DATACOM

DmOS

DATACOM OPERATING SYSTEM

GUIA DE CONFIGURAÇÃO RÁPIDA

204.0309.09 – abril/2019

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.

© 2018 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 www.datacom.com.br.

Para contato telefônico: +55 51 3933-3094

CONTATOS

SUPORTE TÉCNICO

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

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

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

Para contato telefônico: +55 51 3933-3122

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

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

INFORMAÇÕES GERAIS

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

DATACOM

Rua América, 1000

92990-000 – Eldorado do Sul – RS – Brasil

+55 51 3933-3000

DOCUMENTAÇÕES DE PRODUTO

- Sobre este Documento

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 (QUICK CONFIGURATION GUIDE) –** Fornece orientações sobre como configurar as funcionalidades de forma rápida no equipamento
- **GUIA DE SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING GUIDE) –** Fornece orientações sobre como analisar, identificar e resolver problemas com o produto (apenas em inglês)
- **REFERÊNCIA DE COMANDOS (COMMAND REFERENCE) -** 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 (DATASHEET) -** Fornece as características técnicas do produto
- **GUIA DE INSTALAÇÃO (INSTALLATION GUIDE) –** Fornece orientações sobre os procedimentos para instalação do produto

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

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

ÍNDICE

1 INTRODUÇÃO AO DOCUMENTO

1.1 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.

1.2 PÚBLICO-ALVO

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

1.3 CONVENÇÕES

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

1.3.1 Ícones

Ícone	Tipo	Descrição
	Nota	As notas explicam melhor algum detalhe apresentado no texto.
	Advertência	Esta formatação indica que o texto aqui contido tem grande importância e há risco de danos.
	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.

	Advertência	Indica equipamento ou parte sensível à eletricidade estática. Não deve ser manuseado sem cuidados como pulseira de aterramento ou equivalente.
	Advertência	Indica emissão de radiação não ionizante.
	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.

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.

1.3.2 Usando a CLI

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

```
# comando [Enter]
```

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

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

2 INICIANDO

2.1 INSTALANDO E ENERGIZANDO O EQUIPAMENTO

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

2.2 CONECTANDO VIA PORTA CONSOLE

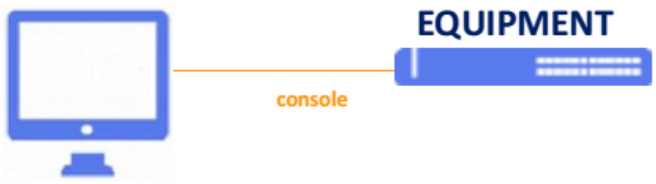

Figura 1 – Conectando via porta console

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**.

2.3 CONECTANDO VIA PORTA DE GERÊNCIA OUT-OF-BAND

Figura 2 – 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.

2.4 CONECTANDO PELA PRIMEIRA VEZ NO EQUIPAMENTO

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

```
login as: admin
Password: admin
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.

3 ATUALIZAÇÃO DE FIRMWARE

O DmOS possui posições de memória flash para armazenamento de firmware e salva automaticamente a nova versão de firmware na posição não utilizada.

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

3.1 ATUALIZAÇÃO DO SOFTWARE DMOS

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

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

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

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

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

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

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

O firmware enviado estará na posição Inactive. É possível verificar o novo firmware copiado através do seguinte comando:

```
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: In case of performing a firmware downgrade, please load the factory-
config before the activation.
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/Startup usando novamente o comando:

```
show firmware
```

3.2 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.

3.2.1 Realizando o download do firmware

Para baixar o 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.

3.2.2 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.

3.2.3 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**.

4 GERENCIAMENTO DA CONFIGURAÇÃO

O equipamento pode ser gerenciado através da **CLI** com o uso da porta console do equipamento e 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.

4.1 MODO OPERACIONAL

Ao realizar o login no equipamento o usuário automaticamente entrará no mode 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
```

4.2 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.

4.2.1 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
```

4.2.2 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
```

4.3 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 do candidato 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
```

4.4 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
```

4.5 RESTAURANDO CONFIGURAÇÃO

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

```
rollback configuration
```

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

```
rollback configuration file-name
```

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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

4.6 SALVANDO A CONFIGURAÇÃO EM ARQUIVO

O usuário pode salvar a configuração candidata em um arquivo (incluindo as configurações padrão) sem aplica-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*).

4.7 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
```

4.8 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
```

4.9 CONFIGURAÇÃO A PARTIR DE ARQUIVOS

É possível mesclar a configuração candidata com um arquivo salvo. 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
```

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

```
load override file-name
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

4.10 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.

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

4.11 CRIANDO UM ALIAS

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

Suponha que o usuário frequentemente execute uma sequencia 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"
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

O comando alias não permite auto-complete.

5 GERENCIAMENTO DO EQUIPAMENTO

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

• CLI (*Command-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

5.1 CONFIGURANDO SENHAS NO DMOS

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.

5.2 CONFIGURANDO A GERÊNCIA OUT-OF-BAND

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

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

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.

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

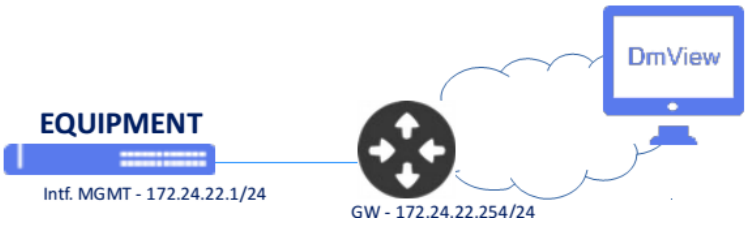

Figura 3–Exemplo de Gerenciamento Out-Of-Band

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:

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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

5.3 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.

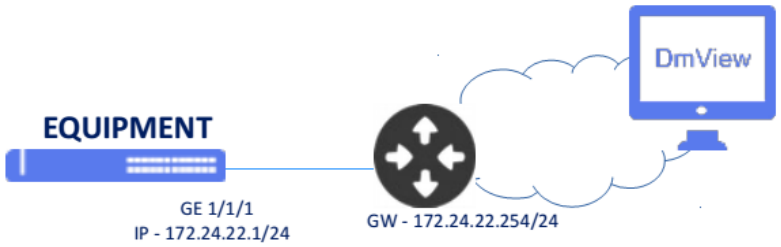

Figura 4–Exemplo de Gerenciamento In-Band

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:

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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

5.4 CONFIGURANDO O HOSTNAME

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

Configuração

```
config
hostname DATACOM-ROUTER-R1
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

5.5 CONFIGURANDO O BANNER

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

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

Configuração

```
config
banner login "\nAcesso restrito\n"
```

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

Também é possível configurá-lo em múltiplas linhas.

Configuração

```
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
Proibido\n):
[Multiline mode, exit with ctrl-D.]
>
> Acesso restrito
>
> <CTRL-D>
```

Troubleshooting

```
show banner login
```

5.6 CONFIGURANDO O RELÓGIO E DATA DO SISTEMA

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

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

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:

Configuração

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

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

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show system clock
```

5.7 CONFIGURANDO O SNTP

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

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

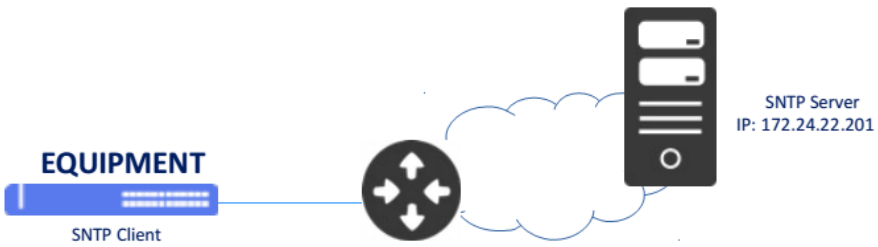

Figura 5–Exemplo de configuração SNTP

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:

Configuração

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

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

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show sntp
```

5.8 CONFIGURANDO O SYSLOG REMOTO

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

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

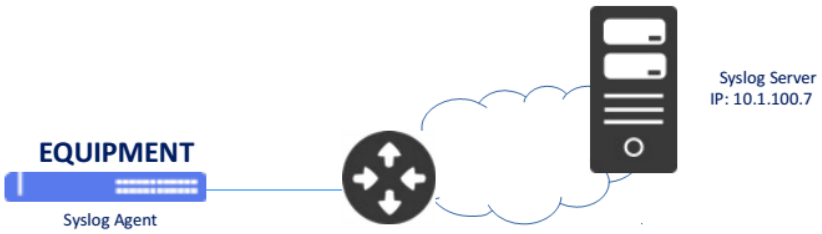

Figura 6 – Exemplo de configuração do Syslog Remoto

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:

Configuração

```
config
log syslog 10.1.100.7
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting
`show log`

5.9 CONFIGURANDO O SNMP

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

Versão	Descrição
SNMP v1	Versão original do SNMP, strings das comunidades enviadas em texto simples com segurança fraca.
SNMP v2c	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.
SNMP v3	Versão mais recente do SNMP, suportando segurança e autenticação SHA e MD5 completas. Deve ser usado, se possível, especialmente em redes não confiáveis.

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

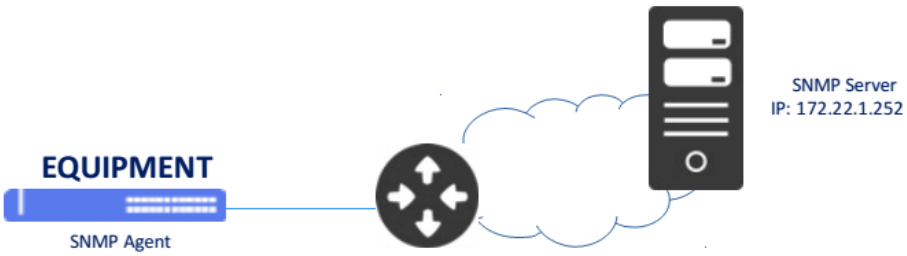

Figura 7–Exemplo de configuração SNMP

Para conectar o equipamento a um servidor SNMPv2 que está na comunidade public com endereço IPv4 172.22.1.152, proceda da seguinte forma:

Configuração

```
config
snmp agent enabled
snmp agent version v2c
snmp community public
 sec-name public
snmp target SNMP-Trap-Server
 ip 172.22.1.252
 v2c sec-name public
snmp notify std_v2_trap
 tag std_v2_trap
!
snmp vacm group public
 member public
  sec-model [ v2c ]
!
access v2c no-auth-no-priv
  read-view root
  write-view root
  notify-view root
!
snmp vacm view root
 subtree 1.3
  included
 !
!
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Para conectar o equipamento a um servidor SNMPv3 que está na grupo VACM-SNMPv3 com usuário dmview e que possui senha autenticação em MD5 igual a dmview123-md5 e senha de privacidade em AES igual a dmview123-aes, proceda da seguinte forma:

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
  notify-view root
 !
!
snmp vacm view root
 subtree 1.3
```

```
   included
  !
!
snmp usm local user dmview
 auth md5 password "dmview123-md5"
 priv aes password "dmview123-aes"
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade.
```

5.10 Ativando a licença MPLS

Uma licença é necessária para a operação do MPLS. Para obte-la entre em contato com o time de Suporte da DATACOM. Para solicitar a licença MPLS será necessário ter o número de série e o MAC do equipamento. Estes podem ser verificados a partir do 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
...
```

Os próximos passos irão demonstrar como ativar a licença MPLS.

Configuração

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show license
```

5.11 Ativando a licença das portas GPON

Uma licença pode ser necessária para utilizar algumas interfaces dos OLTs, para o DM4615 as interfaces de 9 a 16 precisam de licença para operarem. Caso ainda não tenha recebido a licença, entre em contato com o time

de Suporte da DATACOM. Para solicitar a licença GPON será necessário ter o número de série e o MAC do equipamento. Estes podem ser verificados a partir do comando "**show inventory**" conforme abaixo:

```
show inventory
...
  Chassis/Slot       : 1/1
   Product model     : 16GPON+4GT+4XS
   Part number       : 800.5198.01
   Serial number     : 4461034
   Product revision  : 0
   PCB revision      : 0
   Hardware version  : 0
   Manufacture date  : 05/08/2018
   Manufacture hour  : 12:00:00
   Operat. temp.     : 0 - 65 Celsius degrees
   Base MAC address  : 00:04:df:5c:0c:77
...
```

Os próximos passos irão demonstrar como ativar a licença GPON.

Configuração

```
config
license gpon-16-ports enabled key
(<string>): **********************
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show license
```

6 FERRAMENTAS DE CONECTIVIDADE

O DmOS fornece algumas ferramentas para executar a verificação da conectividade de rede bem como acessar equipamentos a partir do próprio DmOS.

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

6.1 PING E PING6

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

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

```
ping 5.178.41.1

PING 5.178.41.1 (5.178.41.1) 56(84) bytes of data.
64 bytes from 5.178.41.1: icmp_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
```

6.2 TRACEROUTE E TRACEROUTE6

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

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

```
traceroute 5.178.41.1
```

```
traceroute to 5.178.41.1 (5.178.41.1), 30 hops max, 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
```

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
```

6.3 SSH CLIENT E TELNET CLIENT

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

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

```
ssh admin@192.168.1.254
```

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

```
telnet 192.168.1.254
```

7 OAM – OPERAÇÃO, ADMINISTRAÇÃO E MANUTENÇÃO

Este capítulo exibe um grupo de funcionalides de gerenciamento de rede que fornecem indicação de falha de rede, localização de falhas, informações de desempenho e funções de dados e diagnóstico.

7.1 CONFIGURANDO CFM

O protocolo **CFM** (*Connectivity Fault Management*) é definido pelo 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.

Atualmente, o DmOS suporta no protocolo **CFM** apenas o envio e recebimento dos CCMs (*Continuity Check Message*).

