intelbras

Manual do usuário

OLT 4840 E

intelbras

OLT 4840 E
OLT EPON com 8 portas Gigabit Ethernet, 4 portas SFP/SFP+ e 4 slots para módulos SFP EPON

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

Este manual destina-se a administradores de rede e fornece informações sobre a Interface de Linha de Comandos (CLI - *Command Line Interface*).

Índice

1. Conexões no OLT

1.1. Visão geral do login no OLT

O sistema suporta várias formas de login no OLT: porta serial, Telnet, SSH.

1.2. Login no OLT

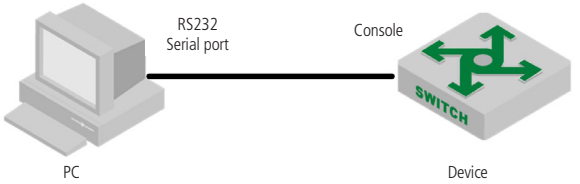
Login no OLT via porta serial

O login através da porta console é a maneira mais básica de conectar-se ao dispositivo.

Por padrão, o usuário pode fazer o login no dispositivo diretamente pela porta serial.

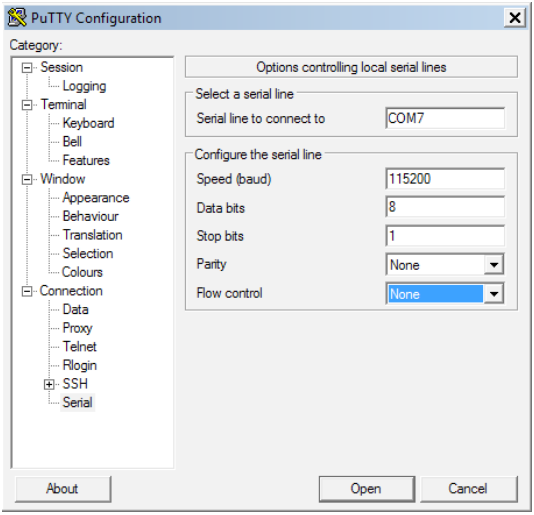
Consulte as orientações a seguir para informações específicas:

1. Conforme exibido a seguir, use um cabo serial dedicado (acompanha com produto), insira o conector DB9 do cabo na porta serial de 9 pinos do PC e, em seguida, insira o conector RJ45 na porta de console do dispositivo;



Conecte o PC na OLT via cabo serial

2. Execute o software do terminal que suporte transmissão serial, como o HyperTerminal™ ou PuTTY. Requisitos de conexão: taxa de transmissão: *115200*, bit de dados: *8*, paridade: *none*, bit de parada: *1*, controle do fluxo de dados: *none*, emulação do terminal: *detecção automática*, como exibido na figura a seguir;



Parâmetros conexão serial

3. Siga as instruções para digitar o nome do usuário e a senha e, em seguida, insira os dados do OLT. O nome de usuário padrão do OLT é *admin* e a senha padrão é *admin*. Recomenda-se que você modifique esta senha inicial após efetuar o login no dispositivo. Lembre-se da senha modificada.

Obs.: *consulte o item 2. Gerenciamento do equipamento para informações de como modificar a senha.*

Login no OLT via Telnet

Configurando o equipamento para ser o servidor Telnet

Faça o login no OLT através do Telnet e o dispositivo atuará como servidor Telnet. Por padrão, a função *Telnet-server* está habilitada e o seu IP padrão é *192.168.10.1*.

» Configuração do servidor Telnet:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-

Operação	Comando	Obrigatório/ opcional
Habilitar o servidor Telnet	**telnet** enable	Opcional
Desabilitar o servidor Telnet	**telnet** disable	Opcional
Limitação do número de usuários conectados	**telnet limit** value	Opcional
Visualização do limite de usuários conectados	**show telnet** limit	Opcional
Visualização dos clientes conectados	**show telnet client**	Opcional
Acesse o modo de execução	**enable**	-
Desconectar um usuário	**stop telnet client** [all | user-id]	Opcional
Timeout de cliente	**[no]timeout**	Opcional
Configuração de timeout de cliente	**timeout** value	Opcional

Obs.: *como um servidor Telnet, o OLT irá desconectar automaticamente os clientes que não executarem nenhuma operação por um tempo. Isto é o* timeout. *Esta função está habilitada por padrão com o valor de* 20 minutos.

Configurar o OLT como cliente Telnet para conectar-se em outros equipamentos

O usuário iniciou sessão com sucesso no dispositivo e deseja fazer login em outro dispositivo via Telnet. Atuando como cliente Telnet, o OLT deve garantir que a comunicação entre o cliente e o servidor esteja funcional para conectar-se.

» Configuração de cliente Telnet:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de execução	**enable**	-
Conexão ao servidor Telnet	**telnet[6]** server-ip [número-porta] [/localecho]	Obrigatório
Acesse o modo de configuração global	**configure terminal**	-
Função de timeout	**[no] telnetclient timeout**	Opcional
Configuração de tempo de timeout	**telnetclient timeout** value	Opcional

Login no OLT via SSH

O OLT pode atuar como um servidor SSH, mas não como um cliente.

Por padrão, esta função está desabilitada. Portanto, antes de acessar o dispositivo, você precisa fazer o login através da porta console ou via Telnet, em seguida, habilitar o servidor SSH e os outros atributos para assegurar o login.

» Configuração SSH:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilite/desabilite o SSH	**[no] ssh**	Obrigatório
Visualização das configurações SSH	**show ssh**	Opcional
Limitação do número de usuários	**[no] ssh limit** value	Opcional
Visualização do número de usuários	**show ssh limit**	Opcional
Acesse o modo de configuração privilegiado	**configure terminal**	-
Desconecte usuários	**stop vty** [all | user-id]	Opcional
Configuração de chave padrão	**crypto key generate rsa**	Obrigatório
Remover o arquivo de chaves	**crypto key zeroize rsa**	Opcional
Ativar a chave	**crypto key refresh**	Opcional
Fazer o download de uma chave externa de um servidor para este equipamento	**loadkeyfile {public | private} tftp inet[6]** server-ipfilename	Opcional
	loadkeyfile {public | private} ftp inet[6] server-ip filaname username passwd	Opcional
Fazer o upload de uma chave local para um servidor de chaves	**upload keyfile { public | private } tftp inet[6]** server-ip filename	Opcional
	upload keyfile { public | private } ftp inet[6] server-ip filename username passwd	Opcional
Visualização do arquivo de chaves	**show keyfile {public | private}**	Opcional

Obs.: » *Caso você precisar utilizar o login no OLT via SSH, o modo mais simples será:*
- » *Abrir o SSH.*
- » *Configurar uma chave padrão.*
- » *Ativar a chave.*

» *O arquivo de chaves e as configurações são salvas na memória flash e não são recompiladas.*

1.3. Interface de linha de comando

Visão geral da interface de linha de comando

O sistema fornece uma série de configurações e interfaces de linha de comando e os usuários podem configurar ou gerenciar o OLT através dela.

Recursos da interface de linha de comando:

- » Configuração local através da porta console.
- » Configuração local / remota através de Telnet e SSH.
- » Configuração da proteção hierárquica para proibir usuários não autorizados de acessar o sistema.
- » Os usuários podem digitar *?* para obter informações de ajuda a qualquer momento.
- » Fornecer comando de testes de rede, como ping, para diagnosticar se a rede está ativa.
- » Suporte FTP, TFTP, xmodem, para o cliente carregar o arquivo ou fazer o download de arquivo.

Não há necessidade dos usuários digitarem os comandos completos, porque o interpretador de linha de comando adota um método de pesquisa de correspondência incompleta. Por exemplo, o usuário pode obter o comando da *interface* digitando apenas *interf*.

Modo de configuração via linha de comando (CLI)

O modo de comando foi adotado para impedir o acesso de usuários não autorizados ao sistema. Modos diferentes dão acesso a configurações diferentes. Por exemplo, após o login, usuários de qualquer nível podem acessar o modo de usuário normal com permissão para verificar informações do sistema; no entanto, o administrador pode digitar *enable* para entrar no modo de configuração privilegiado. Sob este modo, ele pode acessar o modo de configuração global digitando o *configure terminal*. Neste modo, é possível acessar modos de comando diferentes através dos comandos correspondentes. Por exemplo, se você digitar *VLAN VLAN-list*, você entrará no modo de configuração VLAN.

A linha de comando fornece os seguintes modos de comando:

» Modo de usuário.
» Modo de configuração privilegiado.
» Modo de configuração global.
» Modo de configuração da interface Ethernet.
» Modo de configuração da VLAN.
» Modo de configuração AAA.
» Modo de configuração RADIUS.
» Modo de configuração de domínio.
» Modo de configuração da interface VLAN.
» Modo de configuração da interface SuperVLAN.

As características de cada um dos modos de comando podem ser verificadas a seguir:

» Modo de linha de comando:

Modo	Função	Prompt	Entrar no modo	Sair do modo
Modo de usuário	Visualização do sistema do OLT	OLT4840E>	Conecte-se ao OLT e insira o usuário e senha	Digite **exit** para desconectar do OLT.
Modo de configuração privilegiado	Visualização e configuração do sistema do OLT	OLT4840E#	No modo do usuário, digite **enable**	Digite **exit** para voltar para o modo *Usuário.* Digite **quit** para desconectar do OLT.
Modo de configuração global	Configura parâmetros globais	OLT4840E(config)#	No modo *Privilegiado*, digite **configure terminal**	Digite **exit end** para voltar ao modo *Privilegiado.* Digite **quit** para desconectar do OLT.
Modo de configuração de interface Ethernet	Configura parâmetros de portas Ethernet	OLT4840E(config-if-ethernet-0/1)#	No modo de configuração global, digite **interface Ethernet 0/0/1**	Digite **end** para voltar para o modo *Privilegiado.* Digite **exit** para voltar para o modo de configuração global. Digite **quit** para desconectar do OLT.
Modo de configuração de VLAN	Configura parâmetros de VLAN	OLT4840E(config-if-vlan)#	No modo de configuração global, digite **vlan2**	
Modo de configuração AAA	Configura o domínio	OLT4840E(config-aaa)#	No modo de configuração global, digite **aaa**	

Modo	Função	Prompt	Entrar no modo	Sair do modo
Modo de configuração RADIUS	Configura os parâmetros RADIUS	OLT4840E(config-radius-default)#	No modo de configuração AAA, digite **radius host default**	Digite **end** para voltar para o modo *Privilegiado*. Digite **exit** para voltar para o modo de configuração AAA. Digite **quit** para desconectar do OLT.
Modo de configuração de domínio	Configura parâmetros de domínio	OLT4840E(config-aaa-test.com)#	No modo de configuração AAA, digite **domain test.com**	
Modo de configuração de interface VLAN	Configura interface VLAN	OLT4840E(config-if-vlanInterface-22)#	No modo de configuração global, digite **interface vlan-interface 22**	Digite **end** para voltar para o modo *Privilegiado*. Digite **exit** para voltar para o modo *Global* de configuração. Digite **quit** para desconectar do OLT.
Modo de configuração de SuperVLAN	Configura interface SuperVLAN	OLT4840E(config-if-superVLANInterface-1)#	No modo de configuração global, digite **interface supervlan-interface 1**	Digite **end** para voltar para o modo *Privilegiado*. Digite **exit** para voltar para o modo *Global* de configuração. Digite **quit** para desconectar do OLT.

Compreendendo a sintaxe de comandos

Este capítulo descreve, principalmente, as etapas de configuração ao inserir a linha de comando. Por favor use este e os seguintes capítulos para informações detalhadas sobre como usar a interface de linha de comando.

A autenticação de login do console do sistema é principalmente para operar a identidade do usuário. Ele faz uma verificação através de usuário e senha, para permitir ou negar um login.

» **O primeiro passo:** quando o seguinte prompt de login aparecer na interface da linha de comando:

'Username (1-32 chars):'

Digite o nome do usuário de login e pressione o botão *Enter* e, em seguida, o prompt exibirá:

'Password (1-16 chars):'

Introduza a senha de login, se ela estiver correta, você pode acessar o modo de usuário normal, o prompt informará:

OLT4840E>

Existem duas permissões diferentes no sistema OLT. Um é o privilégio de administrador e a outra são permissões comuns de usuários. Usuários comuns geralmente só podem ver as informações de configuração, sem o direito de modificá-los. No entanto, o administrador pode usar comandos específicos para alterar as configurações do OLT.

Se você realizar o login como administrador do sistema, acesse o modo de usuário privilegiado a partir do modo de usuário comum, conforme exibido:

OLT4840E> enable

OLT4840E#

» **O segundo passo:** digite o comando.

Se o comando que você inserir não requerer outros parâmetros, você pode pular para a terceira etapa. Caso contrário, continue com as seguintes etapas:

» Se o comando requerer um parâmetro, insira-o. Você pode ter que incluir palavras-chave antes deles para definir o que será configurado.

» Geralmente, seu valor é especificado pelo seu tipo. Isto é: um valor numérico dentro de um determinado escopo, ou uma informação de texto, ou um endereço IP. Se você tiver alguma dúvida, você pode digitar *?*, para então, inserir o valor correto de acordo com o prompt. Palavras-chave referem-se ao o que será configurado no comando.

» Se o comando requerer múltiplos parâmetros, insira palavras-chave e cada valor de acordo com o prompt de comando até aparecer a indicação *<enter>*. Após isso, pressione a tecla *<enter>* para terminar este comando.

» **O terceiro passo:** digite o comando completo e em seguida pressione a tecla *<enter>*.

Por exemplo:

! O usuário não precisa inserir parâmetros

OLT4840E # quit

quit é um comando sem parâmetros. *quit* é o nome do comando, pressionando *<enter>*, o comando será executado.

! Os usuários devem inserir parâmetros

OLT4840E (config) #vlan 3

VLAN 3 é um comando com parâmetro e palavra-chave. *VLAN* é a palavra-chave e *3* é o valor do parâmetro.

Ajuda de sintaxe

Há uma ajuda de sintaxe na interface de linha de comando. Se você não tem certeza da sintaxe de comando, você pode inserir *?* em qualquer momento, ou você pode obter todos os comandos e suas descrições do modo de comando ativo através do comando *help*; insira o comando (ou apenas parte dele) que deseja e em seguida digite *?* e o sistema listará todas as palavras-chave começando com este texto. Se você digitar *?* no lugar de uma palavra-chave, a linha de comando listará todas as palavras-chave e uma breve descrição; se você digitar *?* no lugar de um parâmetro, a linha de comando listará uma orientação do parâmetro que deve ser inserido. Você pode digitar comandos de acordo com a ajuda até o comando prompt exibir *<enter>*, neste momento, o que você deve fazer é apenas apertar a tecla *<enter>* para executar o comando.

