pw-mtu, o valor considerado será o especificado na AC (access-interface), que, por padrão, utiliza 9198 bytes.

11.6 Verificando L2VPNs

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



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

```
show mpls l2vpn hardware
show mpls l2vpn vpws-group brief
show mpls l2vpn vpws-group detail
show mpls l2vpn vpls-group brief
show mpls l2vpn vpls-group detail
show mpls ldp database
show mpls ldp neighbor
show mpls ldp parameters
show mpls forwarding-table
```

11.7 Configuração de L3VPNs

11.7.1 Configurando uma L3VPN Site-to-Site

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.



É necessário ter o protocolo LDP já configurado na rede para que seja possível utilizar L3VPN.



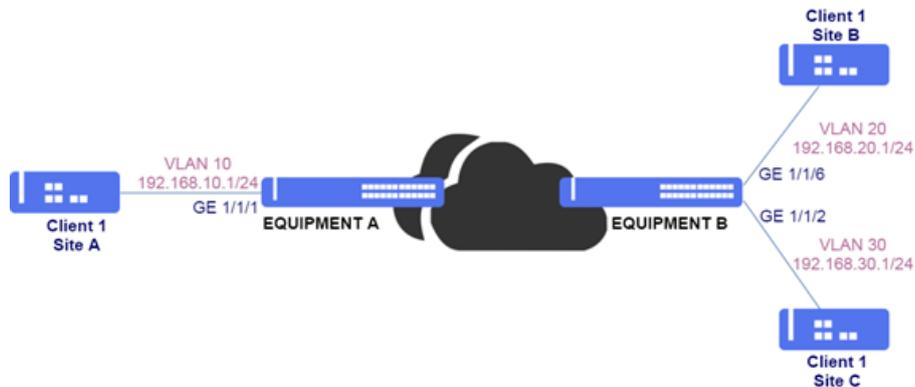
Apesar do formato do route-distinguisher ser semelhante ao route-target, ambos são independentes e tem funções diferentes.



A troca de labels e redes das L3VPN é feita através do BGP. Para isto, é necessário habilitar a família vpnv4 no protocolo BGP.

Na topologia a seguir, serão configurados dois switches PE (EQUIPMENT A e EQUIPMENT B). No EQUIPMENT A, há uma

interface com endereço IP 192.168.10.1/24 conectada a um CE (Site A). No EQUIPMENT B há duas interfaces, uma com o endereço IP 192.168.20.1/24 e outra com o endereço IP 192.168.30.1/24 conectadas a outros dois CEs (Site B e Site C). Os EQUIPMENT A e B possuem endereços de loopback 1.1.1.1/32 e 2.2.2.2/32, respectivamente. As redes diretamente conectadas serão redistribuídas entre os PEs. Os PEs estão conectados pela interface gigabit-ethernet-1/1/5 com o uso dos protocolos OSPF e LDP para prover a infraestrutura para L3VPN através do AS1000.



L3VPN em cenário Site-to-Site

```

!Equipment A
config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1
!
vlan 1000
interface gigabit-ethernet-1/1/5
untagged
!
!
switchport
interface gigabit-ethernet-1/1/5
native-vlan
vlan-id 1000
!
!
vrf cli1
rd 1000:10
address-family ipv4 unicast
route-target import 1000:10
!
route-target export 1000:10
!
!
interface l3 OSPF
lower-layer-if vlan 1000
ipv4 address 10.10.10.1/30
!
interface l3 VRF-CLI1-VLAN10
vrf cli1
lower-layer-if vlan 10
ipv4 address 192.168.10.1/24
!
interface loopback 0
ipv4 address 1.1.1.1/32
!
router ospf 1
router-id 1.1.1.1
area 0
interface l3-OSPF
network-type point-to-point
!
interface loopback-0
!
!
router bgp 1000
router-id 1.1.1.1
address-family ipv4 unicast
!
address-family vpnv4 unicast

```

```

!
neighbor 2.2.2.2
  update-source-address 1.1.1.1
  remote-as 1000
  next-hop-self
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
!
vrf cli1
  address-family ipv4 unicast
  redistribute connected
  !
  exit-address-family
  !
!
!
mpls ldp
  lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 2.2.2.2
  !
!
!
commit

```

```

!Equipment B
config
dot1q
vlan 20
  interface gigabit-ethernet-1/1/6
  !
vlan 30
  interface gigabit-ethernet-1/1/2
  !
vlan 1000
  interface gigabit-ethernet-1/1/5
  untagged
  !
!
!
switchport
interface gigabit-ethernet-1/1/5
  native-vlan
  vlan-id 1000
  !
!
!
vrf cli1
  rd 1000:10
  address-family ipv4 unicast
  route-target import 1000:10
  !
  route-target export 1000:10
  !
!
!
interface l3 OSPF
  lower-layer-if vlan 1000
  ipv4 address 10.10.10.2/30
  !
interface l3 VRF-CLI1-VLAN20
  vrf cli1
  lower-layer-if vlan 20
  ipv4 address 192.168.20.1/24
  !
interface l3 VRF-CLI1-VLAN30
  vrf cli1
  lower-layer-if vlan 30
  ipv4 address 192.168.30.1/24
  !
interface loopback 0
  ipv4 address 2.2.2.2/32
  !
router ospf 1
  router-id 2.2.2.2
  area 0
  interface l3-OSPF
  network-type point-to-point
  !
  interface loopback-0
  !
!
!
router bgp 1000
  router-id 2.2.2.2
  address-family ipv4 unicast
  !