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

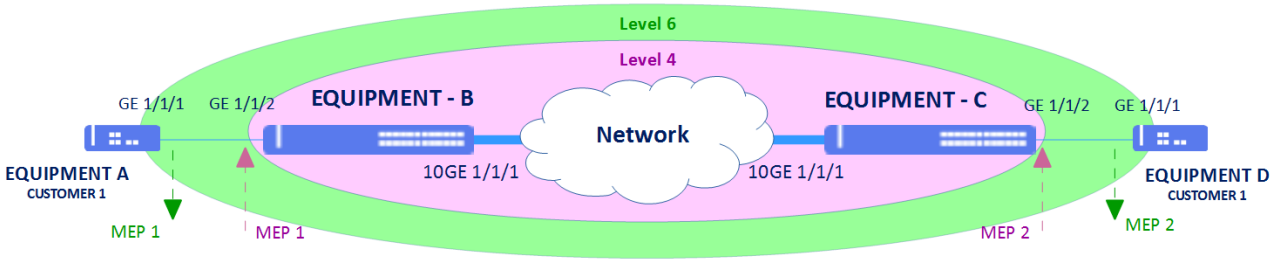

Figura 8 – Exemplo de cenário com CFM

A seguir, são exemplificadas 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.

EQUIPMENT – A:

Configuração

```
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
```

EQUIPMENT – B:

Configuração

```
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
```

EQUIPMENT - C:

Configuração

```
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
```

EQUIPMENT - D:

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

7.1.1 Configuration o action block

O CFM suporta a configuração de bloqueio das interfaces quando os meps estão com status down. Quando as interfaces estão no estado de bloqueio, os outros protocolos 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.

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

O cenário abaixo será usado para demonstrar a configuração do MEP com action block.

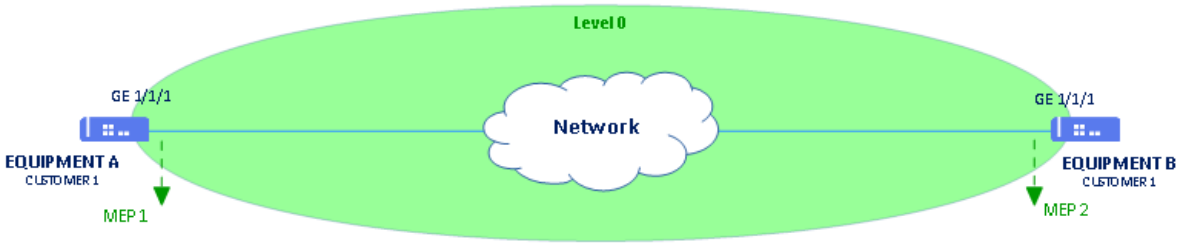

Figura 9 – Cenário com CFM action block

EQUIPMENT – A:

Configuração

```
config
dot1q
 vlan 2000
  interface gigabit-ethernet-1/1/1 tagged
  !
 !
!
oam
 cfm
  md Client
   level 0
   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
      fault-action block-port
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 2000
  interface gigabit-ethernet-1/1/1 tagged
  !
 !
!
oam
 cfm
  md Client
   level 0
   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
      fault-action block-port
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show oam cfm
show oam cfm brief
show oam cfm detail
show oam cfm local
show oam cfm remote
show oam cfm statistics
show alarm
```

7.2 CONFIGURANDO TRAFFIC LOOP

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.

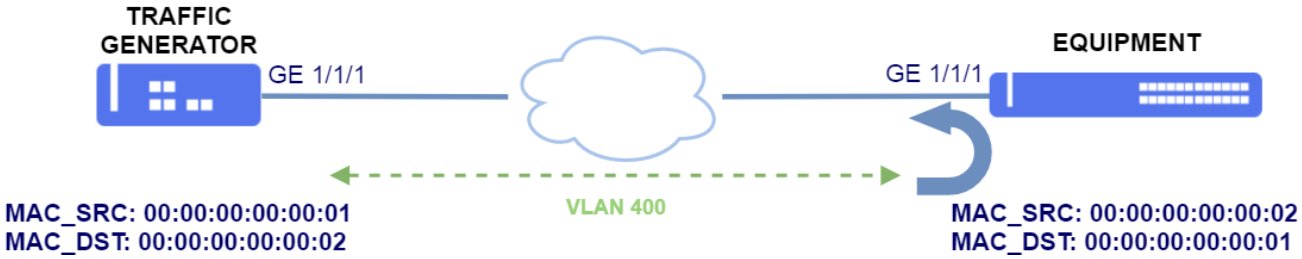

Figura 10 – Cenário com traffic loop

Neste exemplo, será feito um loop do tráfego utilizando a VLAN 100 na interface gigabit-ethernet-1/1/1 como interface de 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.

Configuração

```
config exclusive
dot1q
 vlan 100
  interface gigabit-ethernet-1/1/1
!
traffic-loop 1
 interface gigabit-ethernet-1/1/1
 source-mac-address 00:00:00:00:00:02
 destination-mac-address 00:00:00:00:00:01
 vlan 100
!
```

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. Para que não seja feito *rollback* da configuração após o *commit confirmed*, dar um novo *commit*.

```
commit confirmed 10
```

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

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade
```

7.3 CONFIGURANDO 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 5337.

A arquitetura da solução de servidor do TWAMP possui os seguintes componentes lógicos:

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

A arquitetura da solução de cliente do TWAMP possui os seguintes componentes lógicos:

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

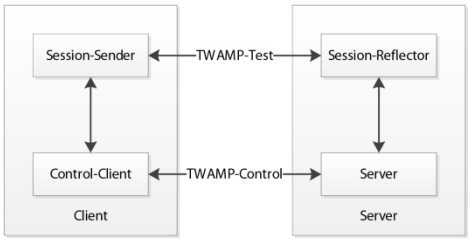

Figura 1 – Arquitetura do TWAMP

Somente o TWAMP Reflector é suportado no DmOS.

Configuração

```
config
oam twamp reflector
```

Por padrão, o TWAMP executa na porta 862, porém esta pode ser alterada.

Configuração

```
config
oam twamp reflector port 4000
```

Pode-se também limitar quais clientes podem comunicar-se com o reflector. Na configuração abaixo, apenas os clientes com endereço *IPv4 192.168.80.26* ou endereço *IPv6 2001:c0a8:ff23::1* serão aceitos pelo *reflector*.

Configuração

```
config
oam
 twamp
  reflector
   ipv4
    client-address 192.168.80.26
    !
   !
   ipv6
    client-address 2001:c0a8:ff23::1
    !
   !
  !
 !
!
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
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
debug enable proto-twamp
```

7.4 CONFIGURANDO LLDP

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

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

Configuração

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

Troubleshooting

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

8 AUTENTICAÇÃO DE USUÁRIOS

O DmOS utiliza níveis de provilégios para determinar o quanto de acesso uma conta de usuário terá no equipamento. 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:

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

8.1 Configurando Usuários Locais

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

Configuração

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

Os próximos passos irão demonstrar como deletar o usuário "joao".

Configuração

```
config
 no aaa user joao
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
who
```

8.2 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* (contabilidade) de forma segura, com criptografia do pacote inteiro. Esta criptografia depende de uma chave secreta configurada no equipamento.

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

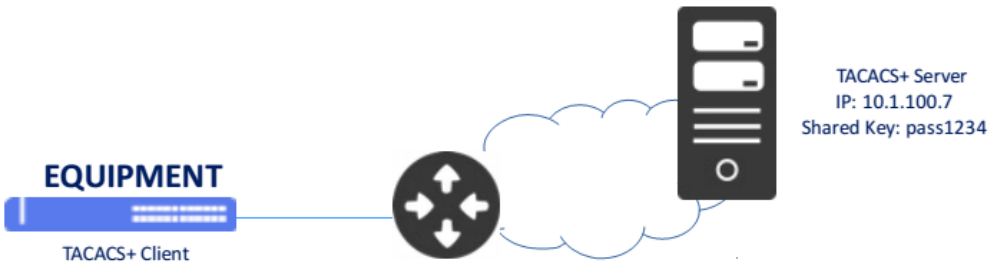

Figura 11 – Exemplo de configuração do servidor TACACS+

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 **10.1.100.7** e senha "**pass1234**", habilitando *autenticação*, *autorização* e *accounting*.

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade.
```

8.3 CONFIGURANDO O RADIUS

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

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

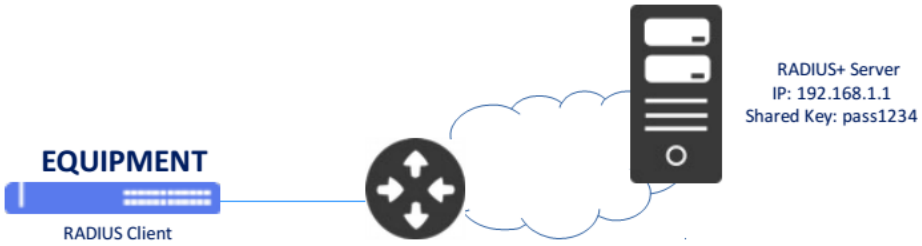

Figura 12 – Exemplo se configuração do servidor RADIUS

Suponha que u 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 e autorização:

Configuração

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade.
```

8.4 CONFIGURANDO A ORDEM DE AUTENTICAÇÃO

O usuário pode definir a ordem de autenticação entre: local, RADIUS e TACACS+. Quando um usuário tentar efetuar login no sistema, o DmOS tentará autenticá-lo seguindo a ordem definida pelo comando da CLI "authentication-order".

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:

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

9 INTERFACES

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

9.1 CONFIGURANDO 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:

Configuração

```
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:

Configuração

```
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:

Configuração

```
config
interface forty-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 ou 40G.

Configuração

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

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.

Configuração

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

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

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação das interfaces ethernet. O usuário deve usar a palavra-chave **"do"** antes do comando caso estiver no modo de configuração. O mesmo procedimento é utilizado caso o usuário queira verificar as interfaces de outras capacidades, como 10G ou 40G.

Troubleshooting

```
show interface gigabit-ethernet chassis/slot/port
```

9.2 Configurando Interfaces 10G para operar em 1G modo não negociado

O DmOS permite a utilização de módulos óticos 1G em interfaces 10G.

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

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação das interfaces ethernet. O usuário deve usar a palavra-chave "do" antes do comando caso estiver no modo de configuração. O mesmo procedimento é utilizado caso o usuário queira verificar as interfaces de outras capacidades, como 10G ou 40G.

Troubleshooting

```
show interface ten-gigabit-ethernet chassis/slot/port
```

A configuração de auto-negociação esta desabilitada por padrão.

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

9.3 CONFIGURANDO MTU EM INTERFACES

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

Configuração

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

O valor padrão de MTU é diferente para cada plataforma.

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

Troubleshooting

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

9.4 CONFIGURANDO TPID EM INTERFACES

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

Configuração

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

```
tpid <tpid>
```

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

PDUs 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 se encaminhado sem *tag* na *VLAN* nativa.

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade
```

9.5 CONFIGURANDO INTERFACES 10G PARA OPERAR EM 1G MODO NEGOCIADO

O DmOS permite a utilização de módulos óticos 1G em interfaces 10G no modo negociado.

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

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação das interfaces ethernet. O usuário deve usar a palavra-chave **"do"** antes do comando caso estiver no modo de configuração. O mesmo procedimento é utilizado caso o usuário queira verificar as interfaces de outras capacidades, como 10G ou 40G.

Troubleshooting

```
show interface ten-gigabit-ethernet chassis/slot/port
```

9.6 Configurando Link-Aggregation (Port-Channel Estático)

A agregação de link **IEEE 802.3ad** permite criar uma interface lógica contendo uma ou mais interfaces físicas. A agregação de vários links ou interfaces físicas cria um único link lógico (LAG) ponto-a-ponto. O LAG possibilita dividir os fluxos entre as interfaces físicas aumentando efetivamente a largura de banda. Outra vantagem da agregação de links é o aumento da disponibilidade do link de comunicação entre os dois equipamentos, se uma das interfaces físicas falhar, o LAG continuará a transportar o tráfego através das interfaces remanescentes.

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

O modo de balanceamento de tráfego no *link-aggregation* suportado pelo DmOS é o **enhanced mode**.

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

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show link-aggregation
show link-aggregation brief
show link-aggregation interfaces
```

9.7 CONFIGURANDO LINK-AGGREGATION (LACP)

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

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

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

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

O modo de balanceamento de tráfego no *link-aggregation* suportado pelo DmOS é o **enhanced mode**.

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.

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
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
```

9.8 CONFIGURANDO UM NÚMERO MÁXIMO DE LINKS ATIVOS NO LINK-AGGREGATION

O DmOS permite configurar o número máximo e mínimo de links ativos no Link-Aggregation. 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.

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

O número máximo de links ativos por padrão é oito (8).

Configuração

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show link-aggregation
show link-aggregation brief
show link-aggregation interfaces
```

9.9 Configurando um número mínimo de links ativos no Link-Aggregation

O DmOS permite configurar o número máximo e mínimo de links ativos no Link-Aggregation. 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.

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

O número mínimo de links ativos por default é um (1).

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show link-aggregation
show link-aggregation brief
show link-aggregation interfaces
```

9.10 Configurando Port Mirroring

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

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

Configuração

```
config
```

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10 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.

10.1 Utilizando as interfaces GPON licenciadas

Uma licença é necessária para a utilização das interfaces licenciadas do OLT. Para mais detalhes de como ativá-la, verifique Ativando a licença das portas GPON..

10.2 Configurando as interfaces 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:

Configuração

```
config
interface gpon 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.

Por padrão, todas as interfaces GPON estão desativadas.

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

Configuração

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

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

Configuração

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

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:

Configuração

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação das interfaces GPON. O usuário deve usar a palavra-chave "do" antes do comando caso estiver no modo de configuração.

Troubleshooting

```
show interface gpon chassis/slot/port
show interface gpon chassis/slot/port brief
```

10.3 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 usuário deve selecionar o método de autenticação entre número de série (*serial-number*), senha (*password-only*) ou misto (*serial-number-and-password*) uma combinação de número de série mais senha.