Por exemplo:

1. Digite *?* no modo de privilégio, para aparecer:
   OLT4840E #?
   System mode commands:
   cls clear screen
   help description of the interactive help
   ping ping command
   quit disconnect from switch and quit
   ……

2. Digite *?* logo após palavras-chave incompletas:
   OLT4840E (config) #interf?
   Interface
3. Digite *?* após um comando e um caractere de espaço:
   OLT4840E (config) # spanning-tree?

forward-time	config switch delaytime
hello-time	config switch hellotime
max-age	config switch max agingtime
priority	config switch priority
<enter>	The command end.

4. Formato/intervalo dos parâmetros:
   OLT4840E(config)#spanning-tree forward-time ?
   INTEGER<4-30> switch delaytime: <4-30>(second)
5. Ending prompt command line:
   OLT4840E(config)#spanning-tree ?
   <enter> The command end.
   OLT4840E #?

Comando de histórico

Os comandos inseridos pelos usuários podem ser salvos automaticamente pela CLI e você pode invocá-los ou executar novamente a qualquer momento. O buffer de histórico de comandos é definido previamente como 100. Ou seja, é possível armazenar no máximo 100 comandos de histórico para cada usuário.

Você pode acessar o último comando digitando *Ctrl + P*; você pode acessar o próximo comando digitando *Ctrl + N*.

Tipos de parâmetros de comando

Existem 5 tipos de parâmetros:

» Integer (inteiro).

Os dois números nos colchetes angulares (<>), conectados pelo hífen (-) significam que esse parâmetro é o número inteiro entre esses dois números.

Por exemplo: INTEGER <1-10> significa que o usuário pode digitar qualquer número inteiro maior ou igual a 1 e menor ou igual a 10, como 8.

» IP Address (endereço IP).

A.B.C.D significa um endereço de IP

Por exemplo: 192.168.0.100 é um IP válido.

» MAC Address (endereço MAC).

H:H:H:H:H:H significa um endereço MAC. Se um endereço MAC multicast for necessário, será apresentado um endereço correspondente do prompt.

Por exemplo: 01:02:03:04:05:06 é um endereço MAC válido.

» Interface list (lista de interface).

A lista de interface é solicitada como STRING <3-4>. A interface do parâmetro da porta consiste no tipo de porta e no número da porta. O tipo de porta é Ethernet e o número da porta é slot-num/port-num. *Slot-num* significa número do slot, o intervalo de dados é 0-1; *Port-num* é o número da porta no slot, o intervalo de dados é de 1-12. Um parâmetro de porta *interface-list* significa múltiplas portas. Portas em série do mesmo tipo podem ser conectadas escrevendo *to*, mas o número da porta atrás do *to* deve ser maior do que o da frente, e esse argumento só pode ser repetido até 3 vezes. A declaração especial da lista da interface do parâmetro da interface será exibida no comando.

Por exemplo: **show spanning-tree interface ethernet 0/1 ethernet 0/3 to ethernet 0/5**

Significa mostrar a informação de spanning-tree sobre as interfaces Ethernet 0/1, Ethernet 0/3, Ethernet 0/4 e Ethernet 0/5.

» String.

Se o prompt apresentar STRING <1-19> significa um texto que pode variar de 1 caractere a 19 caracteres. Digite *?* para verificar a descrição do parâmetro deste comando.

Mensagens de erro

Mensagem no prompt	Explicação do erro	Causa	Solução
Incomplete command	O comando está incompleto e o sistema não pôde reconhecê-lo	Pode haver mais de um comando no sistema. O sistema não pôde reconhecer a abreviação. O comando não está completo e é necessário inserir mais parâmetros.	Digite *?* para visualizar a tabela de comandos disponíveis ou digite o comando completo.
Invalid parameter	Parâmetro inválido	Parâmetro fora do intervalo permitido pelo comando.	Verifique o intervalo do parâmetro e o reinsira.
Unrecognized command	Você digitou um comando errado e o sistema não pôde reconhecê-lo	Erros de digitação, ou um comando que não existe no sistema.	Digite *?* para ver a lista de comandos disponíveis.

2. Gerenciamento do equipamento

2.1. Visão geral das funções de gerenciamento de funções

Faça o login no OLT para executar a configuração de gerenciamento, deve ser feita a autenticação e a autorização para impedir acesso ilegal de usuários e/ou acessos não autorizados. A gestão de usuários é o gerenciamento na autenticação e autorização de usuários. Se esta função é executada pelo próprio sistema do OLT, ela é chamada de autenticação local. Se é realizada por um sistema diferente do sistema do OLT (geralmente através de um servidor de autenticação, como o servidor do RADIUS), ela é chamada de autenticação remota. O conteúdo de gerenciamento de usuário neste capítulo refere-se à autenticação local.

O OLT possui três tipos de permissões:

» Usuário comum.

  Usuários comuns têm o nível de privilégio mais baixo. Eles só podem acessar o modo de execução e ver as informações do sistema. No entanto, eles não podem fazer outras alterações e não podem modificar suas próprias senhas.

» Usuário administrador.

Os administradores não só têm os direitos dos usuários comuns, mas também podem configurar o OLT e modificar suas próprias senhas. No entanto, eles não podem criar usuários e modificar a senha de outros.

» Superusuário.

O superusuário é o usuário padrão do sistema: *admin*. O sistema possui apenas um superusuário e ele não pode ser excluído. O superusuário tem todas as permissões: pode fazer qualquer configuração OLT, criar usuários, modificar a sua própria senha e as senhas de outros usuários, excluir usuários e assim por diante. A senha padrão para o usuário admin é *admin*. Todas as configurações citadas neste manual utilizam o usuário *admin*, a não ser que esteja explicitado de outra forma.

Configuração de gerenciamento de usuários

O sistema pode criar até 15 usuários. Após você acessar o equipamento como usuário admin, você pode adicionar novos usuários, modificar suas senhas, modificar seus direitos, excluir contas, limitar os métodos de login e assim por diante. Usuários comuns não podem modificar suas próprias senhas. Os administradores podem modificar suas próprias senhas, mas não podem modificar as senhas de outros usuários. Os super usuários podem modificar a senha de qualquer usuário. Além disso, pode visualizar as informações das configurações dos usuários em todos os modos.

Permissões: *0-1* para usuário comum, *2-15* para usuário administrador. Para o super usuário (admin) não é necessária configuração. Se você não inserir um valor de permissão ao criar um usuário, o sistema irá atribuí-lo automaticamente com permissões de usuário comum.

Por padrão, o usuário pode fazer o login via porta serial, SSH, Telnet.

Até 5 usuários podem estar *online* ao mesmo tempo.

» Configuração do gerenciamento de usuários:

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Crie usuários	**username** username privilege pri-value **password** { 0|7 } password	Opcional
A senha do usuário é salva em texto criptografado	**service password-encryption**	Opcional

Operação	Comando	Obrigatório/ opcional
Modificar a senha do usuário	**username change-password**	Opcional
Modificar a permissão do usuário	**username change-privilege-pwd** { 0|7 } password	Opcional
Remover usuário	**no username** username	Opcional
Configuração do modo de login	**username** username **terminal** { all | console | ssh | telnet | none }	Opcional
Configuração do limite de usuários conectados	**username online-max value**	Opcional
Visualização das configurações dos usuários	**show username [**username**]**	Opcional
Visualização dos usuários	**show users**	Opcional
Acesse o modo de execução	**enable**	-
Desconecte usuários manualmente (modo *Forçado*)	**stop {username |vty [all | user-id] }**	Opcional
Configuração do tempo de timeout	**[no]timeout value**	Opcional

Obs.: *quando você cria um usuário, o tipo de senha é dividido em 0 e 7, 0 significa que a senha está em texto simples, 7 significa que a senha é um texto criptografado. Portanto, quando você cria um usuário, o tipo de senha deve ser 0. Quando você configura criptografia de senha do serviço, a senha configurada em texto simples, torna-se sem criptografia na decompilação e o tipo de senha desencriptada muda para 7.*

Por exemplo:

» Crie o usuário test, com a senha 123, e salve a senha em texto simples:
OLT4840E(con1fig)#username test privilege 0 password 0 123

Add user successfully.

OLT4840E(config)#show running-config oam

![OAM]

username test privilege 0 password 0 123

ipaddress 192.168.1.1 255.255.255.0 0.0.0.0

» Salve a senha do usuário em texto criptografado:
OLT4840E(config)#service password-encryption

OLT4840E(config)#sh running-config oam

![OAM]

service password-encryption

username test privilege 0 password 7 884863d2

ipaddress 192.168.1.1 255.255.255.0 0.0.0.0

Salvando a senha em texto criptografado, você pode reduzir o risco de roubo de senhas.

Mecanismo de silenciamento

Mecanismo de silenciamento do sistema: se os tempos de falhas consecutivas de login excederem o valor permitido, o usuário não poderá tentar fazer login por um determinado período de tempo. A função está desativada por padrão, e a configuração para tempos de tentativas de login com falha está habilitada.

» Mecanismo de silêncio:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Configuração de limite de tentativas consecutivas de logins sem sucesso	**[no] username failmax** {fail-value | username fail-value}	Obrigatório
Configuração de tempo de silêncio	**username silent-time** value	Opcional
Visualização de configuração de silêncio	**show username silent**	Opcional

2.2. Autenticação de senha de segundo nível

Visão geral para autenticação de senha de segundo nível

Normalmente, os usuários normais só podem entrar no modo de execução e não podem acessar outros modos de configuração. Além disso, os usuários normais só podem visualizar as informações de configurações e não podem modificá-las. A autenticação de senha de segunda camada fornece o mecanismo para aumentar a autoridade dos usuários normais, se eles passarem na autenticação de segunda camada, eles adquirem privilégios de administrador, ou seja, podem ter autoridade para realizar outras operações.

Esta autenticação inclui autenticação local e autenticação remota. Se o gerenciamento de usuários é local, a autenticação de senha de segunda camada também será local. Da mesma forma, se o gerenciamento de usuários usa autenticação remota, a autenticação de senha de segunda camada também usará a autenticação remota. O gerenciamento de usuários e a autenticação de senha usam o mesmo servidor de autenticação.

Configuração de senha de autenticação de segundo nível

A função de autenticação de senha de segundo nível está desativada por padrão. Se o usuário local (nível de privilégio 0-1) logar no OLT e tentar entrar no modo *Privilegiado*, o sistema solicita uma senha. Digite a senha secundária e em seguida a autenticação será executada. Se você estiver usando autenticação remota, quando um usuário comum (nível de privilégio 0-1) logar no OLT e tenta entrar no modo *Privilegiado*, o OLT usa automaticamente o nome do usuário e a senha configurada para autenticação de senha de segundo nível para executar a autenticação. Se a autenticação passar, a autenticação de senha de segunda camada é considerada bem-sucedida.

Ao usar a autenticação remota, consulte o Manual do Usuário na Autenticação Remota para a sua configuração.

» Configuração de senha de autenticação de segundo nível:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
(Des)Habilite a função	**[no] username privilege-auth**	Obrigatório
Configuração de senha de segundo nível	**username change-privilege-pwd {0|7}** senha	Obrigatório
Configuração de usuário de autenticação de segundo nível	**[no] username privilege-auth-user** usuário	Obrigatório
Visualização de configurações de autenticação de segundo nível	**show username privilege-auth**	Opcional

Obs.: *se a senha for selecionada como 0, ela indica que a senha está em texto simples. Se você selecionar 7, a senha é texto criptografado. Você deve usar o texto simples correspondente para autenticação.*

Exemplo de configuração para autenticação de segundo nível

Requisitos de rede

Os usuários normais acessam o OLT através do terminal da porta serial e possuem os privilégios de administrador após passar a autenticação de senha secundária.

Passos para configuração

» Utilize o usuário admin para fazer o login e crie um usuário normal: test/test.
OLT4840E(config)#username test privilege 0 password 0 test

» Se a autenticação de segundo nível não estiver configurada, faça o login como um usuário normal.
OLT4840E(config)#quit

Username:test

Password:**** (Senha: test)

» Após realizar o login, faça uma tentativa de acesso ao modo *Privilegiado*, esta tentativa deve falhar.
OLT4840E>en

OLT4840E>en

» Realize novamente o login como admin para configurar os parâmetros de autenticação de segundo nível.

» Habilite a autenticação de segundo nível.
OLT4840E(config)#username privilege-auth

» Configure o usuário da autenticação de segundo nível.
OLT4840E(config)#username privilege-auth-remote-user testtest

» Configure a senha do usuário da autenticação de segundo nível (quando o usuário acessar o modo *Privilegiado*, esta senha será solicitada).
OLT4840E(config)#username change-privilege-pwd 0 123456

Please input your login password : **** (Verifique se você possui os privilégios)

Change password successfully.

» Realize novamente o login utilizando o usuário test/test.
OLT4840E(config)#quit

Username:test

Password:**** (senha: test)

» Tente acessar o modo *Privilegiado* e insira a senha solicitada.

OLT4840E>

» Digite a senha do usuário normal *test*. O sistema irá informar que a senha está errada.

OLT4840E>enable

Please input password : **** (senha: test)

Password is error.

OLT4840E>

» Digite a senha de autenticação de segundo nível correta: 123456. O sistema irá permitir o acesso e você terá acesso ao modo *Privilegiado* e ao modo *Global*, podendo modificar outros parâmetros do sistema.

OLT4840E>enable

Please input password : ****** (enter the password of second-tier password authentication:

123456)

OLT4840E#configure terminal

OLT4840E(config)#

2.3. Autenticação remota

As informações do usuário podem ser salvas no banco de dados do OLT ou salvas em um servidor externo, conhecidos por servidores de autenticação, como o servidor RADIUS, TACACS+. As informações dos usuários são armazenadas no OLT local, se o OLT não puder completar a autenticação local, ele deve autenticar através do servidor, esta é a autenticação remota. Ao usar a autenticação remota, assegure-se de que a comunicação entre o OLT e o servidor esteja funcional e que o usuário que fez login está configurado no servidor de autenticação.