```

```

address-family vpnv4 unicast
!
neighbor 1.1.1.1
  update-source-address 2.2.2.2
  remote-as 1000
  next-hop-self
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
!
vrf cli1
  address-family ipv4 unicast
  redistribute connected
  exit-address-family
!
!
!
mpls ldp
  lsr-id loopback-0
  interface l3-OSPF
  neighbor targeted 1.1.1.1
!
!
commit

```



Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L3VPNs](#).

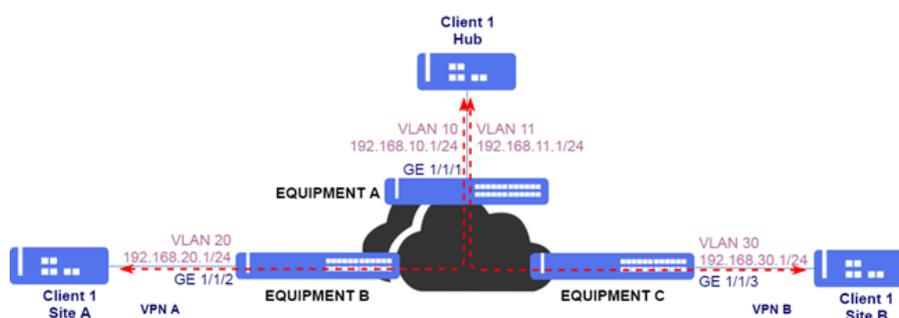
11.7.2 Configurando uma L3VPN Hub and Spoke

Em uma topologia hub-and-spoke, diferentes CEs (Hub, Site A e Site B) de um cliente conseguem acessar um site central chamado hub, porém não conseguem se comunicar entre si.

No diagrama abaixo, os sites A e B devem ter conectividade com o site central, porém não devem conseguir se comunicar entre eles. O tráfego dos sites A e B será sempre encaminhado ao hub. Para isto, é necessário haver duas VPNs, uma entre o site A e o hub e outra entre o site B e o hub.

O hub, sendo o site central por onde passa todo o tráfego, poderá controlar o roteamento entre os sites.

Na topologia a seguir, os PEs (EQUIPMENT A e EQUIPMENT B) estão conectados pela interface gigabit-ethernet-1/1/5 e os PEs (EQUIPMENT A e EQUIPMENT C) estão conectados pela interface gigabit-ethernet-1/1/6 com o uso dos protocolos OSPF e LDP para prover a infraestrutura para a L3VPN através do AS1000.



L3VPN em cenário Hub and Spoke

```

!Equipment A
config
dot1q
vlan 10
!
interface gigabit-ethernet-1/1/1
!
vlan 11
interface gigabit-ethernet-1/1/1
!
vlan 1000
interface gigabit-ethernet-1/1/5
untagged
!
!
vlan 2000
interface gigabit-ethernet-1/1/6
untagged
!
!
!
switchport
interface gigabit-ethernet-1/1/5
native-vlan
vlan-id 1000
!
!
interface gigabit-ethernet-1/1/6
native-vlan
vlan-id 2000
!
!
!
!
vrf cli1-A
rd 1000:20
address-family ipv4 unicast
route-target import 1000:20
!
route-target export 1000:20
!
!
!
vrf cli1-B
rd 1000:30
address-family ipv4 unicast
route-target import 1000:30
!
route-target export 1000:30
!
!
!
!
interface l3 OSPF_A-B
lower-layer-if v_lan 1000
ipv4 address 10.10.10.1/30
!
interface l3 OSPF_A-C
lower-layer-if v_lan 2000
ipv4 address 20.20.20.1/30
!
interface l3 VRF-CLI1-A-VLAN10
vrf cli1-A
lower-layer-if v_lan 10
ipv4 address 192.168.10.1/24
!
interface l3 VRF-CLI1-B-VLAN11
vrf cli1-B
lower-layer-if v_lan 11
ipv4 address 192.168.11.1/24
!
interface loopback 0
ipv4 address 1.1.1.1/32
!
router static
vrf cli1-A
address-family ipv4
0.0.0.0/0 next-hop 192.168.10.2
!
!
!
vrf cli1-B
address-family ipv4
0.0.0.0/0 next-hop 192.168.11.2
!
!
!
!
router ospf 1
router-id 1.1.1.1
area 0
interface l3-OSPF_A-B
network-type point-to-point
!

```

```

interface l3-OSPF A-C
  network-type point-to-point
!
interface loopback-0
!
!
!
router bgp 1000
  router-id 1.1.1.1
  address-family ipv4 unicast
!
  address-family vpnv4 unicast
!
  neighbor 2.2.2.2
    update-source-address 1.1.1.1
    remote-as 1000
    next-hop-self
  address-family ipv4 unicast
!
  address-family vpnv4 unicast
!
  neighbor 3.3.3.3
    update-source-address 1.1.1.1
    remote-as 1000
    next-hop-self
  address-family ipv4 unicast
!
  address-family vpnv4 unicast
!
!
vrf cli1-A
  address-family ipv4 unicast
    redistribute connected
    redistribute static
!
  exit-address-family
!
vrf cli1-B
  address-family ipv4 unicast
    redistribute connected
    redistribute static
!
  exit-address-family
!
!
!
mpls ldp
  lsr-id loopback-0
  interface l3-OSPF_A-B
!
  interface l3-OSPF_A-C
!
  neighbor targeted 2.2.2.2
!
  neighbor targeted 3.3.3.3
!
!
!
commit