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

Configuração

```
config
gpon 1/1
```

```
onu-auth-method password
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação das ONUs descobertas mas não autenticadas. O usuário deve usar a palavra-chave **"do"** antes do comando caso estiver no modo de configuração.

Troubleshooting
`show gpon chassis/slot`

10.4 Descobrindo 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.

10.5 Configurando os profiles GPON

Em uma típica rede PON, existem muitos usuários finais, mas poucos tipos de serviços e modelos 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.

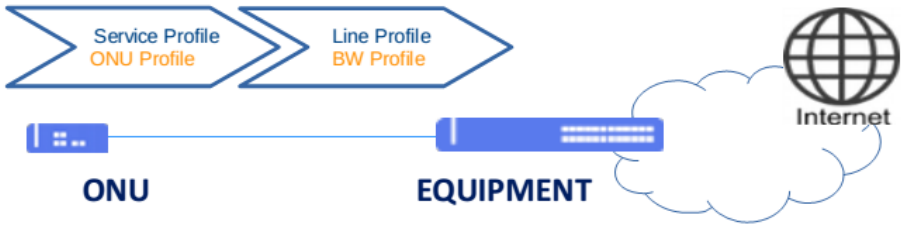

Figura 13–Profiles GPON

10.5.1 ONU Profile

Este perfil descreve os atributos físicos da ONU, como o número de portas Ethernet e POTS. O procedimento abaixo exemplifica a criação de um ONU profile para ser aplicado a ONUs com quatro interfaces Ethernet.

Configuração

```
config
profile gpon onu-profile <ONU_PROFILE_NAME>
 ethernet 4
```

10.5.2 Service Profile

Este perfil define atributos de serviços que serão aplicados a uma ONU como mapeamento de VLAN, CoS e transparência de protocolos L2. Um perfil da ONU deve estar vinculado a um perfil de serviço.

Configuração

```
config
profile gpon service-profile <SERVICE_PROFILE_NAME>
 onu-profile <ONU_PROFILE_NAME>
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.5.3 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				
		Type 1	Type 2	Type 3	Type 4	Type 5
Fixed	Sim	X				X
Assured	Não		X	X		X
Non-Assured	Não			X		X
Best Effort	Não				X	X
Max	Não			X	X	X

Figura 14–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.

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Configuração

```
config
profile gpon line-profile <LINE_PROFILE_NAME>
 tcont 1 bandwidth-profile <BANDWIDTH_PROFILE_NAME>
 gem 1
  tcont 1 priority 5
  map <MAPPING_NAME>
   ethernet 1 vlan 100 cos any
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.5.5 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.

- **Registrar 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.
- **Outbound Proxy:** O proxy de saída recebe a solicitação de um cliente, mesmo que não seja o servidor resolvido pelo URI de solicitação.

Se o usuário deseja definir um perfil do Agente SIP em uma interface POTS, deve usar os seguintes comandos:

Configuração

```
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>
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.5.6 GEM Traffic Agent Profile

Este serviço é usado para aplicar um limite de taxa de *Upstream* e *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 máxima em Kbps que pode passar pela interface, sendo necessariamente maior que o especificado no CIR.

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:

Configuração

```
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>
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.5.7 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.*

As configurações presentes neste perfil podem ser realizadas, alternativamente, através do acesso à interface WEB das ONUs DM984-42x.

É possível configurar três principais tipos conexões: wan-pppoe-connection, wan-ip-connection, wan-bridge-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 procedimento a seguir apresentará como realizar esta configuração:

Configuração

```
config
profile gpon rg-profile PPPoE
 wan-pppoe-connection PPPoE
  vlan-mux vlan 2000 cos 0
  nat
  no fullcone-nat
  no firewall
  no multicast-proxy igmp
  no multicast-source igmp
  auth-type pap
  username pppoemikrotik
  password pppoemikrotik
  service-name internet-pppoe
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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 procedimento a seguir apresentará como realizar esta configuração:

Configuração

```
config
profile gpon rg-profile DHCP
 wan-ip-connection DHCP
  vlan-mux vlan 2100
  nat
  no fullcone-nat
  no firewall
  no multicast-proxy igmp
  no multicast-source igmp
  ipv4 dhcp
  primary-dns 10.0.1.1
  secondary-dns 10.0.1.2
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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:

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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.6 CARREGANDO OS PROFILES DEFAULT

É possível carregar os profiles GPON o quais viabilizam uma rápida configuração nos serviços de GPON. É possível carregar os profiles default apenas para ONUs Bridge, apenas para ONUs Router ou para ambos os tipos de ONUs.

Para carregar os profiles default o usuário deverá realizar o procedimento abaixo:

Configuração

```
config
load default-gpon-profiles
Loading.
Done.
```

Para verificar os profiles 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
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.7 Configurando uma aplicação GPON com ONU Bridge

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

- 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).

- 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.
- 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.

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

Figura 15 – Cenário para Serviço de Acesso a Internet usando a Service-VLAN N:1

Os próximos passos irão guiar o usuário em como proceder com estas configurações.

10.7.1 VLANs

Suponha que o usuário queira usar a VLAN ID 100 e a interface Gigabit Ethernet 1/1/1 para encaminhar o tráfego do serviço.

Configuração

```
config
dot1q
 vlan 100
  interface gigabit-ethernet-1/1/1 tagged
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.7.2 Service Type

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.

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.7.3 Profiles

O usuário deve criar profiles que serão parte das configurações. O procedimento a seguir carrega os **profiles default** para serem utilizados na configuração.

Configuração

```
config
load default-gpon-profiles
Loading.
Done.
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.7.4 ONU

Suponha que o usuário decida usar o método de autenticação do número de série na interface GPON 1/1/1, portanto, deverá usar os seguintes comandos para configurar as ONUs.

Configuração

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

! Configurando a ONU-1 e ONU-2 com o profile default
onu 1
  serial-number ABCN00000001
  line-profile DEFAULT-LINE
onu 2
  serial-number ABCN00000002
```

```
  line-profile DEFAULT-LINE
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.7.5 Service Port

Uma porta de serviço é usada para preencher o espaço entre o tráfego da porta GEM e a VLAN de serviço. Por exemplo, o tráfego oriundo da VLAN ID 100 nas ONUs será mapeado para a Service VLAN 100 através dos seguintes comandos:

Configuração

```
config
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.8 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 profiles 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 profiles default carregados.

Figura 16 – Cenário para Serviço de Acesso a Internet usando a Service-VLAN TLS

Os próximos passos irão guiar o usuário em como proceder com estas configurações.

10.8.1 VLANs

Suponha que o usuário queira usar a VLAN ID 2000 e a interface Gigabit Ethernet 1/1/1 para encaminhar o tráfego do serviço.

Configuração

```
config
dot1q
 vlan 2000
  interface gigabit-ethernet-1/1/1 tagged
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.8.2 Service Type

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

Configuração

```
config
service vlan 2000 type tls
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.8.3 Profiles

O usuário deve criar profiles que serão parte das configurações. O procedimento a seguir carrega os **profiles default** para serem utilizados na configuração.

Configuração

```
config
load default-gpon-profiles
Loading.
Done.
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.8.4 Auto provisionamento

Para ativar o auto provisionamento o usuário deve entrar na configuração global do GPON. Os próximos passos irão demonstrar como proceder com esta configuração:

Configuração

```
config
gpon 1/1
 onu-auto-provisioning
  enable
  line-profile DEFAULT-LINE
  snmp-profile DEFAULT-SNMP
  service-port 1 gem 1 match vlan vlan-id any action vlan add vlan-id 2000
```

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.

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

10.8.5 Interface GPON (PON-Link)

Quando o PON link for habilitado as ONUs descobertas passam a ser autoconfiguradas.

Configuração

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

11 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*) e não marcados (*untagged*) por um identificador de 1 a 4094. Alguns benefícios de utilizar VLANs são:

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

11.1 CONFIGURANDO O AGING TIME DA TABELA MAC

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

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

Configuração

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

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação dos MACs aprendidos pelo equipamento. O usuário deve usar a palavra-chave "do" antes do comando caso estiver no modo de configuração.

Troubleshooting

```
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>
```

11.2 CONFIGURANDO VLAN COM INTERFACES TAGGED

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

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

Configuração

```
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.

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show vlan brief
show vlan detail
show vlan membership detail
```

11.3 Configurando VLAN com Interfaces untagged

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

Para tráfego ***untagged*** é necessário configurar uma native-vlan nas interfaces 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.

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show vlan brief
show vlan detail
show vlan membership detail
```

11.4 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.

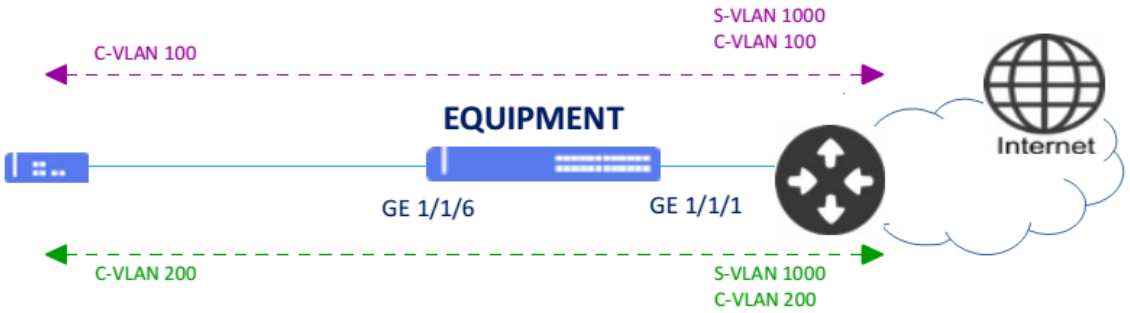

Figura 17 – Exemplo de cenário com QinQ

Os próximos passos irão demonstrar como configurar o QinQ para transportar dois clientes conectados a interface Gigabit-Ethernet-1/1/6. Ambos os clientes possuem uma VLAN (C-VLAN) e serão transportados para a rede da operadora 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.

Configuração

```
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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

11.5 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.

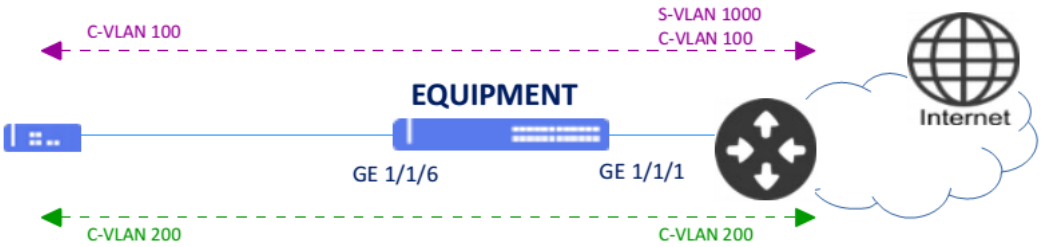

Figura 18 – Exemplo de cenário QinQ Seletivo

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**.

Configuração

```
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
  ingress
   rule qinq-seletivo-vlan-100
    match vlan vlan-id 100
```

```
    action add vlan vlan-id 1000
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

11.6 CONFIGURANDO VLAN-TRANSLATE

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

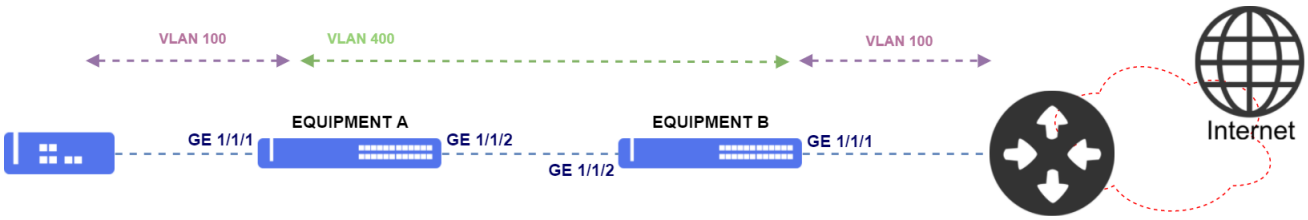

Figura 19 – Exemplo de cenário com VLAN Translate

Os próximos passos irão demonstrar como configurar *VLAN Translate* para traduzir a VLAN 100 para a VLAN 400 na **entrada (ingress)** da interface gigabit ethernet 1/1/1 do equipamento A e realizar a operação contrária na **saída (egress)** no equipamento B.

A configuração do VLAN-Translate se dá através da funcionalidade de mapeamento de VLANs (vlan-mapping), utilizando a action **replace**.