Configuração do modo de autenticação

A autenticação local (padrão) e remota são usadas para a autenticação do sistema OLT. Ambas modalidades podem ser usadas em combinação e a autenticação remota terá precedência. Além disso, a autenticação local é executada somente quando a autenticação remota falhar. A autenticação remota suporta autenticação RADIUS e autenticação TACACS +.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração para utilizar autenticação local	**muser local**	Opcional (configuração padrão)
Configuração para utilização de servidor RADIUS remoto	**muser radius** radius-name { pap | chap } [[account] local]	Opcional
Configuração para utilização de servidor TACACS+ remoto	**muser tacacs+** [[author] [account] [command-account] [local]]	Opcional
Visualização de configurações de autenticação	**show muser**	Opcional

Configuração de autenticação RADIUS remota

» Configuração da autenticação RADIUS remota:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração para utilização de servidor RADIUS remoto	**muser radius** radius-name { pap | chap } [[account] local]	Obrigatório
Visualização de configurações de autenticação	**show muser**	Opcional

» Configuração de servidor RADIUS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração AAA	**Aaa**	Obrigatório
Configuração do nome do servidor RADIUS	**radius host** radius-name	Obrigatório
Configuração do servidor de autenticação RADIUS	**{primary-auth-ip | second-auth-ip }** ip-addressauth-port	Obrigatório

Operação	Comando	Obrigatório/ opcional
Configuração da chave de autenticação RADIUS	**auth-secret-key** key-value	Obrigatório
Configuração do servidor de contas RADIUS	**{ primary-acct-ip | second-acct-ip }** ip-address acct-port	Obrigatório
Configuração de chave de contas RADIUS	**auth-secret-key** key-value	Obrigatório
Configuração de troca para o servidor primário após falha	**preemption-time** value	Opcional, *0* por padrão (significa que não será trocado)
Visualização de configurações	**show radius host** [radius-name]	Opcional

» Configuração de domínio:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração AAA	**Aaa**	Obrigatório
Configuração do nome do domínio RADIUS	**domain** domain-name	Opcional
Vínculo do domínio com o servidor RADIUS	**radius host binding** radius-name	Obrigatório
Ativação do domínio	**state active**	Obrigatório
Desativar o domínio	**state block**	Opcional, configuração padrão
Configuração de domínio padrão	**default domain-name enable** domain-name	Opcional, modo de configuração AAA
Remover domínio padrão	**default** domain-name **disable**	Opcional, modo de configuração AAA
Visualização de configurações	**show domain** [domain-name]	Opcional

Configuração de autenticação TACACS+ remota

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração para utilização de servidor TACACS+ remoto	**muser tacacs+ [** [author] [account] [command-account] [local] **]**	Obrigatório
Visualização da criptografia do password	**[no] tacacs+ encrypt-key**	Opcional, visualização de texto simples por padrão
Configuração de tipo de autenticação	**tacacs+ authentication-type** ascii | chap | pap	Opcional, por padrão *ASCII*
Configuração do servidor TACACS+	**tacacs+** { primary | secondary } **serverip-address** [keyvalue] [portport-number] [timeout value]	Obrigatório
Configuração de troca para o servidor primário após falha	**tacacs+ preemption-time** value	Opcional, *0* por padrão (significa que não será trocado)
Visualização de configurações de autenticação TACACS+	**show tacacs+**	Obrigatório

Exemplo de configuração de autenticação remota

» Requisitos de rede:

Aqui, apenas o TACACS + é usado como servidor de autenticação. Para a configuração do servidor RADIUS de autenticação, consulte o manual 802.1x.

» Antes da autenticação, verifique se o OLT pode comunicar-se com o servidor de autenticação.

» O usuário de login existe no servidor de autenticação.

» Os parâmetros configurados no OLT são os mesmos do servidor de autenticação, como a chave e o número da porta.

» Exemplo de configuração:

» Configure os parâmetros relacionados do servidor TACACS+.

» Configure o tipo de autenticação (o tipo padrão *ascii* é opcional).

OLT4840E (config) # tacacs+ authentication-type ascii

» Configure o endereço e a chave do servidor de autenticação mestre.
OLT4840E (config) # tacacs+ primary server 192.168.1.10 key 123456

» Configure o endereço e a chave do servidor de autenticação escravo (não é necessária nenhuma configuração quando não há servidor de backup).
OLT4840E (config) # tacacs+ secondary server 192.168.1.11 key 123456

» Configure para usar o servidor mestre após a recuperação de falhas do servidor mestre (nenhuma configuração é necessária quando não há servidor de backup).
OLT4840E (config) # tacacs+ preemption-time 20

» Exibir a informação:
OLT4840E (config) #show tacacs+

Primary Server Configurations:

IP address: : 192.168.1.10

Connection port: : 49

Connection timeout: : 5

Key: : 123456

Secondary Server Configurations:

IP address: : 192.168.1.11

Connection port: : 49

Connection timeout: : 5

Key: : 123456

» Configure para usar tacasc + para executar autenticação remota:
OLT4840E (config) # muser tacacs+

2.4. Limitação de IP

Visão geral de limitação de IP

A limitação de IP restringe o IP dos usuários que efetuam login no OLT, ou seja, apenas os usuários com IP específicos possuem acesso. A limitação de IP pode melhorar a segurança do sistema.

Configuração de limitação de IP

Por padrão, não há restrição, ou seja, qualquer IP pode acessar o OLT, desde que o nome de usuário e a senha estejam corretos. Se você precisa permitir que os usuários com o IP específico acessem o OLT, primeiro você deve configurá-lo para não permitir o acesso de qualquer IP e em seguida, configurar os endereços IP permitidos.

A configuração para o acesso do usuário Telnet também se aplica aos usuários via SSH.

» Configuração de limitação de IP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o acesso a qualquer IP	**login-access-list** [snmp | telnet] 0.0.0.0 [0.0.0.0 | 255.255.255.255]	Opcional, configuração padrão
Proibir acesso de todos os IPs	**no login-access-list** [all | telnet | snmp | software]	Obrigatório
Habilitar acesso de IPs específicos	**login-access-list** [snmp | telnet | software] ip-address mask	Obrigatório
Visualização de configurações	**show login-access-list**	Opcional
Limitação do número de usuários simultâneos online através de Telnet no modo *Privilegiado*	**login-access-list telnet-limit user-number**	Opcional, *5* por padrão

Exemplo de configuração

» Requisitos de rede:

OLT IP = 192.168.1.1 / 24, só permite o segmento de rede 192.168.1.0/24 IP através do OLT de gerenciamento de login Telnet.

» Passos de configuração:

» Verifique a configuração padrão: todos os IPs podem fazer login no OLT através do Telnet.

OLT4840E (config) #show login-access-list

sno ipAddress wildcard bits terminal

1 0.0.0.0 255.255.255.255 snmp

2 0.0.0.0 255.255.255.255 web

3 0.0.0.0 255.255.255.255 telnet

total [3] entry.

» Não permita que nenhum IP faça Telnet para o OLT:
OLT4840E (config) #no login-access-list telnet all

» Configure para permitir que a rede 192.168.1.0/24 acesse o OLT via Telnet:
OLT4840E (config) # login-access-list telnet 192.168.1.0 0.0.0.255

OLT4840E (config) #show login-access-list

sno ipAddress wildcard bits terminal

1 0.0.0.0 255.255.255.255 snmp

2 0.0.0.0 255.255.255.255 web

3 192.168.1.0 0.0.0.255 telnet

Total [3] entry.

2.5. Configuração de timeout

Visão geral de timeout

O usuário que faz o login via Telnet, SSH, console terminal, se estiver logado por um longo período de tempo, mas não executar nenhuma operação, além de tornar o ambiente inseguro estará consumindo carga da CPU, podendo afetar a performance do equipamento. Portanto, se o usuário conectado não estiver ativo por um longo período de tempo, o sistema automaticamente o força a sair, função conhecida como timeout.

Configuração de timeout

Operação	Comando	Obrigatório/ opcional
Acesse o modo *Privilegiado* de configuração	**enable**	-
Habilite e configure o tempo de timeout	**timeout** min	Opcional, habilitado por padrão com valor de *20 minutos*
Desabilite a função *Timeout*	**no timeout**	Opcional
Visualização de configuração de timeout	**show running-config oam**	Opcional

Obs.: *a configuração de timeout apenas aceita os efeitos no Telnet, SSH, console terminal.*

3. Configuração de porta

3.1. Configurações básicas de porta

Estas configurações são aplicadas apenas às portas Ethernet.

Acessar o modo de configuração de porta

» Habilitar porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface** {ethernet|pon} port-number	Obrigatório
Acesse o modo de configuração em massa	**interface range** {ethernet | pon} port-number **to** {ethernet | pon} port-number	Opcional

Habilitar a porta

Por padrão, todas as portas estão habilitadas, ou seja, a porta estará no estado de linkup se o OLT estiver ativo. No entanto, certas portas poderão ser desabilitadas e entrarão em estado de linkdown por razões de segurança.

» Habilitar porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface** {ethernet|pon} port-number	-
Habilita porta	**no shutdown**	Opcional, configuração padrão
Desabilitar porta	**shutdown**	Opcional
Visualização detalhada da porta	**show interface** {ethernet | pon} port-number	Opcional
Visualização resumida da porta	**show interface brief ethernet** [port-number]	Opcional

Descrição de interface

» Descrição de interface:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface** {ethernet|pon} port-number	-
Configuração de descrição de interface	**description**	Opcional
Remover descrição de interface	**no description**	Opcional, configuração padrão
Visualização da descrição da interface	**show description interface** [{ethernet | pon} port-number]	Opcional
Visualização detalhada da descrição da interface	**show interface** {ethernet | pon} port-number	Opcional
Visualização resumida da descrição da interface	**show interface brief ethernet** [port-number]	Opcional

Modo *Duplex*

» Modo *Duplex*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface** {ethernet|pon} port-number	-
Configuração de modo *Duplex*	**duplex** {auto | full | half}	Opcional
Restauração de modo *Padrão*	**no duplex**	Opcional, configuração padrão *auto*
Visualização detalhada da descrição da configuração	**show interface** {ethernet | pon} port-number	Opcional
Visualização resumida da descrição da configuração	**show interface brief ethernet** [port-number]	Opcional

Taxa de transmissão da interface

» Taxa de transmissão da interface:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface** {ethernet|pon} port-number	-
Configuração de taxa de transmissão da interface	**speed** {10auto | 10 | 100auto |100 |1000auto | 1000 |10000 | auto}	Opcional
Restauração de taxa de transmissão da interface	**no speed**	Opcional, configuração padrão automática
Visualização detalhada da descrição da configuração	**show interface** {ethernet | pon} port-number	Opcional
Visualização resumida da descrição da configuração	**show interface brief ethernet** [port-number]	Opcional

Obs.: *interfaces diferentes suportam taxas de transmissão diferentes, por exemplo, a porta óptica de 10G só suporta as taxas de 1000 e 10000.*

Modo *Controle de Taxa*

Quando duas portas gigabit estão conectadas e suas taxas estão configuradas no modo *Forçado*, essas duas portas devem estar no modo *Mestre* e no modo *Escravo*, respectivamente, de modo a tornar o encaixe bem-sucedido.

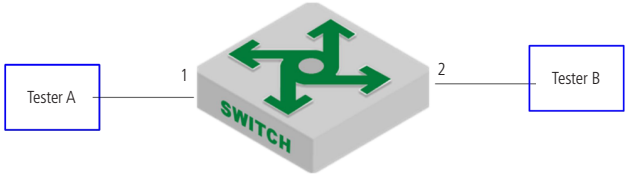
» Modo *Controle de taxa*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**Interface** {ethernet|pon} port-number	-
Configuração de modo *Mestre*	**port-control mode master**	Obrigatório
Configuração de modo *Escravo*	**port-control mode slave**	Obrigatório
Restaurar autonegociação	**no port-control mode**	Opcional, configuração padrão
Visualização das configurações	**show port-control mode**	Opcional

Exemplo de configuração

» Requisitos de rede:

Configure a descrição da porta 1: teste: modifique a prioridade para 7, configure a interface apenas aceitar frames com tag, desative a filtragem de entrada.



OLT

» Passos de configuração:

» Configure a descrição.

OLT4840E (config) #interface ethernet 0/1

OLT4840E (config-if-ethernet-0/1) #description test

» Modificar a prioridade.

OLT4840E (config-if-ethernet-0/1) #priority 7

» Configure a interface para aceitar apenas frame com tag.

OLT4840E (config-if-ethernet-0/1) #ingress acceptable-frame tagged

» Desativar filtro de entrada.

OLT4840E (config-if-ethernet-0/1) #no ingress filtering

» Crie a VLAN 100 e configurar a interface ethernet 2 como modo *Trunk*.

OLT4840E (config) #vlan 100

OLT4840E (config-if-vlan) #switchport ethernet 0/2

OLT4840E (config-if-vlan) #interface ethernet 0/2

OLT4840E (config-if-ethernet-0/2) #switchport mode trunk

» Validação do resultado.

» O tester A encaminha a mensagem da VLAN 100 para a porta 1, e a porta do tester pode ser capaz de receber a mensagem da VLAN 100.

» O tester A encaminha a mensagem não marcada para a porta 1 e a porta 1 descarta a mensagem sem tag.

3.2. Configuração de agregação de portas

Visão geral de agregação de portas

A agregação de portas é a função utilizada para agrupar várias portas físicas para formar um grupo de agregação, com intenção de implementar um balanceamento de carga e um backup redundante de links.

A configuração básica das portas em um grupo de agregação deve ser consistente. Ela inclui STP, VLAN, atributos de porta e assim por diante.

- As configurações STP incluem: ativação/desativação, prioridade e custo do STP.
- As configurações de VLAN incluem: a porta que permite a VLAN, porta PVID.
- A configuração dos atributos da porta são: a velocidade da porta, o modo *Duplex* (deve ser full duplex) e o tipo de link (isto é, trunk, híbrido e acesso). Todos devem ser correspondentes.

Em um mesmo OLT, se esses atributos de uma porta de um grupo forem modificados, as outras portas serão sincronizadas automaticamente.

Existem diferentes modos de agregação, e elas podem ser classificadas em LACP estático e dinâmico.

Existem três tipos de modelos de protocolo:

- **Modo *Estático* (ligado):** não executa o protocolo LACP (apenas pode se conectar com outro modo *Estático*).
- **Modo *Ativo dinâmico*:** no modo *Ativo*, a porta inicia automaticamente a negociação LACP (pode se conectar com modo *Ativo* ou *Passivo*).
- **Modo *Passivo dinâmico*:** no modo *Passivo*, uma porta apenas responde à negociação LACP (apenas pode se conectar com modo *Ativo*).