```

```

!Equipment B
config
dot1q
vlan 20
  interface gigabit-ethernet-1/1/2
!
vlan 1000
  interface gigabit-ethernet-1/1/5
    untagged
!
!
switchport
  interface gigabit-ethernet-1/1/5
    native-vlan
    vlan-id 1000
!
!
!
vrf cli1
  rd 1000:10
  address-family ipv4 unicast
    route-target import 1000:10
!
  route-target export 1000:10
!
!
!
interface l3 OSPF_A-B
  lower-layer-if vlan 1000

```

```

!
ipv4 address 10.10.10.2/30
!
interface l3 VRF-CLI1-VLAN20
vrf cli1
lower-layer-if vlan 20
ipv4 address 192.168.20.1/24
!
interface loopback 0
ipv4 address 2.2.2.2/32
!
router ospf 1
router-id 2.2.2.2
area 0
interface l3-OSPF_A-B
network-type point-to-point
!
interface loopback-0
!
!
!
router bgp 1000
router-id 2.2.2.2
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
neighbor 1.1.1.1
update-source-address 2.2.2.2
remote-as 1000
next-hop-self
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
!
vrf cli1
address-family ipv4 unicast
redistribute connected
!
exit-address-family
!
!
!
mpls ldp
lsr-id loopback-0
interface l3-OSPF_A-B
!
neighbor targeted 1.1.1.1
!
!
commit

```

```

!Equipment C
config
dot1q
vlan 30
interface gigabit-ethernet-1/1/3
!
vlan 2000
interface gigabit-ethernet-1/1/6
untagged
!
!
switchport
interface gigabit-ethernet-1/1/6
native-vlan
vlan-id 2000
!
!
!
!
vrf cli1
rd 1000:30
address-family ipv4 unicast
route-target import 1000:30
!
route-target export 1000:30
!
!
!
interface l3 OSPF_A-C
lower-layer-if vlan 2000
ipv4 address 20.20.20.2/30
!
interface l3 VRF-CLI1-VLAN30
vrf cli1
lower-layer-if vlan 30
ipv4 address 192.168.30.1/24
!
!

```

```
interface loopback 0
  ipv4 address 3.3.3.3/32
!
router ospf 1
  router-id 3.3.3.3
  area 0
    interface l3-OSPF_A-C
      network-type point-to-point
    !
    interface loopback-0
    !
!
!
router bgp 1000
  router-id 3.3.3.3
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
  neighbor 1.1.1.1
    update-source-address 3.3.3.3
    remote-as 1000
    next-hop-self
    address-family ipv4 unicast
    !
    address-family vpnv4 unicast
  !
!
!
vrf cli1
  address-family ipv4 unicast
    redistribute connected
  !
  exit-address-family
!
!
!
mpls ldp
  lsr-id loopback-0
  interface l3-OSPF_A-C
    !
    neighbor targeted 1.1.1.1
  !
!
!
commit
```

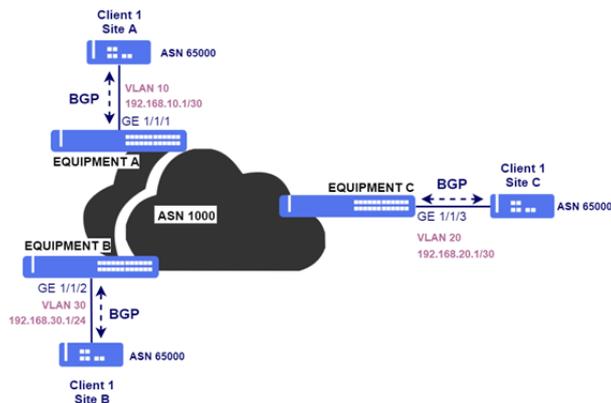


Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L3VPNs](#).

11.7.3 Configurando BGP entre PEs e CEs

Afim de evitar a configuração de rotas estáticas nos PEs (EQUIPMENT A, B e C), recomenda-se configurar um protocolo de roteamento entre PEs e CEs (Hub, Site A e Site B) para que seja feita distribuição de rotas. Na topologia abaixo, será configurado protocolo BGP. Os CEs estão no AS 65000 e os PEs estão no AS 1000. Como estamos utilizando iBGP nos CEs é necessário configurar o parâmetro *as-override* no neighbor BGP para evitar que o mecanismo de detecção de loop do BGP descarte os prefixos trocados entre os CEs.

Pode-se também utilizar o protocolo OSPF entre PEs e CEs para distribuição de rotas, como demonstrado em [Configurando OSPF entre PEs e CEs](#).



L3VPN com sessão eBGP entre o PE e o CE

```

!Equipment A
config
router bgp 1000
router-id 1.1.1.1
address-family ipv4 unicast
!
address-family vpv4 unicast
!
vrf cli1
address-family ipv4 unicast
redistribute connected
!
exit-address-family
!
neighbor 192.168.10.2
update-source-address 192.168.10.1
remote-as 65000
next-hop-self
address-family ipv4 unicast
as-override
exit-address-family
commit

```

```

!Equipment B
config
router bgp 1000
router-id 2.2.2.2
address-family ipv4 unicast
!
address-family vpv4 unicast
!
vrf cli1
address-family ipv4 unicast
redistribute connected
!
exit-address-family
!
neighbor 192.168.20.2
update-source-address 192.168.20.1
remote-as 65000
next-hop-self
address-family ipv4 unicast
as-override
exit-address-family
commit

```

```

!Equipment C
config
router bgp 1000
router-id 3.3.3.3
address-family ipv4 unicast
!
address-family vpv4 unicast
!
vrf cli1
address-family ipv4 unicast
redistribute connected
!
exit-address-family
!