EQUIPMENT A

Configuração

```
Config
dot1q
 vlan 400
  interface gigabit-ethernet-1/1/1
  !
  Interface gigabit-ethernet-1/1/2
  !
 !
!
vlan-mapping
 interface gigabit-ethernet-1/1/1
```

```
  ingress
   rule TRANSLATE-ingress-rule1
    match vlan vlan-id 100
    action replace vlan vlan-id 400
   !
  egress
   rule TRANSLATE-egress-rule1
    match vlan vlan-id 400
    action replace vlan vlan-id 100
   !
  !
 !
!
```

EQUIPMENT B

Configuração

```
config
dot1q
 vlan 400
  interface gigabit-ethernet-1/1/1
  !
  interface gigabit-ethernet-1/1/2
  !
 !
!
vlan-mapping
 interface gigabit-ethernet-1/1/1
  ingress
   rule TRANSLATE-ingress-rule1
    match vlan vlan-id 100
    action replace vlan vlan-id 400
   !
  egress
   rule TRANSLATE-egress-rule1
    match vlan vlan-id 400
    action replace vlan vlan-id 100
   !
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

11.7 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.

Configuração

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

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo estão os principais comandos disponíveis para executar a verificação da desativação do aprendizado de endereços MAC. O usuário deve usar a palavra-chave **"do"** antes do comando caso estiver no modo de configuração.

Troubleshooting

```
show running-config mac-address-table interface learning
```

11.8 Configurando RSTP

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

As BPDU do RSTP são encaminhadas sem a presença de VLAN (*untagged*).

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

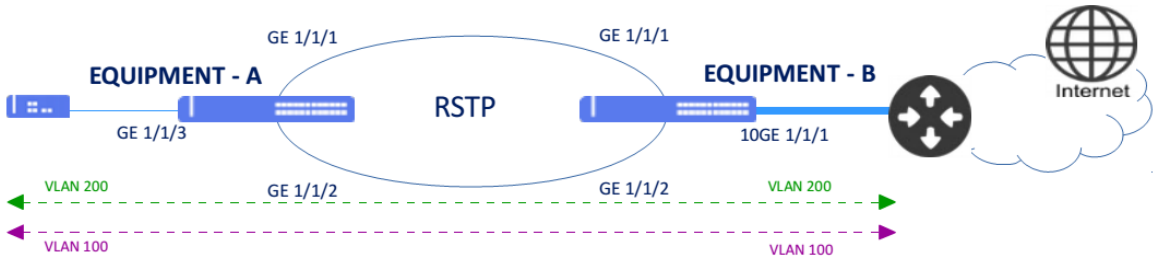

Figura 20 – Exemplo de cenário com RSTP

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:

Configuração

```
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
```

EQUIPMENT - B:

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show spanning-tree
show spanning-tree brief
show spanning-tree detail
show spanning-tree extensive
```

11.9 Configurando EAPS

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

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

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

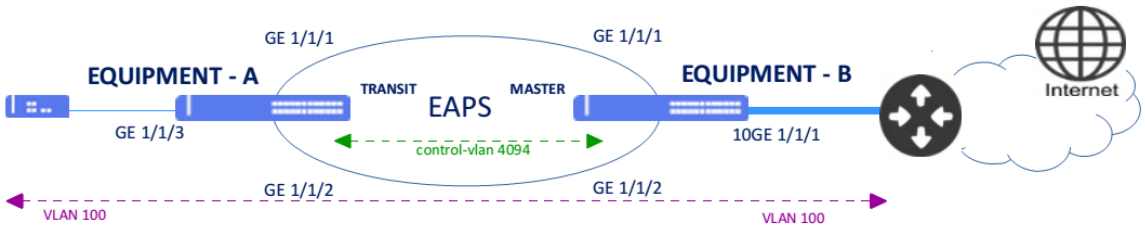

Figura 21 – Exemplo de cenário com EAPS

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:

Configuração

```
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
```

EQUIPMENT - B:

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show eaps
show eaps brief
show eaps detail
```

11.10 CONFIGURANDO 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.

Atualmente, o DmOS suporta o protocolo **ERPS** apenas na configuração em anel principal. Não há suporte para sub-anel com link compartilhado (*shared-link*).

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

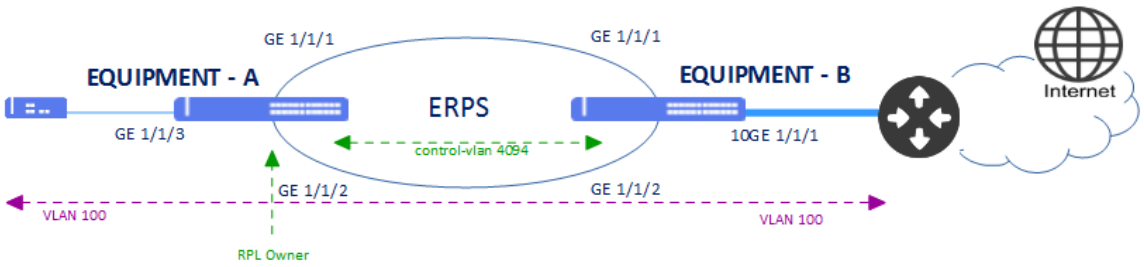

Figura 22 – Exemplo de cenário com ERPS

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:

Configuração

```
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
  !
 !
!
erps
 ring ERPS-PRINCIPAL
  ring-id 1
  control-vlan 4094
  protected-vlans 100
  port0
   interface gigabit-ethernet-1/1/1
  !
  port1
   interface gigabit-ethernet-1/1/2 rpl-role owner
  !
 !
!
```

EQUIPMENT - B:

Configuração

```
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
  !
 !
!
erps
 ring ERPS-PRINCIPAL
  ring-id 1
```

```
  control-vlan 4094
  protected-vlans 100
  port0
   interface gigabit-ethernet-1/1/1
  !
  port1
   interface gigabit-ethernet-1/1/2
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show erps
show erps brief
```

É obrigatório configurar "ring-id 1" caso seja necessario interoperar com outros produtos DATACOM e outros vendors que possuam ERPSv1.

11.11 CONFIGURANDO O 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 BPDUs.

O DmOS suporta o protocolo **L2CP** apenas no modo de configuração extendido (***extended*** **mode**).

Nas plataformas OLT com suporte a tecnologia GPON a transparência de BPDUs 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 BPDUs L2 está desativada sem a possibilidade de alterar este comportamento.

A tabela abaixo resume o comportamento da transparência de BPDUs L2 nas plataformas OLT para cada tipo de serviço GPON.

Tipo da BPDU	Endereços MAC	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
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

Para as demais plataformas, apenas a action ***tunnel*** é suportada, ou seja, qualquer BPDU será encaminhada com a ativação do *tunnel*. A tabela abaixo resume o comportamento padrão do tunelamento de BPDUs L2 caso a ***action tunnel*** não esteja configurada.

Tipo da BPDU	Endereços MAC	Ação padrão
IEEE	01:80:C2:00:00:0X e 01:80:C2:00:00:2X	Bloquear (*drop*)
EAPS	00:E0:2B:00:00:04	Encaminhar (*forward*)
RRPP	00:0F:E2:07:82:XX	Encaminhar (*forward*)
Protocolos Cisco	01:00:0C:CC:XX:XX e 01:00:0C:CD:XX:XX	Encaminhar (*forward*)

O cenário abaixo será usado para demonstrar a configuração do protocolo L2CP.

Figura 23 – Exemplo de cenário com 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.

Configuração (exceto as OLTs)

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do L2CP. O usuário deve usar a palavra-chave **"do"** antes do comando caso estiver no modo de configuração.

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade
```

11.12 Configurando o 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 OLT com suporte a tecnologia GPON.

Para habilitar o DHCP Relay na VLAN 20 o usuário deverá realizar o seguinte procedimento:

Configuração

```
config
dhcp relay vlan 20
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do DHCP Relay L2. O usuário deve usar a palavra-chave "do" antes do comando caso estiver no modo de configuração.

Troubleshooting
`show allowed-ip entry-type dhcp`

12 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.

12.1 CONFIGURANDO ROTEAMENTO ESTÁTICO

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

Figura 24 – Exemplo de cenário com 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.

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show ip route
show ip route static
show ip rib
show ip rib static
show ip interface brief
```

12.2 Configurando o Roteamento entre VLANs

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

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

Figura 25 – Exemplo de cenário com 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. Os próximos passos irão mostrar como realizar estas configurações.

É possível configurar endereço IPv4 secundário nas interfaces L3. Endereço IPv6 secundário não é suportado.

Configuração

```
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
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show ip route
show ip route connected
show ip interface brief
```

12.3 Configurando o VRF Lite

O **VRF** (*Virtual Routing and Forwarding*) é uma funcionalidade que permite a existência de diversas instâncias de roteamento isoladas em um mesmo equipamento. O VRF lite é uma versão mais básica do VRF, sem suporte a sinalização por MPLS.

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.

O cenário abaixo será usado para demonstrar a configuração de duas VRFs lite.

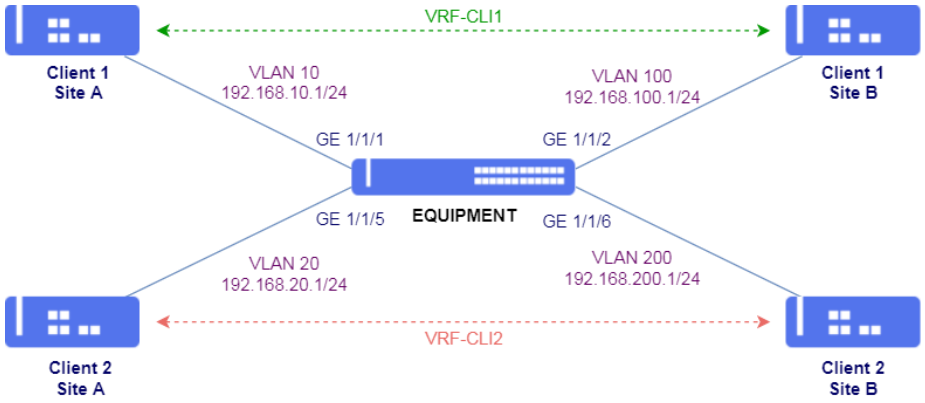

Figura 26 – Isolamento de tráfego entre clientes com VRFs

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

Os próximos passos irão mostrar como realizar estas configurações.

Configuração

```
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
  !
 !
!
vrf VRF-CLI1
!
vrf VRF-CLI2
```

```
!
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
   !
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show ip route vrf <VRF_NAME>
show ip fib vrf <VRF_NAME>
show ip interface vrf <VRF_NAME> brief
```

12.4 Configurando Route Leaking

Utilizando o cenário anterior como base, será incluído um terceiro cliente.

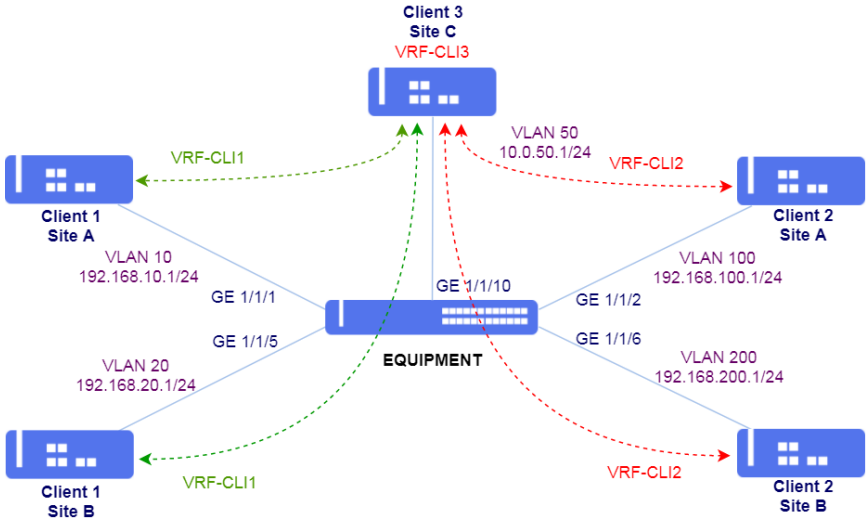

Figura 27 – Route leaking entre VRFs

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.

Serão utilizados os seguintes *RD*'s:

- 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 importas as rotas entre eles.

O route leaking entre VRFs ocorre apenas com a redistribuição de rotas estáticas. A redistribuição de rotas diretamente conectadas ainda não é suportado.

Configuração

```
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
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Rotas importadas e exportadas entre as VRFs irão aparecer como aprendidas via BGP, nas tabelas de roteamento de cada VRF.

Abaixo os principais comandos para realizar a verificação das rotas nas VRFs.

Troubleshooting

```
show ip route vrf <VRF_NAME>
show ip fib vrf <VRF_NAME>
```

12.5 Configurando o OSPFv2

O OSPFv2 (*Open Shortest Path First version 2*) é o *Internal Gateway Protocol* descrito pela RFC 2328 (versão 2) para roteamento de endereços IPv4. Este protocolo é utilizado dentro de um mesmo AS (Autonomous System), justificando a sua denominação de Internal. É baseado no algoritmo de *Dijkstra*, que calcula o caminho mais curto para cada destino com base nos custos de cada link.

Atualmente, o OSPFv2 suporta redes do tipo ponto-a-ponto e broadcast.

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

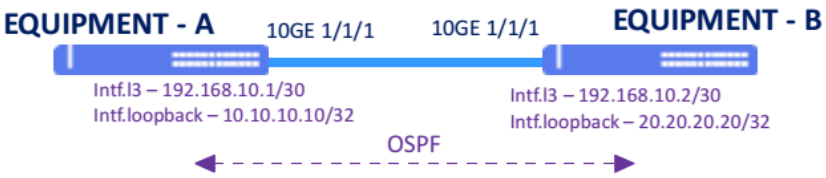

Figura 28 – Exemplo de cenário com básica do protocolo OSPFv2

Suponha que o usuário queira realizar uma sessão OSPF na área 0 com *network-type* do tipo ponto-a-ponto através das seguintes configurações:

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

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

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

EQUIPMENT - A:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
switchport
 interface ten-gigabit-ethernet-1/1/1
  native-vlan
   vlan-id 1000
   !
  !
 !
!
interface l3 OSPF
 ipv4 address 192.168.10.1/30
  lower-layer-if vlan 1000
  !
 !
!
 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
  !
 !
!
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
switchport
 interface ten-gigabit-ethernet-1/1/1
  native-vlan
   vlan-id 1000
   !
  !
 !
!
interface l3 OSPF
 ipv4 address 192.168.10.2/30
  lower-layer-if vlan 1000
  !
 !
!
 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
  !
 !
!
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
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
```

12.6 Configurando o OSPFv3

O OSPFv3 (*Open Shortest Path First version 3*) é o Internal Gateway Protocol descrito pela RFC 2740 para roteamento de endereços IPv6. Este protocolo é utilizado dentro de um mesmo AS (Autonomous System), justificando a sua denominação de Internal. É baseado no algoritmo de *Dijkstra*, que calcula o caminho mais curto para cada destino com base nos custos dos links.

Atualmente, o OSPFv3 suporta apenas redes do tipo ponto-a-ponto.

O cenário abaixo será usado para demonstrar a configuração do OSPFv3.