Configuração de ID do grupo de agregação

A mesma porta não pode se conectar a múltiplos IDs ao mesmo tempo. Se um membro existe em um grupo de agregação, você não pode excluí-lo diretamente, antes é preciso remover seus membros.

Você pode criar diretamente um ID de agregação no modo de configuração global ou criar automaticamente ao adicionar uma porta a um grupo de agregação.

» Configuração de ID LACP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do ID do grupo de agregação	**[no] channel-group** ch-id	Opcional

Configuração do grupo de agregação

A agregação de portas inclui estática e dinâmica. *ON* (ligado) refere-se a agregação estática, ela não realiza a negociação LACP e seu grupo pode ter até 8 portas membro.

active (ativo) ou *passive* (passivo) refere-se à agregação dinâmica. Um LACP dinâmico pode conter até 12 membros, 8 dos quais estão no estado bandl e os outros quatro estão no estado de backup. Somente os membros com status de bandl encaminharão o tráfego normal. Quando os membros *bandl* apresentarem falha na conexão, a porta de backup com a maior prioridade se tornará bandl.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de interface	**interface ethernet** port-number	-
Adicionar uma porta a um grupo de agregação	**channel-group** ch-id **mode** {on | active | passive}	Obrigatório
Remover uma porta do grupo de agregação	**no channel-group** ch-id	Opcional
Visualização das informações de grupo de agregação	**show lacp internal** [ch-id]	Opcional
Visualização das informações vizinhas ao grupo de agregação	**show lacp neighbor** [ch-id]	Opcional

Configuração da política de balanceamento de carga

Depois que o grupo de agregação entrar em vigor, ele encaminhará o fluxo de serviço entre os membros da LACP de acordo com determinadas políticas. O balanceamento de carga padrão usa o src-mac e pode ser modificado. Não há nenhum comando para visualizar a política de carga separadamente. Você pode encontrar as informações de configuração via *show lacp internal [ch-id]*.

» Configuração da política de balanceamento de carga:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da política de balanceamento de carga (para todos os grupos)	**channel-group load-balance** {src-mac | dst-mac | src-dst-mac | src-dst-ip | src-ip | dst-ip }	Opcional
Configuração da política de balanceamento de carga (grupo específico)	**channel-group** ch-id **load-balance** {src-mac | dst-mac | src-dst-mac | src-dst-ip | src-ip | dst-ip }	Opcional
Restaurar a política padrão	**no channel-group load-balance**	Opcional

Configuração de prioridade do sistema

No modo *LACP dinâmico*, o OLT master (mestre) e o OLT slave (escravo) são selecionados de acordo com o ID do sistema. Ele é determinado pela prioridade do sistema e pelo endereço MAC local. Para selecionar o OLT master (mestre) e o OLT slave (escravo), é comparado a prioridade em primeiro lugar, o valor menor ganha; também é comparado o MAC, o menor ganha.

A prioridade padrão do sistema é *32768*.

» Configuração de prioridade do sistema:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da prioridade do sistema	**lacp system-priority** value	Opcional
Restaurar a configuração padrão	**no lacp system-priority**	Opcional
Visualização da prioridade do sistema	**show lacp sys0id**	Opcional

Configuração de prioridade de porta

Quando um LACP dinâmico está sendo executado, o OLT master (mestre) seleciona a porta lógica de acordo com o seu ID, que consiste em sua prioridade e o seu número. A porta lógica no LACP é usada para encaminhar pacotes de protocolo, como o STP.

Quando o OLT master (mestre) seleciona a porta lógica: primeiramente, é comparada a prioridade, o valor menor ganha; se a prioridade for a mesma, então compara-se o número da porta, o valor menor ganha. Por padrão, as prioridades de portas são iguais e seu valor é *128*. No entanto, este valor pode ser modificado, além disso, ele precisa ser um múltiplo de 16, caso contrário, ele usará automaticamente o resultado de N dividido por 16. Por exemplo, se você definir a prioridade da porta como 17, a o valor emitido será 17 \ 16 = 1.

A porta lógica no OLT não precisa ser selecionada e usa diretamente a porta do membro LACP conectada à porta lógica do OLT master (mestre).

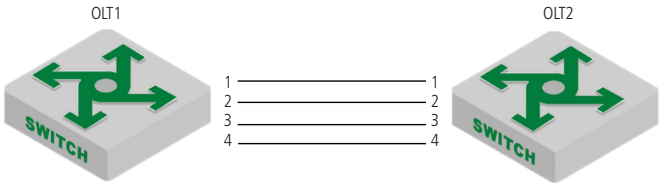
» Configuração de prioridade de porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de interface	**interface ethernet** port-number	-
Configuração da prioridade da interface	**lacp port-priority** value	Opcional
Restaurar a configuração padrão	**no lacp port-priority**	Opcional

Exemplo de configuração de LACP

» Requisitos de rede:

Conforme exibido a seguir, as portas de 1-4 do OLT1 e OLT2, respectivamente, executam LACP dinâmico.



Mapa de esboço do LACP

» Passos de configuração:
  » Configuração do SW1:
    OLT1(config)#channel-group 10
    OLT1(config)#interface range ethernet 0/1 to ethernet 0/4
    OLT1(config-if-range)#channel-group 10 mode active
  » Configuração do SW2:
    OLT2(config)#interface range ethernet 0/1 to ethernet 0/4
    OLT2(config-if-range)#channel-group 2 mode active
» Validação de resultados.
  » Após a negociação dinâmica da LACP ter sucesso, a informação é exibida
    OLT1(config)#show lacp internal
    load balance: src-mac
    Channel: 10, dynamic channel

Port	State	A-Key	O-Key	Priority	Logic-port	Actor-state
e0/1	bndl	11	11	128	1	10111100
e0/2	bndl	11	11	128	1	10111100
e0/3	bndl	11	11	128	1	10111100
e0/4	bndl	11	11	128	1	10111100

    actor-state: activity/timeout/aggregation/synchronization
    collecting/distributing/defaulted/expired

3.3. Configuração de isolamento de portas

Isolamento de portas

Através do recurso de isolamento da porta, você pode adicionar as portas que precisam ser controladas em um grupo de isolamento, separando a camada 2 e a camada 3 entre as portas, fornecendo aos usuários segurança e uma solução de rede flexível.

Se o grupo de isolamento da porta estiver configurado, as portas de downstream não podem se comunicar entre si, enquanto as portas de upstream e de downstream podem.

» Configuração do isolamento de portas baseado em configuração de portas:

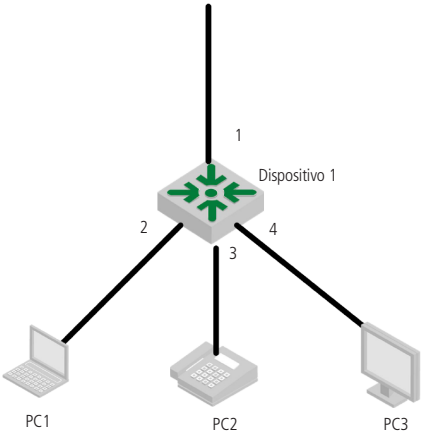
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de portas	**interface {ethernet | pon}** port-number	Obrigatório
Remover todas as portas de uplink	**no port-isolation uplink all**	Obrigatório
Configuração de isolamento de portas	**port-isolation uplink {ethernet | pon}** port-number	Obrigatório
Remover o isolamento de portas	**no port-isolation uplink [all | {ethernet | pon}** port-number**]**	Opcional
Visualização do isolamento de portas	**show port-isolation**	Opcional

Obs.: *nesta configuração, a porta que não está configurada como uma porta isolada é a porta de uplink.*

Exemplo de configuração de isolamento de portas

» Requisitos de rede:

PC1, PC2 e PC3 estão conectados às portas 2, 3 e 4 do OLT. O OLT está conectado à rede externa através da porta 1. PC1, PC2 e PC3 precisam ser isolados entre a camada 2 e a camada 3. O diagrama de rede é o seguinte:



Mapa de esboço da isolação de portas

» Passos de configuração:

  » Configure as portas 2, 3 e 4 como portas de downlink e a porta 1 como porta de uplink.

  OLT4840E(config)#interface rang ethernet 0/2 to interface ethernet 0/4

  OLT4840E(config-if-rang)#port-isolation uplink ethernet 0/1

» Validação de resultados:

OLT4840E(config)#show isolate-port

downlink port :uplink port

e0/2. : e0/1.

e0/3. : e0/1.

e0/4. : e0/1.

As portas e/0/0/2, e0/0/3 e e0/0/4 não podem comunicar-se entre si, apenas com a porta e0/0/1.

3.4. Loopback

Visão geral de loopback

Um teste de loopback permite que você envie e receba dados de uma porta para ela mesma para verificar se ela está operacional. Para executar este teste, você precisa conectar temporariamente os pinos apropriados para permitir que os sinais sejam enviados e recebidos na mesma porta (loopback external). Durante ele, a porta não pode transmitir os pacotes, somente quando este teste terminar.

Configuração de loopback

» Configuração de loopback:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Teste de loop interno	**loopback internal**	Obrigatório
Teste de loop externo	**loopback external**	Obrigatório
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-number	Opcional
Teste de loop interno	**loopback internal**	Opcional
Teste de loop externo	**loopback external**	Opcional

Exemplo de configuração de loopback

» Requisitos de rede:
Nenhum.

» Passos de configuração:
Nenhum.

» Validação de resultados:

» Teste de loop interno:

OLT4840E(config)#interface interface range ethernet 0/1 to ethernet 0/2

OLT4840E(config-if-range)#loopback internal

Port ethernet e0/1 internal looptest successfully

Port ethernet e0/2 internal looptest successfully

» Teste de loop externo:

OLT4840E(config-if-range)#loopback external

Port ethernet e2/0/5 external looptest successfully

Port ethernet e2/0/6 external looptest successfully

3.5. VCT - teste de cabo virtual

Visão geral do VCT

O VCT é usado para testar se a rede está normal, aberta, em curto, com impedância desajustada e assim por diante.

Configuração de VCT

O comando de VCT pode descobrir os erros e sua localização, ele deve ser executado no modo de configuração global e é aplicado a todas as portas; se você executar o comando de VCT no modo de configuração da interface, ele só poderá testar essa interface.

O sistema também suporta o autotest VCT. Quando o VCT está habilitado, ele executará automaticamente o VCT se houver portas no estado linkdown.

» Configuração de VCT:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Executar VCT manualmente	**vct run**	Obrigatório
Executar VCT automaticamente	**vct auto-run**	Opcional
Visualização de configuração de VCT	**show vct auto-run**	Opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Executar VCT manualmente	**vct run**	Opcional
Executar VCT automaticamente	**vct auto-run**	Opcional

Exemplo de configuração de VCT

» Requisitos de rede:

Conecte o tester na OLT.

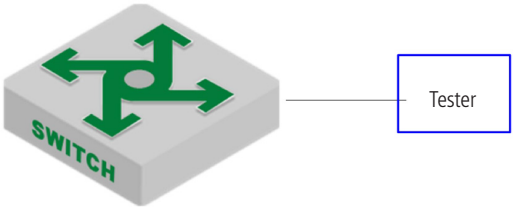


Diagrama esquemático VCT

» Passos de configuração.

Nenhum.

» Validação de resultados.

» Execute o VCT para as portas em que os cabos estão conectados.

OLT4840E(config)#interface ethernet 0/1

Port ethernet 0/1 VCT result :

	TX pair	RX pair
status :	NORMAL	NORMAL
locate :	_	_

» Execute o VCT para as portas em que os cabos não estão conectados.

OLT4840E(config-if-ethernet-0/1)#interface ethernet 0/12

OLT4840E(config-if-ethernet-0/12)#vct run

Port ethernet 0/12 VCT result :

	TX pair	RX pair
status :	OPEN	OPEN
locate :	7	6

3.6. DDM - monitoramento de diagnóstico digital

Visão geral de DDM

O DDM é usado para testar o parâmetro SFP, por exemplo: temperatura, Vdc, corrente de polarização de Tx, potência de Tx, potência de Rx.

Visualização de informações de teste DDM

» Visualização de informações de teste DDM:

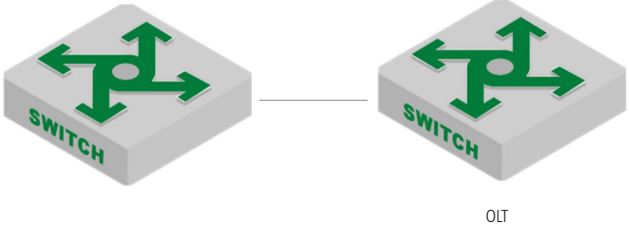
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Visualização de informações de teste DDM	**show interface sfp [ethernet** port-number**]**	Obrigatório

Obs.: *insira o módulo óptico, você pode executar a detecção DDM. A porta PON não suporta esta função.*

Exemplo de configuração de DDM

» Requisitos de rede

O OLT e o dispositivo de referência estão conectados com o SFP que suporta teste DDM para verificar a informação da prova DDM.



Mapa de esboço do teste de DDM

» Passos de configuração.

Nenhum.

» Validação de resultados.

» Visualização das informações do teste DDM no OLT.

OLT4840E(config)#show interface sfp ethernet 0/1/1

Port e0/1/1 :

Common information:

Transceiver Type :SFP

Compliance 10G BASE-LR

Connector Type :LC

WaveLength(nm) :1310

Transfer Distance(m) :10000(9um)

Digital Diagnostic Monitoring :YES

VendorName :WTD

Manufacture information:

Manu. Serial Number :BP132500260047

Manufacturing Date :2013-06-19

VendorName :WTD

Diagnostic information:

Temperature(°C) :28

Voltage(V) :3.3098

Bias Current(mA) :35.419

Bias High Threshold(mA) :70.00

Bias Low Threshold(mA) :15.00

RX Power(dBm) :-2.80

RX Power High Threshold(dBm) :0.00

RX Power Low Threshold(dBm) :-15.20

TX Power(dBm) :-3.10

TX Power High Threshold(dBm) :0.00

TX Power Low Threshold(dBm) :-8.20

3.7. Estatísticas de porta

A porta calculará o status de recebimento de pacotes e de transmissão de pacotes para facilitar ao administrador analisar as causas de falha.