```

```
neighbor 192.168.30.2
update-source-address 192.168.30.1
remote-as 65000
next-hop-self
address-family ipv4 unicast
as-override
exit-address-family
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L3VPNs](#).

11.7.4 Habilitando o AS Override

Em alguns cenários de L3VPN, pode ser necessário alterar o AS PATH para evitar que o mecanismo de detecção de loop do neighbor BGP descarte os prefixos recebidos. Para isto, pode ser utilizada a feature de AS Override.

```
router bgp 1000
vrf cli1
neighbor 192.168.30.2
address-family ipv4 unicast
as-override
exit-address-family
!
commit
```

11.7.5 Habilitando o Allow AS In

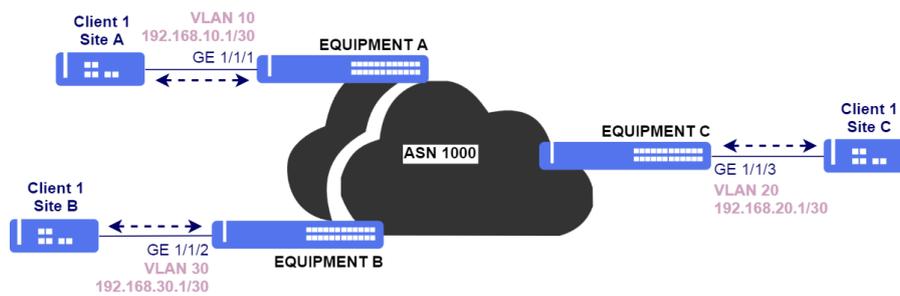
Também pode ser utilizado a feature de Allow AS In para permitir que AS PATHs com loop sejam permitidos no PE.

```
router bgp 1000
vrf cli1
neighbor 192.168.30.2
address-family ipv4 unicast
allow-as-in 1
exit-address-family
!
commit
```

11.7.6 Configurando OSPF entre PEs e CEs

Afim de evitar a configuração de rotas estáticas nos PEs (EQUIPMENT A, B e C), recomenda-se configurar um protocolo de roteamento os PEs e CEs (Hub, Site A e Site B) para que seja feita distribuição de rotas. Na topologia abaixo, será configurado o protocolo OSPF.

Pode-se também utilizar o protocolo BGP entre o CE e PE para distribuição de rotas, como demonstrado em [Configurando BGP entre PEs e CEs](#).



L3VPN com OSPF entre o PE e o CE

Para que as rotas recebidas via MP-BGP dos outros PEs sejam anunciadas aos CEs, deve-se redistribuir as rotas na configuração do OSPF com **redistribute bgp**.

Para que as rotas recebidas dos CEs via OSPF sejam anunciadas aos PEs via MP-BGP, deve-se redistribuir estas rotas com **redistribute ospf** na configuração do BGP.

```
!Equipment A
config
router bgp 1000
vrf cli1
address-family ipv4 unicast
redistribute ospf
!
exit-address-family
!!
!
router ospf 10 vrf cli1
redistribute bgp
!
area 0
interface l3-VRF-CLI1-VLAN10
network-type point-to-point
!!
!
!commit
```

```
!Equipment B
config
router bgp 1000
vrf cli1
address-family ipv4 unicast
redistribute ospf
!
exit-address-family
!!
!
router ospf 10 vrf cli1
redistribute bgp
!
area 0
interface l3-VRF-CLI1-VLAN30
network-type point-to-point
!!
!
!commit
```

```
!Equipment C
config
router bgp 1000
vrf cli1
address-family ipv4 unicast
redistribute ospf
!
exit-address-family
!!
!
router ospf 10 vrf cli1
```

```
redistribute bgp
!
area 0
interface l3-VRF-CLI1-VLAN20
network-type point-to-point
!
!
!
commit
```



Os comandos disponíveis para a realização do Troubleshooting podem ser encontrados no tópico [Verificando L3VPNs](#).

11.7.7 Verificando L3VPNs

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



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

```
show mpls l3vpn vpv4 vrf <vrf-name> brief
show ip bgp vpv4 labels
show ip ospf neighbor brief
show ip route vrf <vrn-name>
show ip fib vrf <vrf-name> brief
show ip interface vrf <vrf-name> brief
```

12 Multicast

Este capítulo descreve a configuração dos protocolos multicast. Ele contém as seguintes seções:

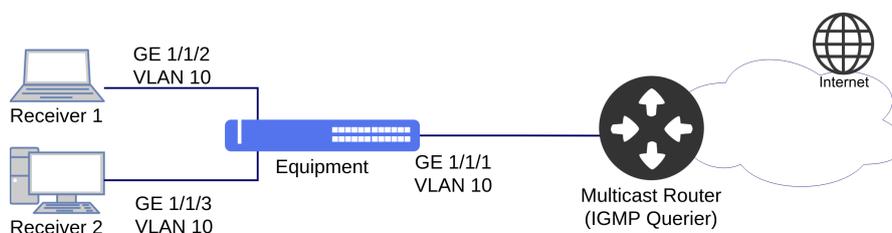
- Configuração do IGMP Snooping

12.1 Configuração do IGMP Snooping

O protocolo IGMP Snooping (Internet Group Management Protocol) analisa os pacotes do protocolo IGMP dentro de uma VLAN a fim de descobrir quais interfaces possuem interesse em receber o tráfego multicast. Utilizando as informações aprendidas pelo protocolo, o IGMP Snooping reduz o consumo de largura de banda em uma LAN, evitando o envio do tráfego multicast por flood para dispositivos que não queiram receber fluxos multicast.

12.1.1 Configurando o IGMP Snooping em Aplicações Ethernet

O cenário abaixo será usado para descrever uma aplicação multicast com IGMP Snooping.



Implementação do IGMP Snooping



O IGMP Querier não é suportado no DmOS.



No DmOS, a versão do IGMP Snooping deve ser igual a versão configurada no IGMP Querier.

Os próximos passos irão demonstrar como configurar o IGMP Snooping versão 2 na **VLAN 10** para inspecionar tráfego multicast na interface de uplink gigabit 1/1/1 e nas interfaces de acesso gigabit 1/1/2 e gigabit 1/1/3 onde estão conectados os receivers 1 e 2 respectivamente.



Caso não seja especificado a versão do IGMP em uma interface, por default é configurado a versão 3 do IGMP Snooping.