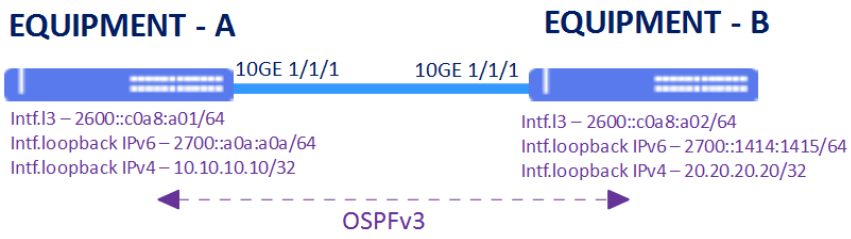

Figura 29 – Exemplo de cenário com básica do protocolo OSPFv3

Suponha que o usuário queira realizar as seguintes configurações:

- EQUIPMENT - A: Interface L3 na VLAN 1000 com endereço IPv6 2600::c0a8:a01/64 e interface loopback com IPv6 2700::a0a:a0a/64 e IPv4 10.10.10.10/32 sendo esta utilizada como router-id no OSPFv3 na área 0.

- EQUIPMENT - B: Interface L3 na VLAN 1000 com endereço IPv6 2600::c0a8:a02/64 e interface loopback com IPv6 2700::1414:1415/64 e IPv4 20.20.20.20/32 sendo esta utilizada como router-id no OSPFv3 na área 0.

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

EQUIPMENT - A:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
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:a01/64
 !
!
interface loopback 0
 ipv4 address 10.10.10.10/32
 ipv6 enable
 ipv6 address 2700::a0a:a0a/64
 !
!
router ospfv3 1
 router-id 10.10.10.10
 area 0
  interface l3-OSPFv3
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
```

```
    !
   !
  !
!
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
  !
 !
!
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do OSPFv3.

Troubleshooting

```
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
```

12.7 Configurando o BGP IPv4

O protocolo BGP (*Border Gateway Protocol*) é o protocolo usado para a troca de informações de roteamento entre AS (*autonomous-system*) na Internet. Ao estabelecer uma vizinhança com um 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*).

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

Figura 30 – Exemplo de cenário com básica do 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:

Configuração

```
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
   !
  !
 !
!
```

EQUIPMENT - B:

Configuração

```
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
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do BGP IPv4.

Troubleshooting

```
show ip bgp
show ip bgp neighbor
show ip bgp prefixes
show ip bgp summary
show ip route bgp
show ip rib bgp
```

12.8 Configurando o BGP IPv6

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*).

O cenário abaixo será usado para demonstrar a configuração do protocolo BGP com endereçamento IPv6 no mesmo AS, ou seja, iBGP.

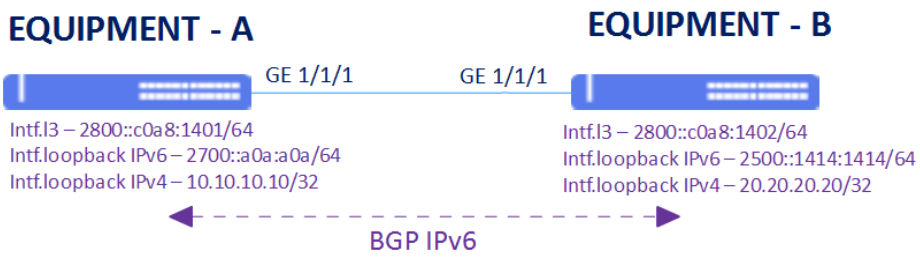

Figura 31 – Exemplo de cenário com básica do protocolo BGP IPv6

Suponha que o usuário queira realizar as seguintes configurações:

- EQUIPMENT - A: Interface L3 na VLAN 2000 com endereço IPv6 2800::c0a8:1401/64 e interface loopback com IPv6 2700::a0a:a0a/64 e IPv4 10.10.10.10/32 sendo esta utilizada como router-id no BGP com AS local 20000 e AS remoto 20000.

- EQUIPMENT - B: Interface L3 na VLAN 2000 com endereço IPv6 2800::c0a8:1402/64 e interface loopback com IPv6 2500::1414:1414/64 e IPv4 20.20.20.20/32 sendo esta utilizada como router-id no BGP com AS local 20000 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:

Configuração

```
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::c0a8:1401/64
 !
!
 interface loopback 0
  ipv4 address 10.10.10.10/32
  ipv6 enable
  ipv6 address 2700::a0a:a0a/64
  !
 !
!
router bgp 20000
 router-id 10.10.10.10
 address-family ipv6 unicast
 !
 neighbor 2500::1414:1414
  update-source-address 2700::a0a:a0a
  remote-as 20000
  ebgp-multihop 255
  address-family ipv6 unicast
  !
```

```
 !
!
router static
 address-family ipv6
  2500::/64 next-hop 2800::c0a8:1402
```

EQUIPMENT - B:

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do BGP IPv6.

Troubleshooting

```
show ip bgp
show ip bgp neighbor
show ip bgp prefixes
show ip bgp summary
show ipv6 route bgp
show ipv6 rib bgp
```

12.9 CONFIGURANDO O 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.

O cenário abaixo será usado para demonstrar a configuração do protocolo VRRPv2.

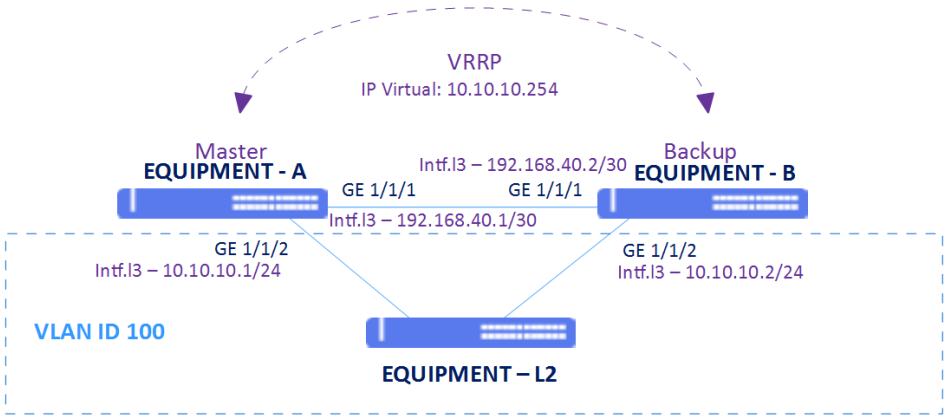

Figura 32 – Exemplo de cenário com básica do protocolo VRRP

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:

Configuração

```
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
```

EQUIPMENT - B:

Configuração

```
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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show router vrrp brief
```

13 MPLS

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

13.1 Utilizando as funcionalidades do MPLS

Uma licença é necessária para a operação do MPLS. Para mais detalhes de como ativá-la, verifique Ativando a licença MPLS.

13.2 Configurando uma L2VPN Port Based com VPWS

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

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

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

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

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

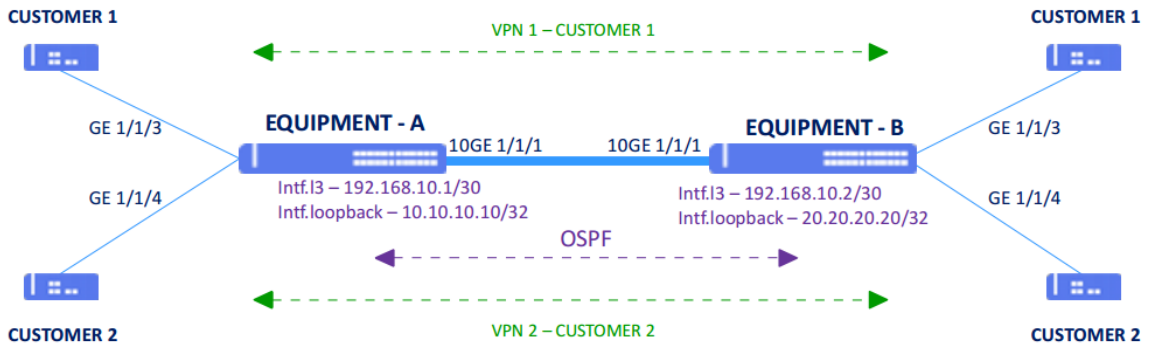

Figura 33 – Exemplo de cenário com L2VPN Port Based com VPWS

Suponha que o usuário deseje configurar duas VPN Port Based usando VPWS entre dois equipamentos. Os próximos passos irão mostrar como realizar estas configurações.

- 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 e como lsr-id no LDP. VPN1 com pw-id 10 e interface gigabit 1/1/3 como interface de acesso. VPN2 com pw-id 20 e interface gigabit 1/1/4 como interface de acesso.

- 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 e como lsr-id no LDP. VPN1 com pw-id 10 e interface gigabit 1/1/3 como interface de acesso. VPN2 com pw-id 20 e interface gigabit 1/1/4 como interface de acesso.

EQUIPMENT - A:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
switchport
 interface ten-gigabit-ethernet-1/1/1
  native-vlan
   vlan-id 1000
   !
  !
 !
!
interface l3 OSPF
 ipv4 address 192.168.10.1/30
 lower-layer-if vlan 1000
 !
!
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
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  neighbor targeted 20.20.20.20
  !
 !
!
mpls l2vpn
 vpws-group VPWS-DATACOM
  vpn VPN1
   neighbor 20.20.20.20
    pw-id 10
    !
   !
   access-interface gigabit-ethernet-1/1/3
   !
  !
  vpn VPN2
   neighbor 20.20.20.20
    pw-id 20
    !
   !
   access-interface gigabit-ethernet-1/1/4
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
switchport
 interface ten-gigabit-ethernet-1/1/1
  native-vlan
   vlan-id 1000
   !
  !
 !
!
interface l3 OSPF
```

```
   ipv4 address 192.168.10.2/30
   lower-layer-if vlan 1000
   !
  !
!
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
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  neighbor targeted 10.10.10.10
  !
 !
!
mpls l2vpn
 vpws-group VPWS-DATACOM
  vpn VPN1
   neighbor 10.10.10.10
    pw-id 10
    !
   !
   access-interface gigabit-ethernet-1/1/3
   !
  !
  vpn VPN2
   neighbor 10.10.10.10
    pw-id 20
    !
   !
   access-interface gigabit-ethernet-1/1/4
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show mpls l2vpn hardware
show mpls l2vpn vpws-group
show mpls ldp database
show mpls ldp neighbor
show mpls ldp parameters
```

```
show mpls forwarding-table
```

13.3 Configurando uma L2VPN VLAN Based com VPWS

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

Com L2VPNs VLAN Based é possível concentrar diversas VPNs em um único link.

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

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

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

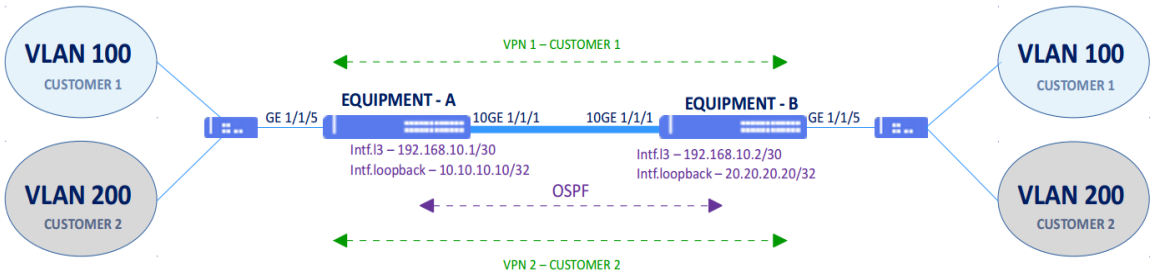

Figura 34 – Exemplo de cenário com L2VPN VLAN Based com VPWS

Suponha que o usuário deseje configurar duas L2VPN VLAN Based usando VPWS entre dois equipamentos. Os próximos passos irão mostrar como realizar estas configurações.

- 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 e como lsr-id no LDP. VPN1 com pw-id 10 e VLAN 100. VPN2 com pw-id 20 e VLAN 200.

- 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 e como lsr-id no LDP.

VPN1 com pw-id 10 e interface gigabit 1/1/3 como interface de acesso. VPN1 com pw-id 10 e VLAN 100. VPN2 com pw-id 20 e VLAN 200.

EQUIPMENT - A:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
switchport
 interface ten-gigabit-ethernet-1/1/1
  native-vlan
   vlan-id 1000
   !
  !
 !
!
interface l3 OSPF
 ipv4 address 192.168.10.1/30
 lower-layer-if vlan 1000
 !
!
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
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  neighbor targeted 20.20.20.20
  !
 !
!
mpls l2vpn
 vpws-group VPWS-DATACOM
  vpn VPN1
   neighbor 20.20.20.20
    pw-type vlan
    pw-id 10
   !
   access-interface gigabit-ethernet-1/1/5
    dot1q 100
```

```
    !
   !
   vpn VPN2
    neighbor 20.20.20.20
     pw-type vlan
     pw-id 20
    !
    access-interface gigabit-ethernet-1/1/5
     dot1q 200
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/1
   untagged
   !
  !
 !
!
switchport
 interface ten-gigabit-ethernet-1/1/1
  native-vlan
   vlan-id 1000
   !
  !
 !
!
interface l3 OSPF
  ipv4 address 192.168.10.2/30
  lower-layer-if vlan 1000
  !
 !
!
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
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  neighbor targeted 10.10.10.10
  !
 !
!
mpls l2vpn
```