Estatística de pacote nas portas

De modo geral, as informações estatísticas incluem a taxa de o erro de recebimento e transmissão de pacotes, estatística classificada de acordo com o byte, multicast, unicast e broadcast, estatística de perda de pacotes.

Consulte o exemplo para obter informações detalhadas.

» Estatísticas de portas:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Visualização de estatísticas de porta	**show statistic interface ethernet** [port-number]	Obrigatório
Limpar estatísticas de porta	**clear interface ethernet** [port-number]	Opcional
Visualização de estatísticas de porta em tempo real	**show statistics dynamic interface**	Obrigatório
Visualização de utilização de portas	**show utilization interface**	Obrigatório
Visualização de informação de interface	**show interface [{ethernet | pon}** port-number**]**	Opcional

Estatística de porta CPU

Esta função é usada para calcular os pacotes transmitidos para a CPU.

» Estatísticas de porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Visualização de estatísticas de porta da CPU	**show cpu statistic interface [{ethernet | pon}** port-number**]**	Obrigatório
Limpar estatísticas de porta da CPU	**clear cpu-statistics**	Opcional

Operação	Comando	Obrigatório/ opcional
Visualização de estatísticas confidenciais de porta da CPU	**show cpu-classification [interface {ethernet | pon}** port-number**]**	Opcional
Limpar as estatísticas confidenciais de porta da CPU	**clear cpu-classification [interface {ethernet | pon}** port-number**]**	Opcional
Visualização da utilização de porta	**show utilization interface**	Opcional
Visualização de disponibilidade da CPU	**show cpu-utilization**	Opcional

Estatística da taxa média de portas em 5 minutos

Esta função é usada para calcular a taxa média de pacote recebidos e o de pacotes transmitidos em um período especifico. O ciclo estatístico padrão e o maior período estatístico é de cinco minutos.

» Estatística de taxa média em 5 minutos:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do intervalo de análise	**[no] port-rate-statistics interval** value	Opcional, por padrão é *5* minutos. O comando *no* é utilizado para restaurar o valor padrão.
Visualização das estatísticas da porta	**show statistics interface [{ethernet | pon} port-number]**	Opcional

Grupo de agregação de estatísticas de porta

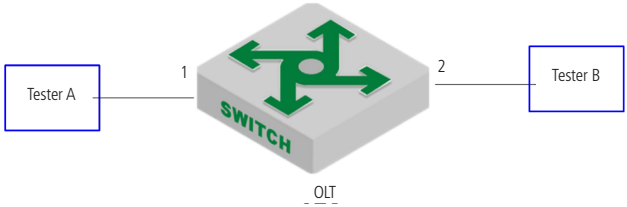
Esta função é usada para calcular os pacotes recebidos e os pacotes de transmitidos do grupo de agregação.

» Estatística de portas do grupo de agregação:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Visualização das estatísticas da porta LACP	**show statistics channel-group [** channel-id **]**	Obrigatório
Limpar estatísticas da porta LACP	**clear channel-group [** channel-id **]**	Obrigatório
Visualização das estatísticas da porta LACP em tempo real	**show statistics dynamic interface channel-group**	Obrigatório

Exemplo de configuração de estatísticas de interface

» Requisitos de rede.
O Tester A envia pacotes para OLT com velocidade de linha para verificar a informação estatística da interface.



Mapa de esboço das estatísticas de interface

» Passos de configuração.
Nenhum.

» Validação de resultado.
» Visualização das estatísticas da interface.
OLT4840E(config)#show statistics interface ethernet 0/1
Port number : e0/1
last 5 minutes input rate 6198600 bits/sec, 12106 packets/sec
last 5 minutes output rate 28256 bits/sec, 55 packets/sec

64 byte packets:4267810
65-127 byte packets:0
128-255 byte packets:0
256-511 byte packets:0
512-1023 byte packets:0
1024-1518 byte packets:0
4267707 packets input, 273132992 bytes , 1 discarded packets
4267707 unicasts, 0 multicasts, 0 broadcasts
1 input errors, 0 FCS error, 0 symbol error, 0 false carrier
1 runts, 0 giants
23763 packets output, 1520832 bytes, 0 discarded packets
0 unicasts, 23763 multicasts, 0 broadcasts
0 output errors, 0 deferred, 0 collisions
0 late collisions
Total entries: 1.

» OLT4840E(config)#show interface ethernet 0/1
Fast Ethernet e0/1 current state: enabled, port link is up
Time duration of linkup is 31 second
Hardware address is 00:0a:5a:00:04:1e
SetSpeed is auto, ActualSpeed is 100M, Duplex mode is full
Current port type: 100BASE-T
Priority is 0
Flow control is disabled
Broadcast storm control target rate is 50000pps
PVID is 1
Port mode: hybrid
Untagged VLAN ID : 1
Input : 5361414 packets, 343130240 bytes
    0 broadcasts, 0 multicasts, 5361414 unicasts
Output : 23763 packets, 1520832 bytes
    0 broadcasts, 23763 multicasts, 0 unicasts

3.8. Controle de fluxo

Visão geral do controle de fluxo

Quando OLTs conectados entre si habilitam a função de controle de fluxo e se um deles estiver congestionado:

1. OLT envia uma mensagem para o OLT de outro lado para notificá-lo para parar de enviar pacotes ou diminuir a velocidade de envio;
2. Depois de receber a mensagem, o OLT do outro lado deixa de enviar pacotes ou retarda a velocidade de envio. Isso evita que os pacotes sejam perdidos e garante o funcionamento normal dos serviços de rede.

Configuração de controle de fluxo

» Configuração de controle de fluxo:

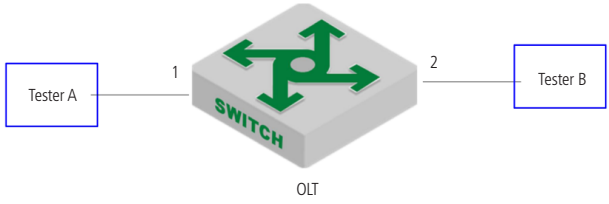
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
(Des) Habilite o controle de fluxo	**[no] flow-control**	Obrigatório, desabilitado por padrão
Visualização das configurações do controle de fluxo	**show flow-control interface [ethernet** port-number**]**	Opcional

Obs.: *as portas PON não suportam esta função.*

Exemplo de configuração de controle de fluxo

» Requisitos de rede

Porta 1 e 2 do OLT permitem controle de fluxo, porta 2 com largura de banda de transmissão de 1M. O tester A envia pacotes para tester B e em seguida, você pode verificar se o quadro de controle de fluxo é emitido pelo OLT.



Mapa de esboço do controle de fluxo

» Passos de configuração.

» Configure o controle de fluxo das portas 1 e 2

OLT4840E(config)#interface range ethernet 0/1 ethernet 0/2

OLT4840E(config-if-range)#flow-control

OLT4840E(config-if-range)#exit

» Configure a porta 2 com banda de transmissão de 1M

OLT4840E(config)#interface ethernet 0/2

OLT4840E(config-if-ethernet-0/2)#bandwidth egress 1024

» Validação de resultados

(1) O Tester A permite o controle de fluxo; ------ Tester A recebe o frame de controle de fluxo emitido pelo OLT e a taxa é ajustada automaticamente para 1M.

3.9. Detecção dos parâmetros ópticos do OLT

Visão geral da detecção dos parâmetros ópticos do OLT

Ele suporta a medição periódica da potência óptica recebida de cada ONU, com a precisão na faixa de -30 dBm a -10 dBm não inferior a ±1 dB, o tempo de amostragem mínimo não superior a 600ns e o tempo mínimo superior a 300ns. Se a potência da conexão de uplink da ONU for muito baixa ou muito alta (levando o limite padrão da potência óptica de sobrecarga do OLT como referência), ocorrerá o Threshold Crossing Alert (alerta de potência fora do padrão) correspondente da potência óptica. Além disso, o OLT é capaz de suportar a detecção de potência óptica de uplink com base na PON-ONU, de modo a realizar o diagnóstico de falha do link. Ele se refere a analisar se o link está normal ou não, de acordo com a potência óptica da ONU recebida, e oferecerá a função de avaliação de falhas.

Sugerimos que o módulo óptico realize a detecção via interface RSSI ou método de transferência AD.

Com base no SFF-8472, o OLT deve poder monitorar os parâmetros de temperatura de operação, tensão de alimentação, corrente de polarização, potência transmitida entre outras informações do módulo SFP.

Os requisitos para a função de detecção de parâmetros são os seguintes:

1. Temperatura de operação do módulo óptico: apresentada por 16 dígitos binários, e a unidade será 1/256 °C. Isso significa que o intervalo de valores é de -128 °C a +128 °C, e a precisão da medição deve estar na faixa de ±3 ºC. A temperatura deve estar em conformidade com as Tabelas 3.13 e Tabelas 3.14 no SFF-8472 Draft 10.3 Dec. 2007;

2. Tensão de alimentação do módulo óptico: apresentada por um número inteiro de 16 dígitos, e a unidade será 100 MV. Isso significa que o intervalo de valores é de 0 a 6,55 V, e a precisão da medição deve estar na faixa de ±3%;
3. Corrente de polarização do transmissor óptico: apresentada por um número inteiro de 16 dígitos e a unidade de 2 μA. Isso significa que o intervalo de valores é de 0 mA a 131 mA, e a precisão da medição deve estar na faixa de ±10%;
4. Potência transmitida do módulo óptico: apresentada por um número inteiro de 16 dígitos e a unidade de 0.1 uW. Isso significa que o intervalo de valores é de 0 mW a 6.5535 mW (-40 dBm ~ +8.2 dBm ou mais), e a precisão da medição deve estar na faixa de ±3 dB;
5. Potência recebida do módulo óptico: refere-se à potência óptica média recebida pelo OLT, apresentada por um número inteiro de 16 dígitos e a unidade de 0.1 uW. Isso significa que o intervalo de valores é de 0 mW para 6.5535 mW (-40 dBm ~ +8.2 dBm ou mais), e sua precisão da medição deve estar na faixa de ±1 dB quando estiver no intervalo de valores de -30 dBm a 10 dBm.

Visualização dos parâmetros ópticos do OLT

Visualização dos parâmetros ópticos do OLT

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da porta PON	**interface pon** slot/port	Obrigatório
Visualização dos parâmetros ópticos do OLT	**show opm option diagnosis**	Visualização de uma porta específica

Exemplo de visualização dos parâmetros ópticos do OLT

» Visualização dos parâmetros ópticos do OLT da porta PON 0/4:

OLT4840E(config)#int pon 0/4

OLT4840E(config-if-pon-0/4)#show opm diagnosis

OPM diagnosis information on PON:

PON [0/4] Temperature: 34. 0 C

PON [0/4] Voltage : 3.33 V

PON [0/4] Bias : 11.20 mA

PON [0/4] TX Power : 4.80 dBm (2.3896 mw)

PON [0/4] RX Power : -7.70 dBm (0.1725 mw)

4. Configuração de VLAN

4.1. Visão geral de VLAN

Virtual Local Area Network (VLAN) é a tecnologia que realiza a divisão por grupo de trabalho virtual através da segmentação dos dispositivos LAN logicamente, sem a necessidade da separação física. A IEEE emitiu o IEEE 802.1Q em 1999, que tinha como objetivo padronizar este tipo solução.

Os gerentes de rede podem segmentar logicamente a LAN física em diferentes domínios de transmissão através desta tecnologia. Cada VLAN contém um grupo de estações de trabalho com as mesmas necessidades, elas não precisam pertencer ao mesmo segmento físico. Além disso o tráfego de broadcast e o tráfego unicast dentro de uma VLAN não serão encaminhados para outras. Portanto, esta solução é muito útil no controle de tráfego, economizando investimento em dispositivos, simplificando o gerenciamento de rede e melhorando a segurança. Utilizando VLAN é possível obter os seguintes recursos:

» Útil no controle de tráfego:

  Na rede tradicional, os dados de broadcast serão enviados para todos os dispositivos de rede diretamente, independentemente de ser necessário ou não, causando um jitter (atrasos) da rede. No entanto, a VLAN suporta configurar o dispositivo de comunicação separadamente, assim quando um broadcast é enviado, ele não será transmitido para todos os equipamentos, mas apenas para aqueles pertencentes a mesma VLAN de origem do broadcast.

» Proporcionando maior segurança:

  Um dispositivo só pode se comunicar com outro dispositivo caso ambos pertençam à mesma VLAN. Por exemplo, deve estar sob o controle do roteador/switch se a VLAN do dispositivo do Departamento de Pesquisa e Desenvolvimento precisa se conectar à VLAN do Departamento de Produto. Caso eles não estejam na mesma VLAN, esses dois departamentos não podem se comunicar diretamente de modo a melhorar a segurança do sistema.

» Reduzindo a carga de trabalho de configuração de rede:

  A VLAN pode ser usada para agrupar hosts específicos. Quando a posição física de um host esteja ao alcance da VLAN, você não precisa alterar sua configuração de rede.

Configurações de VLAN

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Criar / deletar VLAN	**[no] vlan** vlan-list	Obrigatório
Adicionar interface VLAN	**switchport** {ethernet | pon} port-number	Opcional
Especificar descrição da VLAN	**description** string	Opcional

Interface padrão VLAN-ID

A interface padrão da VLAN é também chamada de PVID. Quando o OLT recebe um pacote sem tag, o sistema irá adicionar o valor referente ao PVID nele.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface** {ethernet | pon} port-number	-
Configurar interface PVID	**switchport default vlan** vlan-id	Opcional
Restaurar PVID padrão	**no switchport default vlan**	PVID = *1* (padrão)
Visualizar as configurações detalhadas da interface	**show interface** {ethernet | pon} port-number	Opcional
Visualizar as configurações resumidas da interface	**show interface brief ethernet** [port-number]	Opcional

Tipos de interface

O tipo de interface pode ser dividido em três, de acordo com os diferentes modos de processos executados:

- **Interface access (de acesso):** esta interface pertence apenas a uma VLAN, e geralmente é usada para conectar o dispositivo terminal.
- **Trunk:** as interfaces trunk aceitam tráfego com e sem tag. Caso um frame seja tagged ele será encaminhado para a VLAN referida. Se um pacote chegar sem tag à porta trunk ele será encaminhado para a VLAN default (por padrão é a VLAN 1, mas pode ser definida pelo usuário).
- **Interface hybrid (híbrida):** esta interface pode receber e encaminhar várias VLANs tendo ou tag ou não. No caso de diferentes VLANs sem tag é necessário criar regras de classificação.