```

config
dot1q
vlan 10
interface gigabit-ethernet-1/1/1 tagged
interface gigabit-ethernet-1/1/2 untagged
interface gigabit-ethernet-1/1/3 untagged
!
!
switchport
interface gigabit-ethernet-1/1/2
native-vlan
vlan-id 10
!
interface gigabit-ethernet-1/1/3
native-vlan
vlan-id 10
!
!
multicast igmp snooping 1
bridge-domain id 10
interface gigabit-ethernet-1/1/1 version 2
interface gigabit-ethernet-1/1/2 version 2
interface gigabit-ethernet-1/1/3 version 2
commit

```



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

12.1.2 Configurando o IGMP Snooping em Aplicações GPON

O cenário abaixo será usado para descrever uma aplicação multicast com IGMP Snooping em cenário GPON.



Implementação do IGMP Snooping em cenário GPON



É necessário configurar algum serviço GPON antes de aplicar as configurações a seguir. Também é possível realizar a configuração utilizando uma interface Ethernet como interface de acesso ao invés de uma service-port da interface GPON.

Os próximos passos irão demonstrar como configurar o IGMP Snooping na **VLAN 3000** para inspecionar o tráfego multicast na interface gigabit 1/1/1 e na ONU 1 que está configurada na service-port 1.

```

config
dot1q
vlan 3000
interface gigabit-ethernet-1/1/1 tagged
interface service-port-1

```

```
!  
!  
multicast igmp snooping 1  
  bridge-domain id 3000  
  interface gigabit-ethernet-1/1/1  
  interface service-port 1  
commit
```



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

12.1.3 Verificando o IGMP

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



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

```
show multicast igmp snooping groups  
show multicast igmp snooping groups brief  
show multicast igmp snooping groups detail  
show multicast igmp snooping groups extensive  
show multicast igmp snooping mrouter  
show multicast igmp snooping statistics
```

13 QoS

O QoS (Quality of Service) é um conjunto de mecanismos e algoritmos utilizados para classificar e organizar o tráfego na rede. O objetivo principal é garantir que serviços que necessitem qualidade de transmissão na rede (latência, jitter e largura de banda), por exemplo: VoIP ou multicast funcionem adequadamente.

Este capítulo contém as seguintes seções:

- Configuração do Controle de Congestionamento
- Configuração do Traffic Shapping
- Configuração do Traffic Policing



Nos cenários MPLS, os fluxos dos clientes com VLAN possuem automaticamente o PCP copiado para o campo EXP dos labels, atuando conforme a configuração das filas do scheduler, rate-limit ou do policer.

13.1 Configuração do Controle de Congestionamento

13.1.1 Configurando o escalonador WFQ

O WFQ (Weighted Fair Queuing) é um escalonador que permite definir pesos para as filas proporcionando uma banda para cada uma em condições de congestionamento. A fila quando configurada como SP consumirá toda a banda disponível e somente o excedente será dividido entre as demais filas com o cálculo baseado nos pesos de cada uma.

Os próximos passos irão demonstrar como configurar o WFQ na interface gigabit 1/1/1 com as seguintes especificações:

- **Fila 0:** peso 5
- **Fila 1 e 2:** peso 10
- **Fila 3 e 4:** peso 15
- **Fila 5:** peso 20
- **Fila 6:** peso 25
- **Fila 7:** SP (Strict Priority)

```
config
qos scheduler-profile WFQ-Profile-1
mode wfq
queue 0 weight 5
queue 1 weight 10
queue 2 weight 10
queue 3 weight 15
queue 4 weight 15
queue 5 weight 20
queue 6 weight 25
queue 7 weight SP
!
qos interface gigabit-ethernet-1/1/1 scheduler-profile WFQ-Profile-1
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

13.2 Configuração do Traffic Shapping

O Traffic Shapping ajusta a taxa do tráfego utilizado um buffer no qual são enfileirados pacotes quando o fluxo está acima da banda permitida, o que pode introduzir um maior delay no fluxo.

13.2.1 Configurando o Rate Limit na Interface

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 o burst em KB.

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 100 Mbps (100000 kbps) com burst de 2 MB (2000 kB) na interface gigabit 1/1/1.

```
config
qos interface gigabit-ethernet-1/1/1
  rate-limit
    ingress
      bandwidth 30000
      burst 2000
    egress
      bandwidth 100000
      burst 2000
  commit
```



Não há comandos de troubleshooting para esta funcionalidade.

13.3 Configuração do Traffic Policing

Policer é uma das funcionalidades que permitem o controle do tráfego utilizado sobre uma banda disponível, mas finita. É um mecanismo de classificação e controle de fluxos de acordo com os níveis de serviços desejados. O Policer classifica os fluxos em cores (verde, amarelo e vermelho) dependendo do modo do policer configurado com suas respectivas taxas e bursts possibilitando tomar ações diferentes conforme a classificação realizada.



Os parâmetros relacionados ao burst utilizam a unidade **bytes** e os relacionados a taxa **kbits/s**.