```
vpws-group VPWS-DATACOM
 vpn VPN1
  neighbor 10.10.10.10
   pw-type vlan
   pw-id 10
  !
  access-interface gigabit-ethernet-1/1/5
   dot1q 100
  !
 !
 vpn VPN2
  neighbor 10.10.10.10
   pw-type vlan
   pw-id 20
  !
  access-interface gigabit-ethernet-1/1/5
   dot1q 200
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show mpls l2vpn hardware
show mpls l2vpn vpws-group
show mpls ldp database
show mpls ldp neighbor
show mpls ldp parameters
show mpls forwarding-table
```

13.4 Configurando uma L2VPN Port Based com 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 *L2*. Realiza a emulação de serviços Ethernet ponto-multiponto permitindo que sites geograficamente isolados sejam conectados por meio de uma MAN (*Metropolitan Area Network*) ou de uma WAN (*Wide Area Network*). Todos os serviços em uma VPLS estão no mesmo domínio de broadcast.

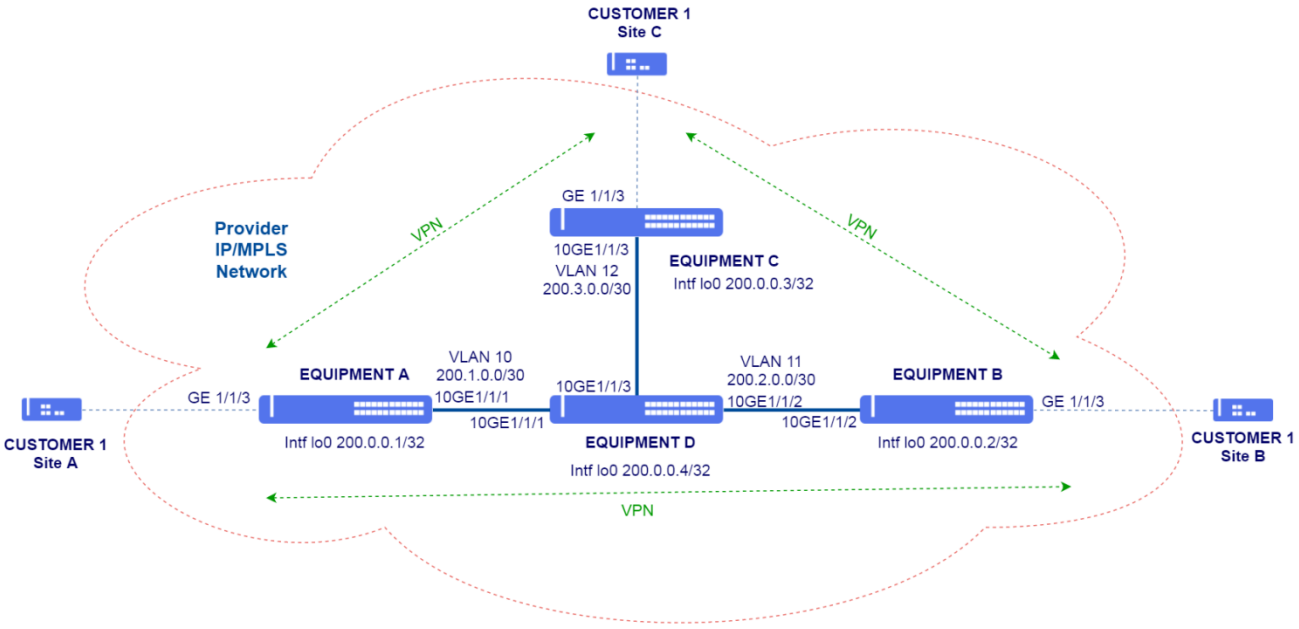

Figura 28 - VPLS Port Based

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

EQUIPMENT - A:

Configuração

```
config
dot1q
 vlan 10
  interface ten-gigabit-ethernet-1/1/1
  !
 !
!
interface l3 OSPF
 ipv4 address 200.1.0.1/30
 lower-layer-if vlan 10
 !
!
interface loopback 0
 ipv4 address 200.0.0.1/32
 !
```

```
!
router ospf 1
 router-id 200.0.0.1
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 200.0.0.2
  !
  neighbor targeted 200.0.0.3
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
    pw-type ethernet
    neighbor 200.0.0.2
     pw-id 100
    !
    neighbor 200.0.0.3
     pw-id 101
    !
   !
   bridge-domain
    access-interface gigabit-ethernet-1/1/3
   !
  !
 !
!
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 11
  interface ten-gigabit-ethernet-1/1/2
  !
 !
!
interface l3 OSPF
 ipv4 address 200.2.0.1/30
 lower-layer-if vlan 11
 !
!
interface loopback 0
 ipv4 address 200.0.0.2/32
 !
```

```
!
router ospf 1
 router-id 200.0.0.2
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 200.0.0.1
  !
  neighbor targeted 200.0.0.3
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
    pw-type ethernet
    neighbor 200.0.0.1
     pw-id 100
    !
    neighbor 200.0.0.3
     pw-id 103
    !
   !
   bridge-domain
    access-interface gigabit-ethernet-1/1/3
   !
  !
 !
!
```

EQUIPMENT - C:

Configuração

```
config
dot1q
 vlan 12
  interface ten-gigabit-ethernet-1/1/3
  !
 !
!
interface l3 OSPF
 ipv4 address 200.3.0.1/30
 lower-layer-if vlan 12
 !
!
interface loopback 0
 ipv4 address 200.0.0.3/32
 !
```

```
!
router ospf 1
 router-id 200.0.0.3
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 200.0.0.1
  !
  neighbor targeted 200.0.0.2
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
    pw-type ethernet
    neighbor 200.0.0.1
     pw-id 100
    !
    neighbor 200.0.0.2
     pw-id 103
    !
   !
   bridge-domain
    access-interface gigabit-ethernet-1/1/3
   !
  !
 !
!
```

EQUIPMENT - D:

Configuração

```
config
dot1q
 vlan 10
  interface ten-gigabit-ethernet-1/1/1
  !
 !
 vlan 11
  interface ten-gigabit-ethernet-1/1/2
  !
 !
 vlan 12
  interface ten-gigabit-ethernet-1/1/3
  !
 !
```

```
!
interface l3 OSPF-10
 ipv4 address 200.1.0.2/30
 lower-layer-if vlan 10
 !
!
interface l3 OSPF-11
 ipv4 address 200.2.0.2/30
 lower-layer-if vlan 11
 !
!
interface l3 OSPF-12
 ipv4 address 200.3.0.2/30
 lower-layer-if vlan 12
 !
!
interface loopback 0
 ipv4 address 200.0.0.4/32
 !
!
router ospf 1
 router-id 200.0.0.4
 area 0
  interface l3-OSPF-10
   network-type point-to-point
  !
  interface l3-OSPF-11
   network-type point-to-point
  !
  interface l3-OSPF-12
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF-10
  !
  interface l3-OSPF-11
  !
  interface l3-OSPF-12
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show mpls l2vpn hardware
show mpls l2vpn vpls-group
show mpls ldp database
show mpls ldp neighbor
show mpls ldp parameters
show mpls forwarding-table
```

13.5 Configurando uma L2VPN VLAN Based com 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 *L2*. Realiza a emulação de serviços Ethernet ponto-multiponto permitindo que sites geograficamente isolados sejam conectados por meio de uma MAN (*Metropolitan Area Network*) ou de uma WAN (*Wide Area Network*). Todos os serviços em uma VPLS estão no mesmo domínio de broadcast.

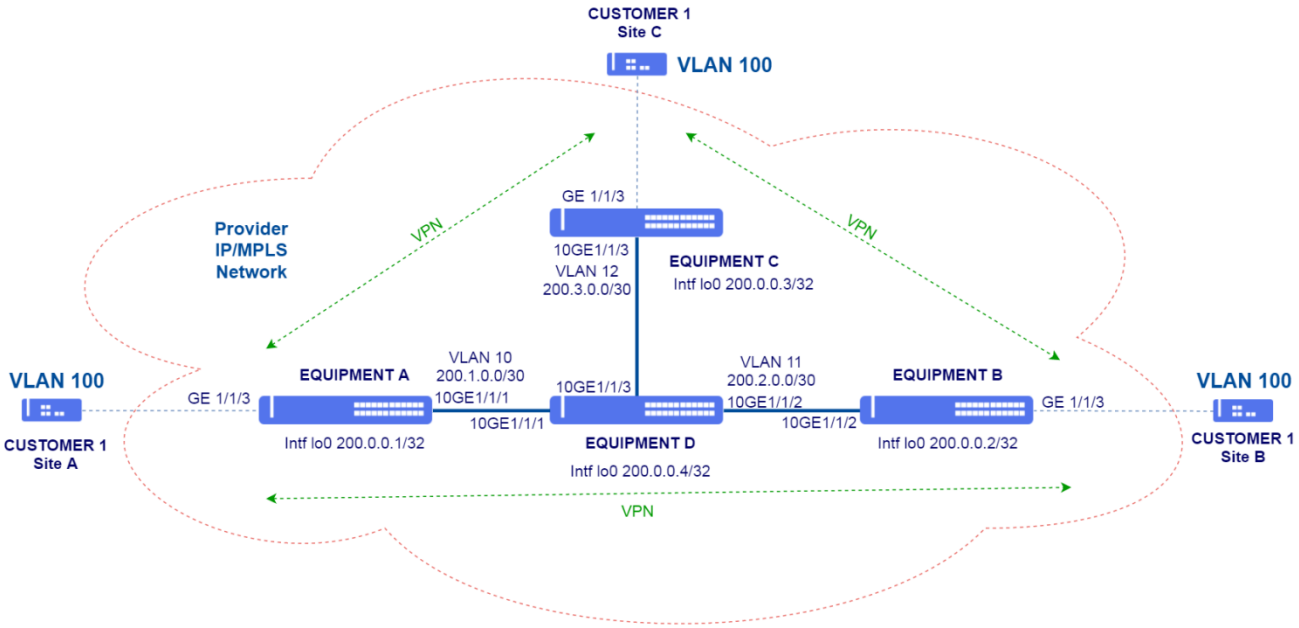

Figura 31 - VPLS VLAN Based

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

EQUIPMENT - A:

Configuração

```
config
dot1q
 vlan 10
  interface ten-gigabit-ethernet-1/1/1
  !
```

```
 !
!
interface l3 OSPF
 ipv4 address 200.1.0.1/30
 lower-layer-if vlan 10
 !
!
interface loopback 0
 ipv4 address 200.0.0.1/32
 !
!
router ospf 1
 router-id 200.0.0.1
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 200.0.0.2
  !
  neighbor targeted 200.0.0.3
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
    pw-type vlan
    neighbor 200.0.0.2
     pw-id 100
    !
    neighbor 200.0.0.3
     pw-id 101
    !
   !
   bridge-domain
    dot1q 100
    access-interface gigabit-ethernet-1/1/3
   !
  !
 !
!
```

EQUIPMENT - B:

Configuração

```
config
dot1q
 vlan 11
  interface ten-gigabit-ethernet-1/1/2
```

```
   !
  !
!
interface l3 OSPF
 ipv4 address 200.2.0.1/30
 lower-layer-if vlan 11
 !
!
interface loopback 0
 ipv4 address 200.0.0.2/32
 !
!
router ospf 1
 router-id 200.0.0.2
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 200.0.0.1
  !
  neighbor targeted 200.0.0.3
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
    pw-type vlan
    neighbor 200.0.0.1
     pw-id 100
    !
    neighbor 200.0.0.3
     pw-id 103
    !
   !
   bridge-domain
    dot1q 100
    access-interface gigabit-ethernet-1/1/3
   !
  !
 !
!
```

EQUIPMENT - C:

Configuração

```
config
dot1q
 vlan 12
```

```
   interface ten-gigabit-ethernet-1/1/3
   !
  !
!
interface l3 OSPF
 ipv4 address 200.3.0.1/30
 lower-layer-if vlan 12
 !
!
interface loopback 0
 ipv4 address 200.0.0.3/32
 !
!
router ospf 1
 router-id 200.0.0.3
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 200.0.0.1
  !
  neighbor targeted 200.0.0.2
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
    pw-type vlan
    neighbor 200.0.0.1
     pw-id 100
    !
    neighbor 200.0.0.2
     pw-id 103
    !
   !
   bridge-domain
    dot1q 100
    access-interface gigabit-ethernet-1/1/3
   !
  !
 !
!
```

EQUIPMENT - D:

Configuração

```
config
dot1q
 vlan 10
  interface ten-gigabit-ethernet-1/1/1
  !
 !
 vlan 11
  interface ten-gigabit-ethernet-1/1/2
  !
 !
 vlan 12
  interface ten-gigabit-ethernet-1/1/3
  !
 !

!
interface l3 OSPF-10
 ipv4 address 200.1.0.2/30
 lower-layer-if vlan 10
 !
!
interface l3 OSPF-11
 ipv4 address 200.2.0.2/30
 lower-layer-if vlan 11
 !
!
interface l3 OSPF-12
 ipv4 address 200.3.0.2/30
 lower-layer-if vlan 12
 !
!
interface loopback 0
 ipv4 address 200.0.0.4/32
 !
!
router ospf 1
 router-id 200.0.0.4
 area 0
  interface l3-OSPF-10
   network-type point-to-point
  !
  interface l3-OSPF-11
   network-type point-to-point
  !
  interface l3-OSPF-12
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF-10
  !
  interface l3-OSPF-11
  !
```

```
  interface l3-OSPF-12
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show mpls l2vpn hardware
show mpls l2vpn vpls-group
show mpls ldp database
show mpls ldp neighbor
show mpls ldp parameters
show mpls forwarding-table
```

13.6 CONFIGURANDO H-VPLS

O Hierarchical VPLS (**H-VPLS**) reduz o número de PWs dividindo uma rede VPLS em um domínio de backbone e domínios de borda para evitar sobrecarga de sinalização PW gerado pela malha completa de PWs entre todos os PEs em uma instância VPLS.

Em H-VPLS:

- Um domínio de borda fornece acesso para uma rede de usuários ao domínio de backbone.
- Os dispositivos NPE (Network Provider Edge, borda do provedor de rede) são totalmente integrados no domínio de backbone. Um PW entre NPEs é referido como um N-PW.
- Um dispositivo UPE (User-Front-Provider Edge - Borda do Provedor de Prova do Usuário) estabelece apenas um PW com o NPE vizinho. Um PW entre um UPE e um NPE é referido como um U-PW.

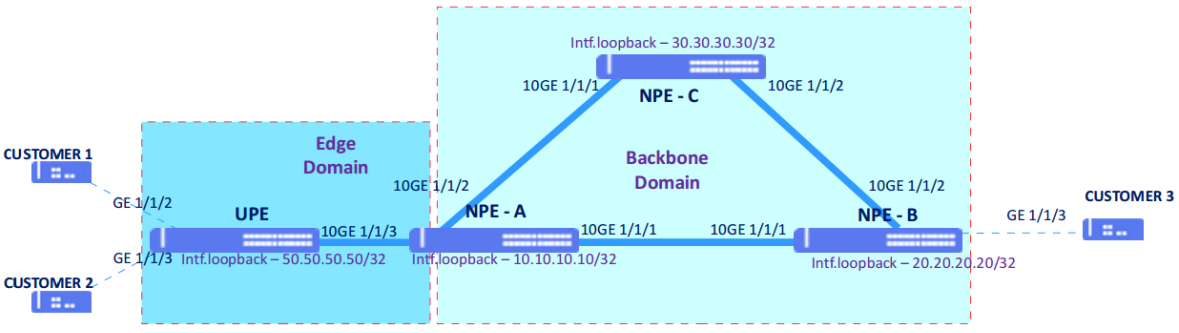

Figura 4 - H-VPLS usando acesso MPLS

Os próximos passos irão mostrar como realizar as configurações da rede com H-VPLS.

UPE:

Configuração