Tipo de interface	Procedimento ao receber um pacote		Procedimento de encaminhamento de pacote
	Untag (sem tag)	Tag	
Access	Recebe o pacote e adiciona a tag configurada no PVID	Se a tag (VID) do pacote for igual à VLAN permitida pela porta, recebe o pacote. Se a tag (VID) for diferente, o pacote é descartado	Remove a tag e transmite o pacote.
Hybrid			Se a tag do pacote é igual a alguma VLAN untag configurada, remove a tag e transmite o pacote. Se a tag do pacote é igual a alguma VLAN permitida, mantém a tag e transmite o pacote.
Trunk			Se a tag do pacote for igual a alguma permitida, mantém a tag e transmite o pacote.

» Configuração do tipo de interface VLAN na porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Configuração da interface VLAN	**switchport mode** {access|hybrid|trunk}	Opcional, valor padrão é *Hybrid*

Atributos da VLAN em interfaces Hybrid

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Configuração da interface VLAN	**switchport mode** hybrid	Opcional, valor padrão é *Hybrid*

Permitir a passagem de VLANs específicas na porta Hybrid.	**switchport hybrid** {tagged | untagged} **vlan** { vlan-list | all }	*tagged* significa que o pacote carrega uma tag VLAN. *Untagged* significa que o pacote não carrega uma tag VLAN.
Proibir a passagem de qualquer VLAN na porta Hybrid	**no switchport hybrid vlan** vlan-list	Opcional

Atributos da VLAN em interfaces Trunk

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Configuração da interface VLAN	**switchport mode** trunk	Obrigatório
Permitir a passagem de VLANs específicas na porta Trunk	**switchport trunk allowed vlan** { vlan-list | all }	Obrigatório
Proibir a passagem de VLANs específicas na porta Trunk	**no switchport trunk vlan** { vlan-list | all }	Opcional

Configuração de prioridade de porta

Quando o OLT recebe um pacote untagged, o sistema adicionará uma tag VLAN ao pacote no qual o valor vid na tag é o valor PVID e o valor de prioridade é o valor da prioridade da interface.

» Configuração de prioridade de interface:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Configuração de prioridade de porta	**priority** value	Opcional, valor *0* por padrão
Restaurar prioridade padrão	**no priority**	Opcional
Visualizar as configurações detalhadas da interface	**show interface** {ethernet | pon} port-number	Opcional

Filtro de entrada

Por padrão, a interface verificará se o pacote recebido pertence à VLAN, se for, a interface executará o processamento direto senão descartará o pacote. Esse processo é chamado de filtragem de entrada. Por padrão essa função vem habilitada.

» Filtro de entrada:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Configuração de filtro de entrada	**[no] ingress filtering**	Opcional, habilitado por padrão
Visualizar as configurações detalhadas da interface	**show ingress [interface** port-number **]**	Opcional

Configuração dos tipos de interfaces aceitáveis

É possível configurar a regra de entrada de pacotes em cada interface, por padrão as interfaces aceitam pacotes com e sem tag.

» Configuração dos tipos de interfaces aceitáveis:

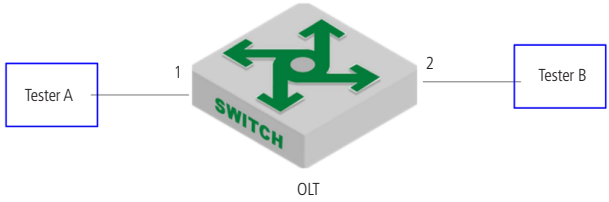
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Configuração do filtro de entrada	**ingress acceptable-frame** { all | tagged }	*all* significa que tanto pacotes com tag ou sem tag podem ser recebidos. *tagged* significa que apenas pacotes com tag podem ser recebidos.
Visualizar as configurações detalhadas da interface	**show ingress [** interface port-number **]**	Opcional

Exemplo de configuração

Exemplo 1

» Requisitos de rede.

Crie a VLAN 100, incluindo a portas 1 e 2, 1 é a porta de acesso e 2 é a porta trunk.



Mapa de esboço da interface padrão VLAN

» Passos de configuração.

» Crie a VLAN 100 e, em seguida, adicione a porta 1 e a porta 2:

OLT4840E (config) #vlan 100

OLT4840E (config-if-vlan) #switchport ethernet 0/1 ethernet 0/2

» Modifique o modo *VLAN* da porta 1 e a porta 2 e, em seguida, configure o PVID como 100.

OLT4840E (config) #interface ethernet 0/1

OLT4840E (config-if-ethernet-0/1) #switchport mode access

OLT4840E (config-if-ethernet-0/1) #switchport default vlan 100

OLT4840E (config-if-ethernet-0/1) #interface ethernet 0/2

OLT4840E (config-if-ethernet-0/2) #switchport mode trunk

OLT4840E (config-if-ethernet-0/2) #switchport default vlan 100

OLT4840E (config-if-ethernet-0/2) #exit

» Validação de resultado:

» Exibir as informações da porta 1 e da porta 2:

OLT4840E (config) #show interface brief ethernet 0/1 ethernet 0/2

Port Desc Link shutdn Speed Pri PVID Mode TagVlan UtVlan

e0/1 up false auto-f100 0 100 acc 100

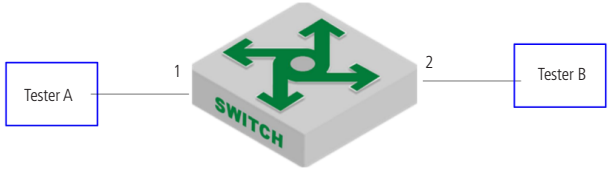
e0/2 up false auto-f100 0 100 trk 100

Total entries: 2.

Exemplo 2

» Requisitos de rede.

Configure a porta 1 para ser o modo access; configure a porta 2 para ser o modo *Trunk*.



Mapa de esboço do modo VLAN da interface

» Passos de configuração.

» Configure a porta 1 para ser o modo *Access*:

OLT4840E (config) #interface ethernet 0/1

OLT4840E (config-if-ethernet-0/1) #switchport mode access

» Configure a porta 2 para ser o modo *Trunk*:

OLT4840E (config-if-ethernet-0/1) #interface ethernet 0/2

OLT4840E (config-if-ethernet-0/2) #switchport mode trunk

OLT4840E (config-if-ethernet-0/2) #exit

» Validação de resultado.

» Exibir as informações da porta 1 e da porta 2:

OLT4840E (config) #show interface brief ethernet 0/1 ethernet 0/2

Port Desc Link shutdn Speed Pri PVID Mode TagVlan UtVlan

e0/1 up false auto-f100 0 100 acc 100

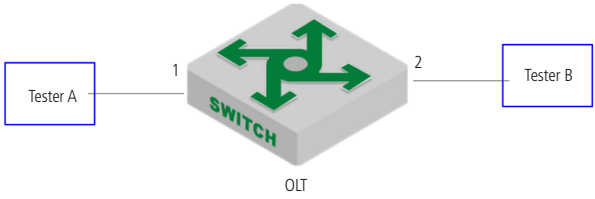
e0/2 up false auto-f100 0 100 trk 100

Total entries: 2

Exemplo 3

» Requisitos de rede:

Crie VLAN 500, incluindo a porta 1 e 2; ambas são hybrid; configure a VLAN 500 com tag na saída.



Atributos de tags na saída híbrida

» Passos de configuração.

» Configure VLAN 500 e adicione a porta 1 e 2:

OLT4840E (config) #vlan 500

OLT4840E (config-if-vlan) #switchport ethernet 0/1 ethernet 0/2

OLT4840E (config-if-vlan) #show vlan 500

Show VLAN information

VLAN ID : 500

VLAN status : static

VLAN member : e0/1-e0/2.

Static tagged ports :

Static untagged Ports : e0/1-e0/2.

Dynamic tagged ports :

Total entries: 1 vlan.#

» Configure VLAN 500 com tag na saída da porta 1 e 2:

OLT4840E(config-if-vlan)#interface range ethernet 0/1 ethernet 0/2

OLT4840E(config-if-range)#switchport hybrid tagged vlan 500

OLT4840E (config-if-range) #show vlan 500

show VLAN information

VLAN ID : 500

VLAN status : static

VLAN member : e0/1-e0/2.

Static tagged ports : e0/1-e0/2.

Static untagged Ports :

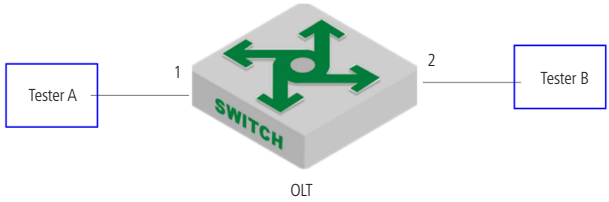
Dynamic tagged ports :

Total entries: 1 vlan.

» Validação de resultados:
  » (1) o tester A encaminha o pacote desconhecido de VLAN = 500, tester B pode receber o pacote de VLAN = 500 com tag.

Exemplo 4

» Requisitos de rede.
Crie a VLAN 100 e 200, depois adicione a porta 1 e 2; ambas em modo *Híbrido* e com as VLANs untagged.



Mapa de esboço de adicionar a porta a VLAN

» Passos de configuração.
  » Crie a VLAN 100 e depois adicione a porta 1 e 2:
  OLT4840E (config) #vlan 100

  OLT4840E (config-if-vlan) #switchport ethernet 0/1 ethernet 0/2

  OLT4840E (config-if-vlan) #show vlan 100

  show VLAN information

  VLAN ID : 100

  VLAN status : static

  VLAN member : e0/1-e0/2.

  Static tagged ports :

  Static untagged Ports : e0/1-e0/2.

  Dynamic tagged ports :

» Crie a VLAN 200 e depois adicione a porta 1 e 2:

OLT4840E (config) #vlan 200

OLT4840E (config-if-vlan) #exit

OLT4840E (config-if-range) #interface range ethernet 0/1 ethernet 0/2

OLT4840E(config-if-range)#switchport hybrid untagged vlan 200

OLT4840E (config-if-range) #show vlan 200

show VLAN information

VLAN ID : 200

VLAN status : static

VLAN member : e0/1-e0/2.

Static tagged ports :

Static untagged Ports : e0/1-e0/2.

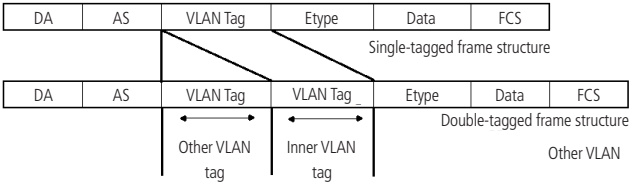
Dynamic tagged ports :

Total entries: 1 vlan.

4.2. Configurações de QinQ

Visão geral do QinQ

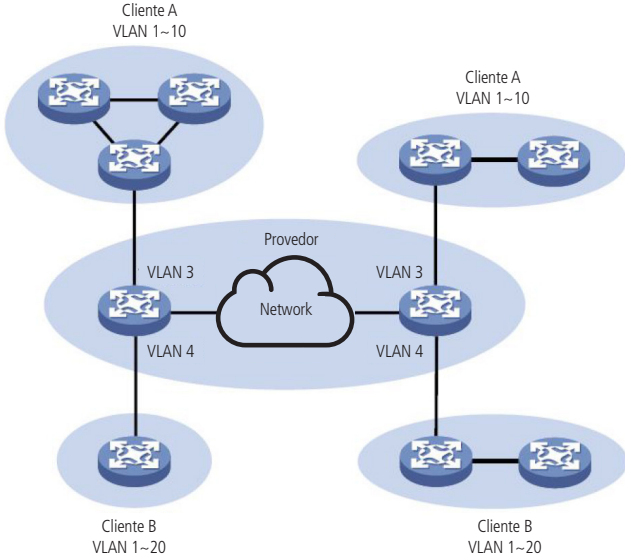
No campo de tag de VLAN definido no IEEE 802.1Q, apenas 12 bits são usados para sua ID, então um OLT pode suportar no máximo de 4.094 VLANs. Em aplicações reais, no entanto, pode ser necessário um grande número de VLANs para isolar usuários, especialmente nas redes de área metropolitana (MANs) e 4.094 estão longe de satisfazer esses requisitos. A tecnologia QinQ resolve este tipo de problema, ela permite que um dispositivo suporte até 4.094 x 4.094 VLANs para satisfazer as necessidades de cada rede. O diagrama a seguir mostra a estrutura dos quadros de Ethernet com uma e duas tags.



Estrutura de frame de QinQ

O recurso QinQ da porta é uma técnica de VPN de camada 2 flexível, ela permite que os quadros Ethernet viajem através da rede backbone do provedor (rede pública) com tags VLAN duplas, isso é possível, pois o ponto de acesso encapsula a tag VLAN externa (stag) em quadros Ethernet de redes de clientes (redes privadas).

A tag de VLAN interna pertence à rede de clientes e é transmitida como parte dos dados, enquanto a externa é atribuída pelo provedor e os quadros são encaminhados com base apenas na stag, com o endereço MAC de origem aprendido como entrada de tabela de endereço MAC.



Aplicação QinQ

Uma tag VLAN usa o campo de protocolo (TPID) para identificar o tipo da tag, seu valor , conforme definido no IEEE 802.1Q, é 0×8100. O dispositivo pode identificar se existe uma tag correspondente de acordo com o TPID, se este campo estiver corretamente configurado, o pacote é considerado *com* tag VLAN.

O TPID em um cabeçalho Ethernet tem a mesma posição do campo do tipo de protocolo em uma moldura sem tag VLAN. Para evitar problemas no encaminhamento e manipulação de pacotes na rede, você não pode definir o valor TPID para nenhum dos valores na tabela a seguir.

» Valores comuns de protocolos:

Protocolo	Valor
ARP	0×0806
PUP	0×0200
RARP	0×8035
IP	0×0800
IPv6	0×86DD
PPPoE	0×8863/0×8864
MPLS	0×8847/0×8848
IPX/SPX	0×8137
IS-IS	0×8000
LACP	0×8809
802.1x	0×888E
GnLink	0×0765
GSTP	0×5524

No QinQ, existem quatro modos de interface: none, customer, customer-no-static e uplink. Depois de ativar QinQ, o modo de interface será *None* por padrão.