O policer suporta os modos flow, srTCM (RFC 2697), trTCM (RFC 2698) e Differentiated Service trTCM (RFC 4115). Dependendo da plataforma utilizada pode ser que alguns modos não sejam suportados.



É possível realizar o Traffic Policer baseado em interface, VLAN, inner-VLAN, PCP, inner-PCP e DSCP.

13.3.1 Configurando o Traffic Policing baseado em VLANs

Os próximos passos irão demonstrar como configurar o Traffic Policer limitando a banda do cliente que utiliza a **VLAN 10** com **download de 15 Mbps** (15000 kbits/s) e **upload de 5 Mbps** (5000 kbits/s) utilizando **burst de 1 MB** (1000000 bytes) realizando o descarte do tráfego excedente.

```
config
qos policer
profile download
mode flow
parameters
cir 15000
cbs 1000000
!
stage egress
actions
red drop
!
!
profile upload
mode flow
parameters
cir 5000
cbs 1000000
!
stage ingress
actions
red drop
!
!
instance 1
interface ten-gigabit-ethernet-1/1/3
profile download
vlan 10
!
instance 2
interface ten-gigabit-ethernet-1/1/3
profile upload
vlan 10
!
commit
```

Caso o cliente utilize as **VLANs 10 e 20** é possível configurar uma lista de VLANs utilizando o comando a seguir:

```
config
qos policer
instance 1
vlan 10,20
!
instance 2
```

```
vlan 10,20
!
commit
```



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

13.3.2 Configurando o Traffic Policing baseado na inner VLAN

Os próximos passos irão demonstrar como configurar o Traffic Policer limitando a banda dos clientes ou serviços associados a diferentes *inner-vlans* em uma service VLAN.

O Policer configurado atua no tráfego das **inner VLANs 300 até 500** na **service vlan 10** com **download de 150 Mbps** (150000 kbits/s) e **upload de 50 Mbps** (50000 kbits/s) utilizando **burst de 1 MB** (1000000 bytes) realizando o descarte do tráfego excedente.

A interface de acesso é a `ten-gigabit-ethernet-1/1/3` e a interface de uplink é a `ten-gigabit-ethernet-1/1/5`.

```
config
qos policer
profile download
mode flow
parameters
  cir 150000
  cbs 1000000
!
stage ingress
actions
  red drop
!
!
profile upload
mode flow
parameters
  cir 50000
  cbs 1000000
!
stage ingress
actions
  red drop
!
!
instance 1
interface ten-gigabit-ethernet-1/1/5
name uplink-interface
profile download
inner-vlan 300-500
vlan 10
!
instance 2
interface ten-gigabit-ethernet-1/1/3
name access-interface
profile upload
inner-vlan 300-500
vlan 10
!
commit
```



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

13.3.3 Configurando o Traffic Policing baseado no PCP

Os próximos passos irão demonstrar como configurar o Traffic Policer limitando a banda do cliente que utiliza o **PCP 5** para **download de 15 Mbps** (15000 kbits/s) e **upload de 5 Mbps** (5000 kbits/s) utilizando **burst de 1 MB** (1000000 bytes) realizando o descarte do tráfego excedente.

```
config
qos policer
profile download
mode flow
parameters
  cir 15000
  cbs 1000000
!
stage egress
actions
  red drop
!
profile upload
mode flow
parameters
  cir 5000
  cbs 1000000
!
stage ingress
actions
  red drop
!
instance 1
interface ten-gigabit-ethernet-1/1/3
profile download
pcp 5
!
instance 2
interface ten-gigabit-ethernet-1/1/3
profile upload
pcp 5
!
commit
```



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

13.3.4 Configurando o Traffic Policing baseado no DSCP

Os próximos passos irão demonstrar como configurar o Traffic Policer limitando a banda do cliente que utiliza o **DSCP cs1** para **download de 15 Mbps** (15000 kbits/s) e **upload de 5 Mbps** (5000 kbits/s) utilizando **burst de 1 MB** (1000000 bytes) realizando o descarte do tráfego excedente.

A interface de acesso é a ten-gigabit-ethernet-1/1/3 e a interface de uplink é a ten-gigabit-ethernet-1/1/5.

```
config
qos policer
profile download
mode flow
parameters
  cir 15000
  cbs 1000000
!
stage ingress
actions
  red drop
!
profile upload
mode flow
```

```
parameters
  cir 5000
  cbs 1000000
!
stage ingress
actions
  red drop
!
instance 1
interface ten-gigabit-ethernet-1/1/5
profile download
dscp cs1
!
instance 2
interface ten-gigabit-ethernet-1/1/3
profile upload
dscp cs1
!
commit
```



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

13.3.5 Verificando QoS policers

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



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



Para visualizar os contadores de QoS policers, é necessário configurar **counters enabled** nas instâncias dos policers.

```
show qos policer
show qos policer resources
```

14 Segurança

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 no DmOS. Ele contém as seguintes seções:

- Configuração do Storm Control
- Configuração de ACLs
- Configuração do Anti IP Spoofing
- Configuração do MAC Limit
- Configuração do CPU DoS Protect

14.1 Configuração do Storm Control

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



O valor especificado para controle do tráfego é uma porcentagem da velocidade nominal da interface que pode ser especificado de 0 a 100 com passos de 0,01.



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

14.1.1 Configurando o Storm Control

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

```
config
switchport
interface gigabit-ethernet-1/1/1
 storm-control
  broadcast 95
  multicast 70
  unicast 5
commit
```



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

14.1.2 Verificando o Storm Control

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



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

```
show interface utilization
show interface <interface> statistics
```

14.2 Configuração de ACLs

ACLs (Access Control Lists) são listas de controle de acesso que tem como objetivo permitir ou negar pacotes, de forma proteger o equipamento contra ataques ou impedir acessos indevidos a recursos na rede.