```
config
dot1q
 vlan 1000
  interface ten-gigabit-ethernet-1/1/3
  !
 !
!
interface l3 OSPF
  ipv4 address 192.168.10.1/30
  lower-layer-if vlan 1000
  !
 !
!
interface loopback 0
 ipv4 address 50.50.50.50/32
 !
!
router ospf 1
 router-id 50.50.50.50
 area 0
  interface l3-OSPF
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF
  !
  neighbor targeted 10.10.10.10
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
  vfi
   pw-type ethernet
   neighbor 10.10.10.10
    split-horizon disable
    pw-id 50
   !
  !
  bridge-domain
   access-interface gigabit-ethernet-1/1/2
   !
   access-interface gigabit-ethernet-1/1/3
  !
 !
!
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

NPE-A:

Configuração

```
config
dot1q
 vlan 1002
  interface ten-gigabit-ethernet-1/1/2
  !
 !
 vlan 1001
  interface ten-gigabit-ethernet-1/1/1
  !
 vlan 1000
  interface ten-gigabit-ethernet-1/1/3
  !
 !
interface l3 OSPF-1000
 ipv4 address 192.168.10.2/30
 lower-layer-if vlan 1000
 !
!
interface l3 OSPF-1001
 ipv4 address 192.168.11.1/30
 lower-layer-if vlan 1001
 !
!
interface l3 OSPF-1002
 ipv4 address 192.168.12.1/30
 lower-layer-if vlan 1002
 !
!
interface loopback 0
 ipv4 address 10.10.10.10/32
 !
!
router ospf 1
 router-id 10.10.10.10
 area 0
  interface l3-OSPF-1000
   network-type point-to-point
  !
  interface l3-OSPF-1001
   network-type point-to-point
  !
  interface l3-OSPF-1002
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF-1000
```

```
   !
   interface l3-OSPF-1001
   !
   interface l3-OSPF-1002
   !
   neighbor targeted 50.50.50.50
   !
   neighbor targeted 30.30.30.30
   !
   neighbor targeted 20.20.20.20
   !
  !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
   pw-type ethernet
   neighbor 50.50.50.50
      split-horizon disable
      pw-id 50
    !
   neighbor 30.30.30.30
      pw-id 20
    !
   neighbor 20.20.20.20
      pw-id 10
    !
   !
  !
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

NPE-B:

Configuração

```
config
dot1q
 vlan 1002
  interface ten-gigabit-ethernet-1/1/1
  !
 !
 vlan 1003
  interface ten-gigabit-ethernet-1/1/2
  !
 !
!
interface l3 OSPF-1002
  ipv4 address 192.168.12.1/30
  lower-layer-if vlan 1002
  !
 !
```

```
!
interface l3 OSPF-1003
  ipv4 address 192.168.13.1/30
  lower-layer-if vlan 1003
  !
 !
!
interface loopback 0
 ipv4 address 20.20.20.20/32
 !
!
router ospf 1
 router-id 20.20.20.20
 area 0
  interface l3-OSPF-1002
   network-type point-to-point
  !
  interface l3-OSPF-1003
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF-1002
  !
  interface l3-OSPF-1003
  !
  neighbor targeted 10.10.10.10
  !
  neighbor targeted 30.30.30.30
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
   pw-type ethernet
   neighbor 10.10.10.10
    pw-id 10
    !
   neighbor 30.30.30.30
    pw-id 30
   !
   bridge-domain
    access-interface gigabit-ethernet-1/1/3
   !
  !
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

NPE-C:

Configuração

```
config
dot1q
 vlan 1002
  interface ten-gigabit-ethernet-1/1/1
  !
 !
 vlan 1003
  interface ten-gigabit-ethernet-1/1/2
  !
 !
!
interface l3 OSPF-1002
  ipv4 address 192.168.12.2/30
  lower-layer-if vlan 1002
  !
 !
!
interface l3 OSPF-1003
  ipv4 address 192.168.13.2/30
  lower-layer-if vlan 1003
  !
 !
!
interface loopback 0
 ipv4 address 30.30.30.30/32
 !
!
router ospf 1
 router-id 30.30.30.30
 area 0
  interface l3-OSPF-1002
   network-type point-to-point
  !
  interface l3-OSPF-1003
   network-type point-to-point
  !
  interface loopback-0
  !
 !
!
mpls ldp
 lsr-id loopback-0
  interface l3-OSPF-1002
  !
  interface l3-OSPF-1003
  !
  neighbor targeted 20.20.20.20
  !
  neighbor targeted 10.10.10.10
  !
 !
!
mpls l2vpn
 vpls-group VPLS-DATACOM
  vpn VPN1
   vfi
   pw-type ethernet
```

```
   neighbor 20.20.20.20
    pw-id 30
    !
   neighbor 10.10.10.10
    pw-id 20
   !
  !
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show mpls l2vpn hardware
show mpls l2vpn vpls-group
show mpls ldp database
show mpls ldp neighbor
show mpls ldp parameters
show mpls forwarding-table
```

13.7 CONFIGURANDO L3VPN

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

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

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.

13.7.1 Habilitando o BGP para L3VPN

A troca de labels e redes das L3VPN é feita através do BGP. Para isto, é necessário habilitar a família *vpnv4* no protocolo.

Configuração

```
router bgp <ASN>
 address-family vpnv4 unicast
 !
 neighbor <neighbor-address>
  address-family vpnv4 unicast
 !
!
```

Troubleshooting

```
show mpls l3vpn vpnv4 vrf <vrf-name> brief
show ip bgp vpnv4 labels
show ip route vrf <vrn-name>
show ip fib vrf <vrf-name> brief
show ip interface vrf <vrf-name> brief
```

13.7.2 Configurando uma L3VPN

Na topologia a seguir, serão configurados dois switches PE. No EQUIPAMENT A, há uma interface com endereço IP 192.168.10.1/24 conectado a um CE. No EQUIPAMENT B, há duas interfaces, com endereços IP 192.168.20.1/24 e 192.168.30.1/24, conectadas a outros dois CEs. Os equipamentos 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.

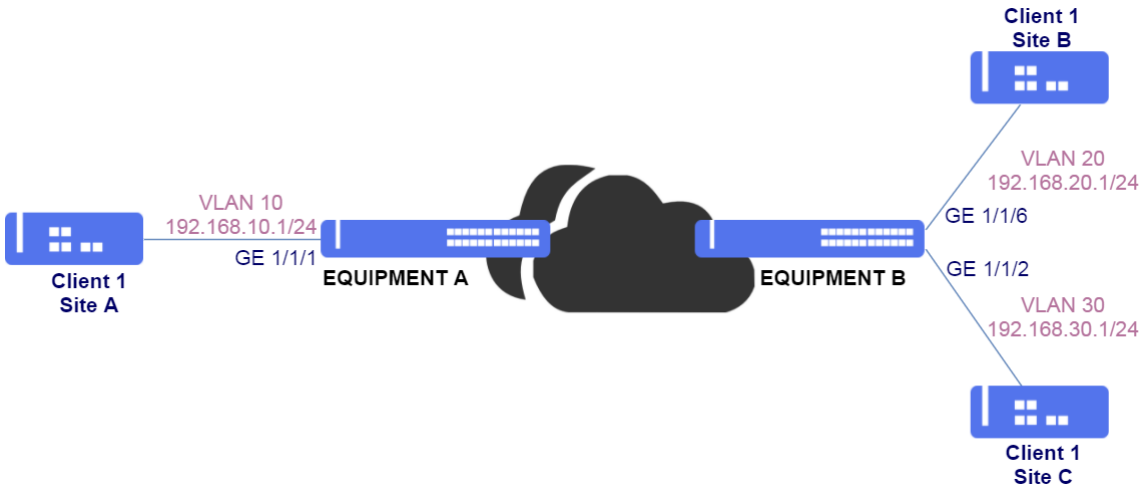

Figura 35 – L3VPN

EQUIPMENT A

Configuração

```
dot1q
 vlan 10
  interface gigabit-ethernet 1/1/1
 !
!
vrf cli1
 rd 2000:10
 address-family ipv4 unicast
  route-target import 2000:10
  !
  route-target export 2000:10
  !
 !
!
interface l3 VRF-CLI1-VLAN10
 vrf cli1
 lower-layer-if vlan 10
 ipv4 address 192.168.10.1/24
!
router bgp 65500
 neighbor 2.2.2.2
  update-source-address 1.1.1.1
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
 !
 vrf cli1
  address-family ipv4 unicast
   redistribute connected
   !
   exit-address-family
  !
!
```

EQUIPMENT B

Configuração

```
dot1q
 vlan 20
  interface gigabit-ethernet 1/1/6
 !
!
vrf cli1
 rd 2000:10
 address-family ipv4 unicast
  route-target import 2000:10
  !
  route-target export 2000:10
  !
 !
!
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
!
router bgp 65500
 neighbor 1.1.1.1
  update-source-address 2.2.2.2
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
 !
 vrf cli1
  address-family ipv4 unicast
   redistribute connected
   !
   exit-address-family
  !
!
```

Troubleshooting

```
show mpls l3vpn vpnv4 vrf <vrf-name> brief
show ip bgp vpnv4 labels
show ip route vrf <vrn-name>
show ip fib vrf <vrf-name> brief
show ip interface vrf <vrf-name> brief
```

13.7.3 Configurando uma L3VPN em topologia Hub and Spoke

Em uma topologia *hub-and-spoke*, diferentes sites 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 pode onde passa todo o tráfego, poderá controlar o roteamento entre os sites.

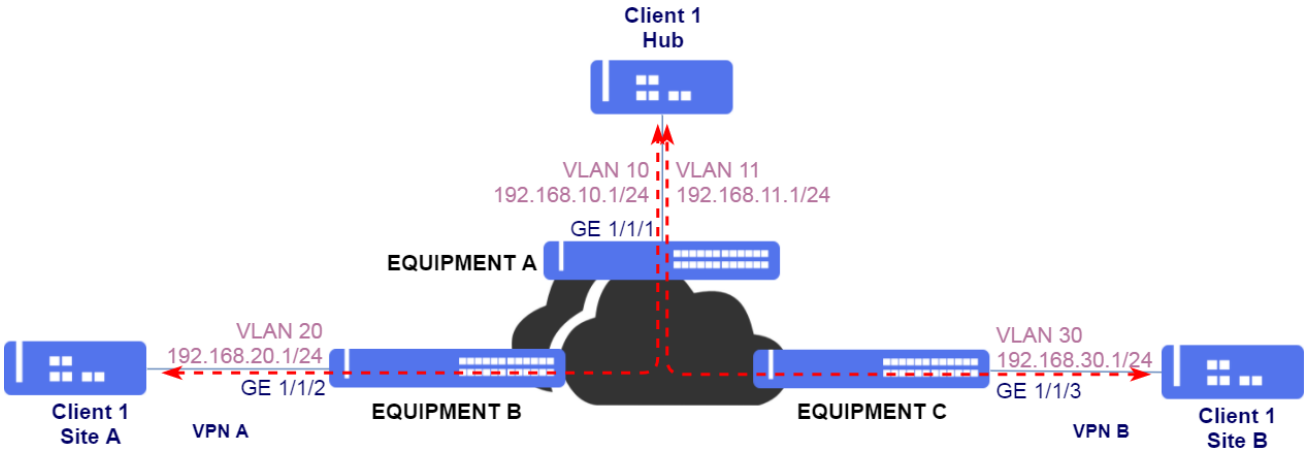

Figura 36 – L3VPN com hub-and-spoke

EQUIPMENT A

Configuração

```
dot1q
 vlan 10
  interface gigabit-ethernet 1/1/1
 !
 vlan 11
  interface gigabit-ethernet 1/1/1
 !
!
vrf cli1-A
 rd 65000:20
 address-family ipv4 unicast
  route-target import 65000:20
  !
  route-target export 65000:20
  !
 !
!
vrf cli1-B
 rd 65000:30
 address-family ipv4 unicast
  route-target import 65000:30
  !
  route-target export 65000:30
  !
 !
!
interface l3 VRF-CLI1-B-VLAN11
 vrf cli1-B
 lower-layer-if vlan 11
 ipv4 address 192.168.11.1/24
!
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 192.168.10.2
   !
  !
 !
!
router bgp 65500
 neighbor 2.2.2.2
  update-source-address 1.1.1.1
  remote-as 65500
  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 65500
  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
  !
!
```

EQUIPMENT B

Configuração

```
dot1q
 vlan 20
  interface gigabit-ethernet 1/1/3
 !
!
vrf cli1
 rd 65000:10
 address-family ipv4 unicast
  route-target import 65000:10
  !
  route-target export 65000:10
  !
 !
```

```
!
interface l3 VRF-CLI1-VLAN20
 vrf cli1
 lower-layer-if vlan 20
 ipv4 address 192.168.20.1/24
!
router bgp 65500
 neighbor 1.1.1.1
  update-source-address 2.2.2.2
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !
 neighbor 3.3.3.3
  update-source-address 2.2.2.2
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !

 vrf cli1
  address-family ipv4 unicast
   redistribute connected
   !
   exit-address-family
  !
!
```

EQUIPMENT C

Configuração

```
dot1q
 vlan 30
  interface gigabit-ethernet 1/1/3
 !
!
vrf cli1
 rd 65500:30
 address-family ipv4 unicast
  route-target import 65500:30
  !
  route-target export 65500:30
  !
 !
!
interface l3 VRF-CLI1-VLAN30
 vrf cli1
 lower-layer-if vlan 30
 ipv4 address 192.168.30.1/24
!
router bgp 65500
 neighbor 1.1.1.1
```

```
  update-source-address 3.3.3.3
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !
 neighbor 3.3.3.3
  update-source-address 2.2.2.2
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !
 vrf cli1
  address-family ipv4 unicast
   redistribute connected
   !
   exit-address-family
  !
!
```

Troubleshooting

```
show mpls l3vpn vpnv4 vrf <vrf-name> brief
show ip bgp vpnv4 labels
show ip route vrf <vrn-name>
show ip fib vrf <vrf-name> brief
show ip interface vrf <vrf-name> brief
```

13.7.4 Estabelecendo sessões BGP em uma L3VPN

É possível estabelecer sessões eBGP entre os PEs e os CEs para que seja feita distribuição de rotas. Na topologia abaixo, os equipamentos do cliente, com AS 65000, tem sessões BGP com os PEs da operadora, com AS 1000.