Quatro modos de interface são adequados para diferentes aplicações:

» **None:** este modo é adequado para que conectar diretamente ao PC e o pacote dessa interface tentará identificar as tags de VLAN externa e interna; a tag interna será removida antes do encaminhamento enquanto a tag externa será removida apenas se a configuração do OLT determinar isso.

» **Customer:** a interface deste modo e a interface do modo *Uplink* formam a aplicação QinQ estática. O pacote que entra nesta interface oriundo do cliente será considerado sem tag externa e com tag interna, assim o pacote tomará o PVID como ID da VLAN externa e será transmitido com as duas tags pela interface de uplink; quando o pacote vier da interface de uplink a tag externa será removida antes do encaminhamento para o cliente independentemente da configuração. Essa interface precisa se conectar ao dispositivo do usuário.

» **Customer-no-static:** a interface deste modo e a interface do modo *Uplink* formarão a aplicação QinQ dinâmica. A interface tentará identificar a tag externa dos pacotes oriundos do uplink, após isso irão passar pela comparação com a regra de QinQ dinâmica, se a regra for atendida, a tag de externa será retirada e o pacote encaminhado somente c-VLAN para o cliente. Os pacotes oriundos do cliente passaram também pela inspeção da regra, se for atendida será feita a inserção da tag externa e os pacotes encaminhados com duas tags pelo uplink.

» **uplink:** a interface deste modo precisa se conectar à interface do dispositivo operador.

O pacote que entra nesta interface oriundo da interface customer tentará identificar a tag da VLAN externa e irá encaminhar os pacotes com as duas tags.

A interface de uplink avalia o valor TPID externo. Se o protocolo VLAN for o mesmo que o valor TPID externo configurado, o pacote será transmitido sem alteração para interface customer com VLAN correspondente; se o número do protocolo VLAN for diferente do valor TPID externo, o pacote será marcado com a tag do PVID da porta.

Obs.: *a interface do modo* Cliente *não pode se comunicar com a interface de modo* None.

Visão geral do QinQ estático

Após habilitar a função *DTAG*, o dispositivo não executará o QinQ estático por padrão. Somente após configurar os modos de interface é que terá efeito. Se a interface não configurar a regra de entrada (QinQ dinâmico), o pacote será processado de acordo com QinQ estático.

O seguinte é o processo de manipulação QinQ estático:

1. Fluxo do processo da porta do cliente:

   A porta do cliente irá adicionar a tag VLAN igual ao PVID ao pacote original e o encaminhará nesta VLAN, mesmo se o pacote tiver tag ou não, se o TPID é o mesmo que o configurado (interno / externo) ou não, ou se a vid existe no equipamento ou não.

2. Fluxo do processo da porta de uplink:

   Se a porta de uplink irá inserir uma tag ou não, depende se o pacote possui uma tag. Se a porta de uplink possui uma tag depende se o número do protocolo VLAN é o mesmo que o valor global do TPID externo:

   » Se o número do protocolo VLAN for o mesmo que o valor global TPID externo, ele será considerado *com tag* e então encaminhará o pacote na VLAN carregada sem inserir uma tag; se a VLAN não existir no sistema, o pacote não será encaminhado.

   » Se o número do protocolo VLAN for diferente do valor global TPID externo, ele irá inserir uma tag VLAN de acordo com o PVID e, em seguida, irá adicionar um TPID externo de acordo com o TPID interno para o encaminhamento.

3. Processamento do valor TPID:

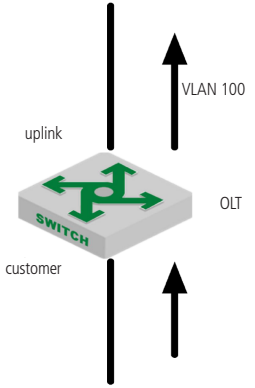
   Quando o pacote encaminhado da porta do cliente ou da porta de uplink, o valor TPID é sempre consistente com o valor TPID externo.

» Configuração de QinQ Static:

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	-
(Des)Habilitar o QinQ global	**[no]dtag**	Obrigatório
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	-
Especificar modo *QinQ* na porta	**dtag mode** {customer|uplink}	Obrigatório, cliente e uplink formam o QinQ estático
Restaurar modo *Padrão* na porta	**no dtag mode**	Opcional, modo *Nenhum* por padrão
Visualizar configurações QinQ	**show dtag**	Opcional

Exemplo de configuração de QinQ estático

» Requisitos de rede:
Enviar pacotes com tag de VLAN externa igual a 100 pela interface de uplink.
O fluxo de rede é o seguinte:



Cenário QinQ

» Passos de configuração:
  » Habilitar DTAG global:
  OLT4840E (config) #dtag
  » Entre na porta 1, configure o modo de porta QINQ como cliente:
  OLT4840E (config) #interface ethernet 0/1
  OLT4840E (config-if-ethernet-0/1) #dtag mode customer
  » Configure a VLAN padrão da porta 1 para ser 100:
  OLT4840E (config-if-ethernet-0/1) #switchport default vlan 100
  » Entre na porta 2, configure o modo de porta QINQ para ser uplink:
  OLT4840E(config)#interface ethernet 0/2
  OLT4840E(config-if-ethernet-0/2)#dtag mode uplink
  » Configure a porta 2 para ser a porta trunk:
  OLT4840E(config-if-ethernet-0/2)#switchport mode trunk

» Validação de resultados:

Não importa se o pacote da interface do cliente possui tag VLAN ou não, bem como o valor da tag, o pacote adicionará ao cabeçalho a tag de VLAN 100 ao transmitir a partir da porta de uplink.

Visão geral de QinQ dinâmico

A porta Uplink pode ser capaz de configurar a regra de entrada. Se a tag de pacote estiver em conformidade com a regra de entrada, ela será tratada de acordo com a regra correspondente, independentemente do valor do TPID externo configurado.

A porta customer-no-static não só verificará se o pacote contém tag ou não, mas também julgará se está em conformidade com a regra de entrada. Se o pacote possui tag e estiver em conformidade com a regra, ele será processado de acordo com o QINQ dinâmico, ou será processado de acordo com a regra 802.1Q. O seguinte é o processo detalhado:

1. Em primeiro lugar compara-se o pacote de entrada oriundo da interface de uplink com o TPID externo configurado. Se o pacote for diferente do TPID externo, o pacote será processado de acordo com a regra 802.1Q, adicionando uma tag de acordo com a interface PVID;
2. Se o TPID do pacote é o mesmo que o TPID externo, mas o pacote VID não está na faixa de inserção, o pacote será processado de acordo com a regra 802.1Q, realizando transmissão ou o descartando;
3. Se o TPID do pacote é o mesmo que o TPID externo e o pacote VID está na faixa de inserção, o pacote será processado de acordo com o QINQ dinâmico:
   - » O pacote será processado de acordo com a regra de inserção independentemente VID do pacote existir ou não, adicionando uma tag externa de acordo com a regra de inserção.
   - » Se a VLAN externa que corresponde à regra de inserção não existe, ou a VLAN existe, mas não inclui a porta de entrada, o pacote será descartado.
   - » Se a VLAN externa que corresponde à regra de inserção existe, mas a VLAN não inclui qualquer porta de entrada, o pacote será processado de acordo com a regra de inserção em primeiro lugar, ou seja, este pacote aprenderá o endereço MAC de acordo com a VLAN externa, mas o pacote será descartado mais tarde.

» Configuração de QinQ Dinâmico:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
(Des)Habilitar o *QinQ* global	**[no]dtag**	Obrigatório
Acesse o modo de configuração de portas	**interface** {ethernet | pon} port-number	
Modo *QinQ* na porta	**stag mode** {customer-no-static|uplink}	Obrigatório, cliente e uplink formam o QinQ estático
Restaurar modo *Padrão* na porta	**no dtag mode**	Opcional, modo *Nenhum* por padrão
Configuração de regra de inserção	**dtag insert** start-vlanend-vlan service-vlan	Obrigatório
Remover regra de inserção	**no dtag insert {**all | start-vlanend-vlan **}**	Opcional
Visualizar configurações QinQ	**show dtag**	Opcional

Obs.: *o QinQ estático e o QinQ dinâmico podem ser habilitados ao mesmo tempo. No entanto, ao configurar a regra QinQ dinâmica, a regra QinQ dinâmica será determinada de acordo com a ID da VLAN externa do QinQ estático. Portanto, o modo de interface QinQ dinâmico é recomendado para ser configurado como customer-no-static.*

Exemplo de configuração de QinQ dinâmico

» Requisitos de rede.

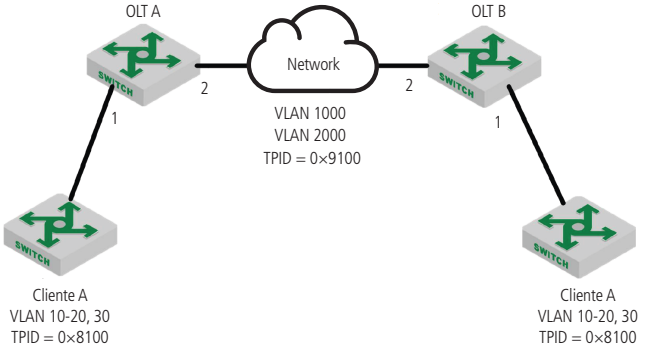
O OLT A e o OLT B atuam como a rede do operador para acessar o dispositivo. O cliente A e o cliente B atuam quando o usuário termina a rede para acessar o dispositivo. O dispositivo A se conecta com o dispositivo B via porta trunk, que permite que VLAN 1000 e VLAN 2000 passem; use o equipamento de outros fabricantes entre o OLT A e o OLT B, TPID = 0×9100.

Requer implementar os seguintes requisitos:

» Depois de encaminhado pela rede VLAN 1000 do operador, o pacote do cliente A VLAN 10-20 pode se comunicar com o pacote B VLAN 10-20 do cliente.

» Depois de encaminhado pela rede VLAN 2000 do operador, o pacote do cliente A VLAN 30 pode se comunicar com o pacote do cliente B VLAN 30.

O diagrama de rede é o seguinte:



Esboço de rede de QinQ

» Passos de configuração:
  » Configuração do OLT A:
    » Crie a VLAN 1000 e a VLAN 2000 e, em seguida, adicione-os à porta de usuário (porta 1) e à porta de serviço (porta 2).
    OLT4840E(config)#vlan 1000,2000
    OLT4840E(config-if-vlan)#switchport ethernet 0/1 ethernet 0/2
    » Configure a porta de serviço para ser porta trunk:
    OLT4840E(config)#interface ethernet 0/2
    OLT4840E(config-if-ethernet-0/2)#switchport mode trunk
    » Habilite a função *QinQ global*:
    OLT4840E (config) #dtag
    » Configure a tag externa TPID para ser 0×9100:
    OLT4840E (config) #dtag external-tpid 9100
  » Configure o modo *QinQ* da porta do usuário:
  OLT4840E (config) #interface ethernet 0/1
  OLT4840E (config-if-ethernet-0/1) # dtag mode customer-no-static
  » Configurar o serviço da porta no modo *QinQ:*
  OLT4840E(config)#interface ethernet 0/2

OLT4840E(config-if-ethernet-0/2)#dtag mode uplink

» Configure a regra de inserção de porta de usuário:
OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#dtag insert 10 20 1000

Set SVLAN successfully.

OLT4840E(config-if-ethernet-0/1)#dtag insert 30 30 2000

Set SVLAN successfully.

A configuração do OLT B é a mesma que o OLT A, então é necessário repetir.

» Validação de resultado:
Após os pacotes com VLAN 10-20 do cliente A passar pelo OLT A, os pacotes iram carregar a tag de VLAN = 1000 e TPID = 0×9100.

Após os pacotes com VLAN 30 do cliente B passar pelo OLT A, o pacote traz a tag externa = 2000 e TPID = 0×9100.

4.3. Função ajustável de VLAN tag TPID

Configuração do valor ajustável do TPID da tag VLAN

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do valor da tag TPID interno	**dtag inner-tpid** tpid	Opcional, *0×8100* por padrão
Restaurar o valor padrão do TPID interno	**no dtag inner-tpid**	Opcional
Acessar o modo de configuração de interface	**interface** {etherne|pon} port-number	TPID externo apenas pode ser configurar no modo de configuração de porta
Configuração do valor da tag TPID externo	**dtag outer-tpid** tpid	Opcional, *0×8100* por padrão
Restaurar o valor padrão do TPID externo	**no dtag outer-tpid**	Opcional

Operação	Comando	Obrigatório/ opcional
Visualizar valores do TPID	**show dtag**	Em qualquer modo

Obs.: » *Quando o pacote de tag dupla se comunica com a CPU, a informação interna do pacote VLAN TPID deve estar de acordo com a configuração do equipamento. Caso contrário, não é possível realizar nenhuma comunicação.*

» *Quando encaminhado a partir da interface de uplink, o valor de TPID do pacote estará em acordo com o valor externo de saída do TPID.*

Exemplo de configuração de valor ajustavel de TPID

» Modifique o tag TPID interno para 0×9100:
OLT4840E(config)#dtag inner-tpid 9100

» Modifique o tag TPID interno para 0×9200:
OLT4840E(config)#dtag outer-tpid 9200

» Exiba a informação do TPID:
OLT4840E(config)#show dtag
Current dtag status: enabled
inner-tpid : 0x9100
outer-tpid : 0x9200
cpu inner-tag : vid 1 priority 0
interface : dtag-mode

4.4. Configuração de GVRP

Visão geral de GVRP

GVRP a é abreviatura do GARP VLAN *Registration Protocol*. É um tipo de aplicação do GARP, com base no seu mecanismo de trabalho para manter informações de registro dinâmico de VLAN do OLT e transferi-lo para outro OLT.

OLTs que suportam o GVRP podem receber informações de registro de VLAN de outros OLTs e atualizar dinamicamente suas informações locais, incluindo: membros atuais de VLAN e por qual interface pode alcançar os membros de cada uma delas. Esta troca de informações é utilizada para tornar as informações de registro de VLAN consistentes. Nelas, são enviadas as informações de registro estático da configuração manual local e de registro dinâmico de outros OLTs.

Habilitando o GVRP

O GVRP possui dois switches, um está no modo de configuração global e o outro está no modo de configuração da interface. Se você quiser ativar o GVRP, esses dois switches devem estar no estado *habilitado*.

Por padrão, ambos GVRP global e GVRP de interface estão desativados. É importante notar que, o GVRP só pode ser habilitado na porta trunk.