O DmOS suporta ACLs de entrada (ingress) e também ACLs específicas para tráfegos com destino ao CPU do equipamento, sendo possível negar (deny), permitir (permit) ou alterar (set) propriedades dos pacotes.



Cada plataforma de hardware suporta um valor máximo de regras ACLs. Consulte o **Descritivo do DmOS** para verificar os valores máximos.

- Filtros L2: Destination and Source MAC, Ethertype, PCP, Inner-PCP, VLAN e Inner-VLAN.
- Filtros L3: Filtros L2, Destination and Source IPv4, TCP/UDP Destination Port, DSCP, IP Protocol e ToS.

14.2.1 Configurando uma ACL L2 para negar o tráfego de uma VLAN

Os próximos passos irão demonstrar como configurar uma ACL L2 com prioridade 0 na interface gigabit 1/1/1 negando o tráfego da VLAN 20 nesta interface.

```
config
access-list
acl-profile ingress l2 ACL-L2 priority 0
access-list-entry 0 match vlan 20
action deny
!
!
!
access-list interface gigabit-ethernet-1/1/1 ingress ACL-L2
```



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

14.2.2 Configurando uma ACL L3 para negar o tráfego de um endereço IPv4

Os próximos passos irão demonstrar como configurar uma ACL L3 com prioridade 256 na interface gigabit 1/1/1 negando o tráfego com endereço de origem 192.168.5.10 nesta interface.

```
config
access-list
acl-profile ingress l3 ACL-L3 priority 256
  access-list-entry 0 match source-ipv4-address 192.168.5.10
  action deny
!
access-list interface gigabit-ethernet-1/1/1 ingress ACL-L3
commit
```



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

14.2.3 Configurando uma ACL para proteção do CPU

Pacotes com destino a interfaces configuradas no equipamento, tanto interfaces l3 como loopbacks, são encaminhados para processamento no CPU, o que pode levar a alto processamento, afetando protocolos, ou, também, levando a vulnerabilidades de segurança no equipamento. Por estes motivos, é recomendada a utilização de ACLs para proteção do CPU (control plane), permitindo estritamente os pacotes necessários para troubleshooting (ex. ICMP, SNMP), gerência (ex. SSH) e para estabelecimento de protocolos.

No exemplo abaixo, é configurada uma ACL para proteção do CPU com os seguintes critérios:

- Permite pacotes ARP
- Permite pacotes ICMP IPv4
- Permite pacotes ICMP IPv6
- Permite acesso via SSH somente para pacotes com origem na rede 10.0.0.0/8
- Permite pacotes OSPF (protocolo IP 89)
- Permite pacotes BGP (porta 179)
- Permite pacotes LDP (porta 646)
- Permite Slow Protocols - LACP, EFM, etc (ethertype 0x8809)
- Permite STP (ethertype 0x4242)
- Bloqueia o restante

A ACL foi configurada com o nome **control-plane-protection** e foi aplicada através da configuração **access-list protection cpu control-plane-protection**.



Mesmo sendo liberadas as portas necessárias, é importante que sejam permitidos também pacotes ARP e ICMP IPv6, como nas entradas 10 e 30 da configuração a seguir. Estes protocolos são necessários para que exista conectividade com os vizinhos.

```
config
access-list
protection
  cpu control-plane-protection
!
acl-profile cpu l3 control-plane-protection
  priority 0
  access-list-entry 10
    match ethertype arp
    action permit
  !
  access-list-entry 20
    match ip-protocol icmp
    action permit
  !
  access-list-entry 30
    match ip-protocol ipv6-icmp
    action permit
  !
  access-list-entry 40
    match source-ipv4-address 10.0.0.0/8
    match destination-port ssh
    action permit
  !
  access-list-entry 50
    match ip-protocol 89
    action permit
  !
  access-list-entry 60
    match destination-port 179
    action permit
  !
  access-list-entry 61
    match source-port 179
    action permit
  !
  access-list-entry 70
    match destination-port 646
    action permit
  !
  access-list-entry 71
    match source-port 646
    action permit
  !
  access-list-entry 80
    match ethertype 0x8809
    action permit
  !
  access-list-entry 90
    match ethertype 0x4242
    action permit
  !
  access-list-entry 100
    action deny
  !
!
commit
```



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

14.2.4 Configurando uma ACL para pacotes com origem no CPU

Pacotes originados no CPU, como exemplo CFM, L3, TWAMP, MPLS, podem passar por regras de ACLs antes de serem encaminhados. Essas regras podem alterar algum campo do pacote ou até mesmo restringí-lo.



Não atua em pacotes encaminhados direto para interfaces. Exemplo de protocolos L2: EAPS/ERPS/xSTP/-LACP/OAM.

No exemplo abaixo é configurada uma ACL para alterar a prioridade (PCP) dos pacotes TWAMP que são enviados pela CPU: A ACL foi configurada com o nome **originated-cpu** e foi aplicada a prioridade 5 (set pcp 5) nos pacotes com destino a porta 9999 do TWAMP reflector.



O TWAMP deve estar configurado com a porta 9999.

```
config
access-list
interface cpu-port-1/1/1 ingress originated-cpu
!
acl-profile ingress l3 originated-cpu
priority 256
access-list-entry 0
match destination-port 9999
action set pcp 5
!
!
!
commit
```



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

14.2.5 Verificando as ACLs

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



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

```
show acl-resources
show acl-resources brief
show acl-resources detail
show acl-resources extensive
```

14.3 Configuração do Anti IP Spoofing

A funcionalidade anti-ip-spoofing é a técnica que consiste em proteger as interfaces do spoofing nos pacotes, evitando ataques do tipo SYN flood, routing redirect entre outros.