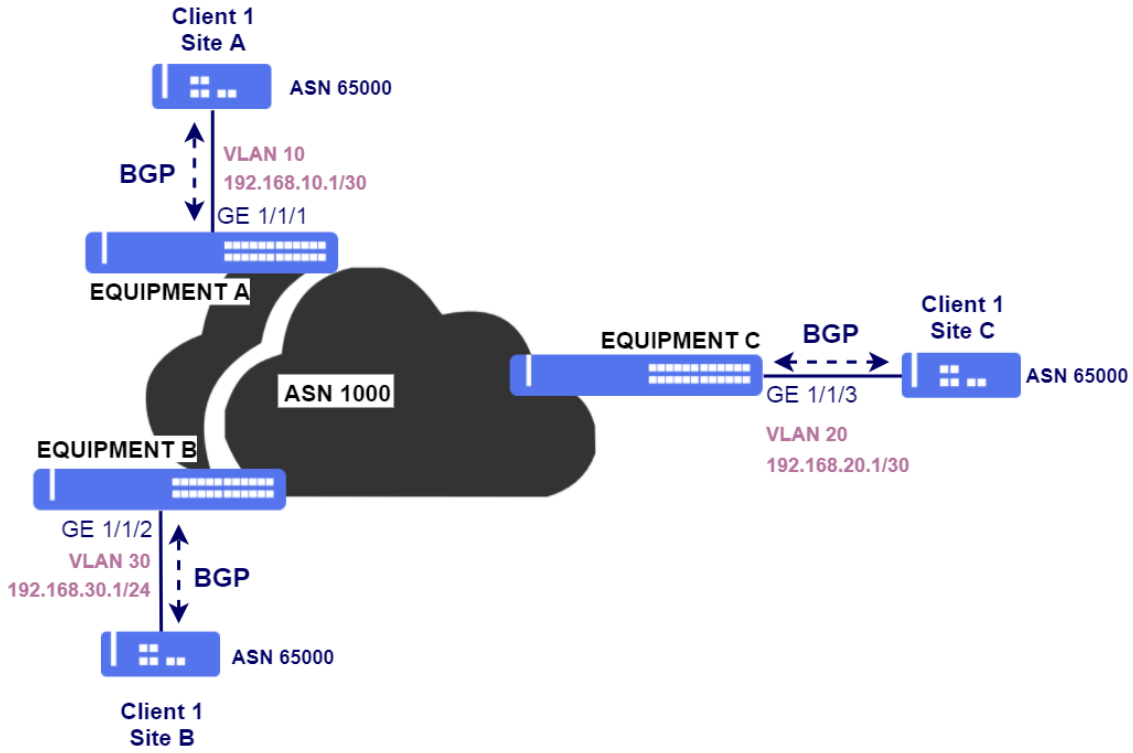

Figura 37 – L3VPN com BGP entre PE e CE

EQUIPMENT A

Configuração

```
dot1q
 vlan 10
  interface gigabit-ethernet 1/1/1
 !
!
vrf cli1
 rd 65000:10
 address-family ipv4 unicast
  route-target import 1000:65000
  !
  route-target export 1000:65000
 !
!
interface l3 VRF-CLI1-VLAN10
 vrf cli1
 lower-layer-if vlan 10
 ipv4 address 192.168.10.1/30
!
router bgp 65000
 neighbor 2.2.2.2
  update-source-address 1.1.1.1
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !
 neighbor 2.2.2.2
```

```
  update-source-address 1.1.1.1
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 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
   exit-address-family
  !
 !
!
```

EQUIPMENT B

Configuração

```
dot1q
 vlan 20
  interface gigabit-ethernet 1/1/2
 !
!
vrf cli1
 rd 65000:10
 address-family ipv4 unicast
  route-target import 1000:65000
  !
  route-target export 1000:65000
 !
!
interface l3 VRF-CLI1-VLAN20
 vrf cli1
 lower-layer-if vlan 20
 ipv4 address 192.168.20.1/30
!
router bgp 65000
 neighbor 1.1.1.1
  update-source-address 2.2.2.2
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !
 neighbor 3.3.3.3
  update-source-address 2.2.2.2
  remote-as 65500
```

```
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 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
   exit-address-family
  !
 !
!
```

EQUIPMENT C

Configuração

```
dot1q
 vlan 30
  interface gigabit-ethernet 1/1/3
 !
!
vrf cli1
 rd 65000:30
 address-family ipv4 unicast
  route-target import 1000:65000
  !
  route-target export 1000:65000
 !
!
interface l3 VRF-CLI1-VLAN30
 vrf cli1
 lower-layer-if vlan 30
 ipv4 address 192.168.30.1/30
!
router bgp 65000
 neighbor 1.1.1.1
  update-source-address 3.3.3.3
  remote-as 65500
  next-hop-self
  address-family ipv4 unicast
  !
  Address-family vpnv4 unicast
  !
 !
 neighbor 2.2.2.2
  update-source-address 3.3.3.3
  remote-as 65500
  next-hop-self
```

```
   address-family ipv4 unicast
   !
   Address-family vpnv4 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
    exit-address-family
   !
  !
!
```

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.

Configuração

```
router bgp 65000
 vrf cli1
  neighbor 192.168.30.2
   address-family ipv4 unicast
    as-override
    exit-address-family
  !
 !
!
```

Também pode ser utilizado a feature de *Allow AS In* para permitir que AS PATHs com loop sejam permitidos no PE.

Configuração

```
router bgp 65000
 vrf cli1
  neighbor 192.168.30.2
   address-family ipv4 unicast
    allow-as-in 1
    exit-address-family
  !
 !
!
```

Troubleshooting

```
show mpls l3vpn vpnv4 vrf <vrf-name> brief
show ip bgp vpnv4 labels
show ip route vrf <vrn-name>
show ip fib vrf <vrf-name> brief
show ip interface vrf <vrf-name> brief
```

14 MULTICAST

Este capítulo descreve como configurar o IGMP Snooping para aplicações Multicast.

14.1 CONFIGURANDO O 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 por *flood* para dispositivos que não queiram receber fluxos multicast.

O cenário abaixo será usado para descrever uma aplicação multicast com IGMP Snooping.

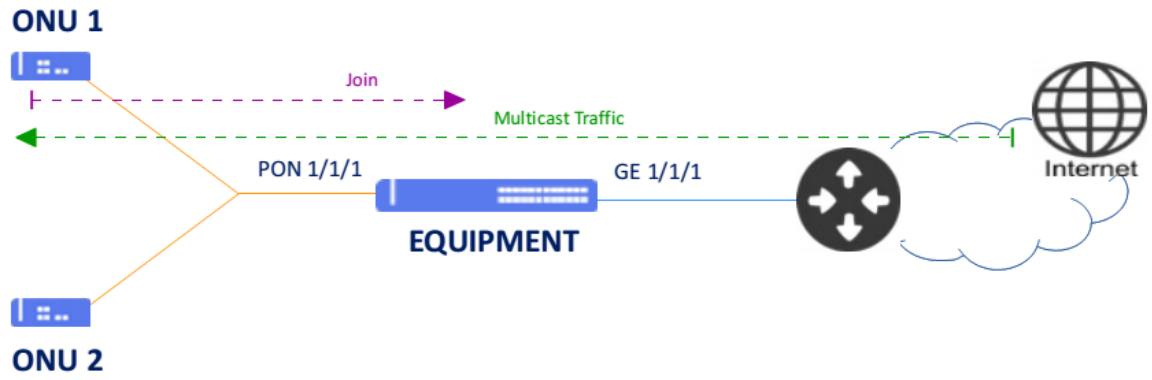

Figura 38 – Exemplo de cenário com IGMP Snooping para tráfego Multicast

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.

Configuração

```
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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do IGMP Snooping.

Troubleshooting

```
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
```

15 QoS - QUALIDADE DE SERVIÇO

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.

15.1 CONFIGURANDO O 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 divido 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*).

Configuração

```
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
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há comandos de troubleshooting para esta funcionalidade
```

15.2 Configurando o Rate Limit

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

A taxa inserida deverá estar na unidade **kbps** e 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

Configuração

```
config
qos interface gigabit-ethernet-1/1/1
 rate-limit
  ingress
   bandwidth 30000
   burst 2000
   !
  !
  egress
   bandwidth 100000
   burst 2000
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

15.3 Configurando o Policer

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) de acordo com as taxas configuradas possibilitando tomar ações diferentes conforme a classificação realizada.

O parâmetro *CBS (Commited Burst Size)* deverá estar na unidade **bytes** e a taxa *CIR (Commited Information Rate)* em **kbits/s**.

Os próximos passos irão demonstrar como configurar o *QoS Policer* limitando a banda do cliente que utiliza a **VLAN 10** para ***download*** de **15 Mbps** (15000 kbits/s) e ***upload*** de **5 Mbps** (5000 kbits/s) utilizando ***burst*** de **1 Mbps** (1000000 bytes) realizando o descarte do tráfego excedente.

Configuração

```
config
qos policer
 profile download
  mode flow
  parameters
   cir 15000
   cbs 1000000
  !
  stage egress
  actions
   red drop
  !
 !
 profile upload
  mode flow
  parameters
   cir 10000
   cbs 1000000
  !
  stage ingress
  actions
   red drop
  !
 !
 instance download
  interface ten-gigabit-ethernet-1/2/3
  profile download
  vlan 2000
 !
 instance upload
  interface ten-gigabit-ethernet-1/2/3
  profile upload
  vlan 2000
 !
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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.

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

16 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.

16.1 CONFIGURANDO O 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.

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

Configuração

```
config
switchport
 interface gigabit-ethernet-1/1/1
  storm-control
   broadcast 95
   multicast 70
   unicast 5
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

16.2 Configurando as ACLs

As ACLs (*Access Control Lists*) garantem que apenas usuários autorizados tenham acesso a recursos específicos enquanto bloqueiam tentativas não comprovadas de acessar os recursos da rede. As ACLs são usadas para fornecer controle de fluxo de tráfego, restringir o conteúdo das atualizações de roteamento, decidir quais tipos de tráfego são encaminhados ou bloqueados e, acima de tudo, fornecer segurança para a rede.

O DmOS suporta filtros de ingresso que permitem descartar (negar), encaminhar (permitir) ou alterar (definir) pacotes com base em correspondências L2 e L3. O número máximo de filtros é 512 (256 para correspondências L2 e 256 para correspondências L3) na plataforma DM4610. As ACLs suportam as seguintes correspondências:

- L2 corresponde a: 802.1p, MAC de origem e destino, Ethertype e VLAN ID
- Correspondências L3: IPv4 e DSCP de origem e destino.

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.

Configuração

```
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
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Os próximos passos irão demonstrar como configurar uma ACL L3 com prioridade 256 na interface gigabit 1/1/1 permitindo o tráfego com endereço de origem 192.168.5.10 nesta interface.

Configuração

```
config
access-list
 acl-profile ingress l3 ACL-L3 priority 256
  access-list-entry 0 match source-ipv4-address 192.168.5.10
   action permit
  !
access-list interface gigabit-ethernet-1/1/1 ingress ACL-L3
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
show acl-resources
show acl-resources brief
show acl-resources detail
show acl-resources extensive
```

16.3 Configurando o 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.

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.

Configuração

```
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 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.

Configuração

```
config
anti-ip-spoofing
 interface service-port-2
  allowed-ip all
```

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.

Configuração

```
config
anti-ip-spoofing
 interface service-port-2
  allowed-ip ipv4 address 192.10.20.1
```

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.

Configuração

```
config
anti-ip-spoofing
 interface service-port-2
  allowed-ip ipv6-all
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

Abaixo os principais comandos disponíveis para realizar a verificação do anti-ip-spoofing. O usuário deve usar a palavra-chave "do" antes do comando caso estiver no modo de configuração.

Troubleshooting

```
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>
```

16.4 Configurando o MAC Limit

O *MAC limit* é a quantidade de endereços MAC que uma interface ethernet pode aprender.

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

Os próximos passos irão demonstrar como configurar o *MAC limit* para o valor de **100 endereços MACs** na interface gigabit 1/1/3.

Configuração

```
config
mac-address-table
 interface gigabit-ethernet-1/1/3
  limit maximum 100
```

Os próximos passos irão demonstrar como configurar o *MAC limit* para o valor de **20 endereços MACs** na interface VLAN 3000.

Configuração

```
config
mac-address-table
 vlan 3000
  limit maximum 20
```

O usuário deve usar o comando **commit** para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```

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

Troubleshooting

```
Não há commandos de troubleshooting para esta funcionalidade
```

16.5 Configurando o SSH e TELNET

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*).

Os próximos passos irão demonstrar como gerar a chave RSA.

Configuração

```
config
ssh-server generate-key rsa

Really want to do this? [yes,no] yes
Generated keys
```

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.

Configuração

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

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.

Configuração

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

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

Configuração

```
config
telnet-server enabled
```

O usuário deve usar o comando commit para salvar e aplicar a configuração. É possível salvar a configuração em partes ou quando todas as alterações forem executadas.

```
commit
```