É possível configurar regras para permitir o tráfego de um endereço IP específico, todos os endereços IPv4, todos os endereços IPv6 ou todos os endereços IPv4 e IPv6.



Este recurso de segurança está disponível apenas nas plataformas OLT com suporte a tecnologia GPON.



Para as service-port que utilizam DHCP ou PPPoE como autenticação dos clientes GPON, os endereços IP serão automaticamente liberados, não necessitando desta configuração.



Não é possível desativar regras nas interfaces GPON. As regras podem ser aplicadas em interfaces Ethernet ou em Service-ports do GPON.

14.3.1 Configurando Anti IP Spoofing para endereço IPv4 e MAC específico

Os próximos passos irão demonstrar como configurar o anti-ip-spoofing na interface gigabit 1/1/3 liberando o tráfego IP para o endereço 1.1.1.1 na service-port 2 com o MAC 00:AA:10:20:30:41.

```
config
anti-ip-spoofing
interface service-port-2
allowed-ip ipv4 1.1.1.1 vlan 10 mac 00:AA:10:20:30:41
```



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

14.3.2 Configurando Anti IP Spoofing para endereço IPv4 específico

Os próximos passos irão demonstrar como configurar o anti-ip-spoofing na service-port-2 liberando apenas o tráfego IP para o endereço IPv4 192.10.20.1.

```
config
anti-ip-spoofing
interface service-port-2
allowed-ip ipv4 address 192.10.20.1
```



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

14.3.3 Configurando Anti IP Spoofing para todos endereços IPv6

Os próximos passos irão demonstrar como configurar o anti-ip-spoofing na service-port-2 liberando apenas o tráfego IP para todos os endereços IPv6.

```
config
anti-ip-spoofing
interface service-port-2
  allowed-ip ipv6-all
commit
```



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

14.3.4 Configurando Anti IP Spoofing para todos endereços IPv4 e IPv6

Os próximos passos irão demonstrar como configurar o anti-ip-spoofing na service-port-2 liberando o tráfego IP para todos os endereços IPv4 e IPv6.

```
config
anti-ip-spoofing
interface service-port-2
  allowed-ip all
```



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

14.3.5 Verificando o Anti IP Spoofing

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



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

```
show allowed-ip
show allowed-ip address <IP address>
show allowed-ip entry-type type
show allowed-ip mac <MAC>
show allowed-ip status status
show allowed-ip vlan <VLAN-ID>
```

14.4 Configuração do MAC Limit

O MAC limit é a quantidade de endereços MAC que uma interface ethernet pode aprender. É possível configurar o MAC Limit nas interfaces e nas VLANs.

14.4.1 Configurando o MAC Limit na Interface

Os próximos passos irão demonstrar como configurar o MAC limit para o valor de 100 endereços MACs na interface gigabit 1/1/3.

```
config
mac-address-table
interface gigabit-ethernet-1/1/3
  limit maximum 100
```



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

14.4.2 Configurando o MAC Limit na VLAN

Os próximos passos irão demonstrar como configurar o MAC limit para o valor de 20 endereços MACs na interface VLAN 3000.

```
config
mac-address-table
vlan 3000
  limit maximum 20
commit
```



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

14.4.3 Verificando o MAC Limit

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



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

```
show mac-address-table interface <interface>
show mac-address-table interface <interface> | lnum | begin 3 | count
show mac-address-table vlan <vlan>
show mac-address-table vlan <vlan> | lnum | begin 3 | count
```

14.5 Configuração do CPU DoS Protect

É importante controlar o número de pacotes enviados para a CPU visando garantir a qualidade, a disponibilidade dos serviços e evitar ataques que possam ocasionar a perda da gerência ou uma mudança de estado equivocada de um protocolo.

O DmOS permite ao usuário controlar o número máximo de pacotes enviados por segundo (pps) para a CPU do equipamento através de configuração global ou por protocolo.



A configuração do número de pacotes no CPU DoS Protect deve ser planejada de acordo com a rede. Configurar um valor muito baixo pode ocasionar mau funcionamento em algum protocolo, assim como configurar um valor muito alto pode deixar o equipamento suscetível a ataques direcionados a CPU.



Na plataforma DM4770 o valor default do CPU DoS Protect é 3000 pps, nas demais plataformas o valor default é 900 pps.

14.5.1 Configurando o CPU DoS Protect Global

Os próximos passos irão demonstrar como configurar o CPU DoS Protect para limitar o número máximo de pacotes que a CPU deve aceitar em 1000 pacotes por segundo (pps).

```
config
cpu-dos-protect global
max-pps 1000
commit
```



Não há comandos de troubleshooting para esta funcionalidade.

14.5.2 Configurando o CPU DoS Protect por Protocolo

É possível configurar o número máximo de pacotes para diversos protocolos, como **ARP, LLDP, PPPoE, VRRP**, entre outros.

Os próximos passos irão demonstrar como atualizar o número máximo de pacotes por segundo que a CPU pode aceitar para os protocolos ARP e PPPoE. Os pacotes excedentes de cada fila serão descartados.

```
config
cpu-dos-protect protocols arp max-pps 90
cpu-dos-protect protocols pppoe max-pps 800
commit
```



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

14.5.3 Verificando o CPU DoS Protect

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



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

```
show cpu-dos-protect protocols
```

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**