» Habilitando o GVRP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar a configuração global de GVRP	**gvrp**	Obrigatório
Desabilitar a configuração global de GVRP	**no gvrp**	Obrigatório
Acessar o modo de configuração de port	**interface ethernet** interface-num	-
Habilitar o GVRP	**[no] gvrp**	Obrigatório, utilize o comando *no gvrp* para desabilitar o GVRP

Configuração de VLAN que precisa do GVRP para encaminhamento

As informações de cadastro de VLAN transmitidas pelo GVRP podem ser: VLAN estática local ou a VLAN aprendida através do protocolo GVRP. A transmissão de VLANs via GVRP só será realizada após especificado pelo administrador.

» Configure a VLAN que precisa do GVRP para encaminhar:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de VLAN que precisa de GVRP para encaminhamento	**(no) gvrp permit vlan** vlan-list	Obrigatório, utilize o comando *no* para cancelar a configuração

Configure a VLAN que proíbe a porta de encaminhar

» Configure a VLAN que precisa do GVRP para encaminhar:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de VLAN que proíbe a porta de encaminhar	**garp forbid** vlan-id	Opcional
Configuração de VLAN que permite a porta de encaminhar	**no garp forbid** vlan id	Opcional

GVRP visualização e depuração

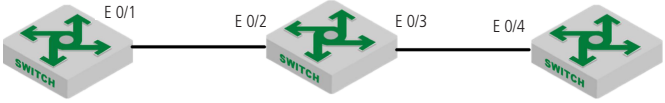
Depois de concluir as configurações acima, você pode verificá-las através dos seguintes comandos.

» GVRP Visualização e depuração:

Operação	Comando	Obrigatório/ opcional
Visualização do estado do GVRP (habilitado, desabilitado)	**show gvrp**	Comandos executáveis em qualquer modo
Visualização do estado da interface GVRP	**show gvrp interface [ethernet** device/ slot/port**]**	
Visualização das VLANs que precisam de GVRP para serem transmitidas	**show garp permit vlan**	

Exemplo de configuração de GVRP

» Requisitos de rede:



Exemplo de configuração de serviço GVRP

Conforme exibido na figura, os OLT 1 e OLT 3 encaminham suas informações de VLAN estáticas para o OLT 2 via protocolo GVRP. O OLT 2 transmite as VLANs estáticas e as VLANs aprendidas via GVRP.

Por fim, as informações de VLAN do OLT 1, OLT 2 e OLT 3 estarão sincronizadas.

» Roteiro de configuração:
  1. Habilite o GVRP no OLT 1, e depois distribua as informações de VLAN;
  2. Habilite o GVRP no OLT 2, e depois distribua as informações de VLAN;
  3. Habilite o GVRP no OLT 3, e depois distribua as informações de VLAN.

» Passos de configuração:
  » Configuração do OLT 1:
    OLT4840E(config)# vlan 2-4
    OLT4840E(config-if-vlan)#switchport ethernet 0/1
  » Adicionar porta VLAN:
    OLT4840E (config-if-vlan)#interface e 0/1
    OLT4840E (config-if-ethernet-0/1)#switchport mode trunk
    OLT4840E (config-if-ethernet-0/1)#exit
    OLT4840E (config)#gvrp / configurar GVRP
    Turn on GVRP succesfully
    OLT4840E (config)#garp permit vlan 2-4
    OLT4840E (config)#interface e 0/1
    OLT4840E (config-if-ethernet-0/1)#gvrp
    OLT4840E (config-if-ethernet-0/1)#exit
    OLT4840E (config)#show gvrp // visualizar de configuração de GVRP
    GVRP state : enable
    OLT4840E (config)#show gvrp interface ethernet 0/1
    port GVRP status fixed-vlan forbidden-vlan
    e0/1 enable 1-4
    Total entries: 1.
    OLT4840E (config)#show garp permit vlan
    VLAN 1 is Garp default permit VLAN
    Other Garp permit VLAN :
    2-4

» Configuração do OLT 2:

OLT4840E (config)#vlan 5-6

OLT4840E (config-if-vlan)# switchport ethernet 0/2 to ethernet 0/3

» Adicionar porta VLAN:

OLT4840E (config-if-vlan)#exit

OLT4840E (config)#interface range ethernet 0/2 to ethernet 0/3

OLT4840E (config-if-range)# switchport mode trunk

OLT4840E (config-if-range)#exit

OLT4840E (config)#gvrp // Configurar GVRP

Turn on GVRP successfully.

OLT4840E (config)#interface range ethernet 0/2 to ethernet 0/3

OLT4840E (config-if-range)#gvrp.

OLT4840E (config-if-range)#exit

OLT4840E (config)#garp permit vlan 5-6

OLT4840E (config)#show gvrp // visualizar configuração de GVRP

GVRP state : enable

OLT4840E (config)#show gvrp interface ethernet 0/2 ethernet 0/3

port GVRP status fixed-vlan forbidden-vlan

e0/2 enable 1,5-6

e0/3 enable 1,5-6

Total entries: 2.

OLT4840E (config)#show garp permit vlan

VLAN 1 is Garp default permit VLAN

Other Garp permit VLAN : 5-6

» Configuração do OLT 3:

OLT4840E (config)#vlan 7-8

OLT4840E (config-if-vlan)#switchport ethernet 0/4

» Adicionar porta VLAN:

OLT4840E (config-if-vlan)#interface e 0/4

OLT4840E (config-if-ethernet-0/4)#switchport mode trunk

OLT4840E (config-if-ethernet-0/4)#exit

OLT4840E (config)#gvrp // Configurar GVRP

Turn on GVRP successfully.

OLT4840E (config)#interface e 0/4

OLT4840E (config-if-ethernet-0/4)#gvrp

OLT4840E (config-if-ethernet-0/4)#exit

OLT4840E (config)#garp permit vlan 7-8

OLT4840E (config)#show gvrp //verificar configurações de gvrp

GVRP state : enable

OLT4840E (config)#show gvrp interface ethernet 0/4

port GVRP status fixed-vlan forbidden-vlan

e0/4 enable 1,7-8

Total entries: 1.

OLT4840E (config)#show garp permit vlan

VLAN 1 is Garp default permit VLAN

Other Garp permit VLAN : 7-8

Depois de terminar a configuração, você pode usar o comando de *Show VLAN* para verificar as informações de registro de VLAN aprendidas via GVRP.

Verifique as informações de VLAN no OLT 1, você pode achar as VLANs 5-8 aprendidas via GVRP.

OLT4840E (config)#show vlan

show VLAN information

VLAN ID : 1

VLAN status : static

VLAN member : e0/1-e0/2/2

Static tagged ports : e0/1

Static untagged Ports : e0/2-e0/2/2

Dynamic tagged ports :

show VLAN information
VLAN ID : 2
VLAN status : static
VLAN member : e0/1.
Static tagged ports : e0/1.
Static untagged Ports :
Dynamic tagged ports :

show VLAN information
VLAN ID : 3
VLAN status : static
VLAN member : e0/1.
Static tagged ports : e0/1.
Static untagged Ports :
Dynamic tagged ports :

show VLAN information
VLAN ID : 4
VLAN status : static
VLAN member : e0/1.
Static tagged ports : e0/1.
Static untagged Ports :
Dynamic tagged ports :

show VLAN information
VLAN ID : 5
VLAN status : dynamic
VLAN member : e0/1
Static tagged ports :
Static untagged Ports :

Dynamic tagged ports : e0/1
show VLAN information
VLAN ID : 6
VLAN status : dynamic
VLAN member : e0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/1

show VLAN information
VLAN ID : 7
VLAN status : dynamic
VLAN member : e0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/1

show VLAN information
VLAN ID : 8
VLAN status : dynamic
VLAN member : e0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/1
Total entries: 8 vlan.

4.5. Tradução de VLAN N:1

Visão geral da tradução de VLAN N:1

Existem dois tipos de traduções de VLAN N:1, uma é 1:1, e a outra é N:1. As definições são as seguintes:

» **1:1:** modifica a tag VLAN específica para ter uma nova tag VLAN.

» **N:1:** modifica as diferentes tags VLAN para terem a mesma tag VLAN.

» A tradução N:1 pode ser realizada via VLAN-Swap ou VLAN-Translate.

Configuração da tradução de VLAN

» Configuração de tradução de VLAN:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da tabela de tradução de VLAN para a entrada	**vlan-translate ingress table** start-vid end-vid new-vid	Obrigatório
Remover tabela de tradução de VLAN para a saída	**no vlan-translate ingress table [**start-vid end-vid**]**	Opcional
Configuração da tabela de tradução de VLAN para a saída	**vlan-translate egress table** start-vid end-vid new-vid	Obrigatório
Remover tabela de tradução de VLAN para a saída	**no vlan-translate egress table [**start-vid end-vid**]**	Opcional
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
(Des)Habilite a função de tradução para a entrada de pacotes	**[no]vlan-translate ingress**	Obrigatório, a função de tradução pode ser habilitada tanto a entrada quanto a saída
(Des)Habilite a função de tradução para a saída de pacotes	**[no]vlan-translate egress**	Obrigatório, a função de tradução pode ser habilitada tanto a entrada quanto a saída
Visualização da tabela de tradução de entrada	**show vlan-translate ingress table [**start-vid end-vid**]**	Opcional
Visualização da tabela de tradução de saída	**show vlan-translate egress table [**start-vid end-vid**]**	Opcional

Operação	Comando	Obrigatório/ opcional
Visualização do estado da função de tradução (habilitado ou desabilitado	**show vlan-translate interface [{ethernet | pon}** port-number**]**	Opcional

Obs.: *a tradução da VLAN pode ser dividida em tradução de entrada e tradução de saída. Ao configurar a tabela VLAN-Translate de entrada, você deve habilitar o VLAN-Translate ingress e adicionar a New_VLAN na entrada, mas não é necessário adicionar a OLD_VLAN; ao configurar a tabela VLAN-Translate de saída, você deve habilitar o VLAN-Translate egress e adicionar a OLD_VLAN na entrada, mas não há necessidade de adicionar a New-VLAN.*

Configuração de VLAN-Swap

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
Configuração da tabela de tradução de VLAN	**vlan-swap** start-vid end-vid swap-vid	Obrigatório
Remover tabela de tradução de VLAN	**no vlan-swap [all |** start-vid end-vid]	Opcional
Visualização da tabela de tradução	**show vlan-swap interface [{ethernet | pon}** port-number**]**	Opcional

Obs.: *VLAN-Swap só suporta tradução de entrada, e a porta de entrada deve adicionar a New_VLAN, mas não precisa adicionar a OLD_VLAN.*

Exemplo de configuração de VLAN-Swap N:1

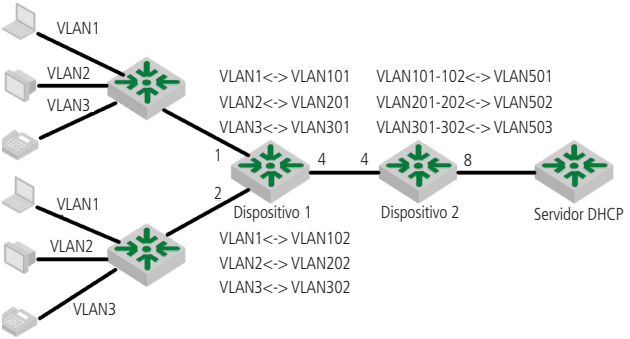
» Requisitos de rede:

Em uma célula de rede, o provedor de serviços fornece três tipos de serviços de aplicativos de dados: PC, Vídeo e VoIP, que estão conectados à rede doméstica. Cada usuário acessa o OLT através do gateway doméstico e obtém automaticamente um endereço IP via DHCP. Ao distribuir o gateway doméstico para o usuário, o provedor de serviços executa configurações unificadas no gateway doméstico: o serviço do PC é dividido em VLAN 1, o serviço Vídeo é dividido em VLAN 2 e o serviço VoIP é dividido em VLAN 3.

O Dispositivo 1 marcou cada serviço de cada usuário com uma VLAN separada para distinguir os mesmos serviços de diferentes usuários, além de evitar vazamentos de informações e ataques maliciosos entre usuários.

O Dispositivo 2 precisa classificar os dados de acordo com o tipo de serviço para salvar os recursos da VLAN. Entre eles: o tráfego do PC é transmitido através da VLAN 501, o serviço Vídeo é transmitido através da VLAN 502 e o serviço VoIP é transmitido através da VLAN 503.

O diagrama de rede é o seguinte:



Esboço mapa de VLAN-Swap N:1

» Configuração do dispositivo 1:

» Crie a VLAN e adicione a porta na VLAN correspondente:

OLT4840E(config)#vlan 1,2,3,101,201,301,102,202,302

OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#switchport hybrid tagged vlan 101,201,301

OLT4840E(config-if-ethernet-0/1)#interface ethernet 0/2

OLT4840E(config-if-ethernet-0/2)#switchport hybrid tagged vlan 102,202,302

OLT4840E(config-if-ethernet-0/2)#interface ethernet 0/4

OLT4840E(config-if-ethernet-0/4)#switchport hybrid tagged vlan 101,201,301, 102,202,302

» Configure a tabela de vlan swap para as portas e0/1 e e0/2:

OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#vlan-swap 1 1 101

OLT4840E(config-if-ethernet-0/1)#vlan-swap 2 2 201

OLT4840E(config-if-ethernet-0/1)#vlan-swap 3 3 301

OLT4840E(config)#interface ethernet 0/2

OLT4840E(config-if-ethernet-0/2)#vlan-swap 1 1 102

OLT4840E(config-if-ethernet-0/2)#vlan-swap 2 2 202

OLT4840E(config-if-ethernet-0/2)#vlan-swap 3 3 302

» Configuração do dispositivo 2:

» Crie a tradução de VLAN (OLD_VLAN e New_VLAN) que inclua a portas de uplink e downlink:

OLT4840E(config)#vlan 101,201,301,102,202,302,501,502,503

OLT4840E(config)#interface ethernet 0/4

OLT4840E(config-if-ethernet-0/4)#switchport hybrid tagged vlan 101,102,201,202,301,302

OLT4840E(config-if-ethernet-0/4)#interface ethernet 0/8

OLT4840E(config-if-ethernet-0/8)#switchport hybrid tagged vlan 501,502,503

» Configure a tabela de tradução de saída no modo de configuração global; habilite o VLAN-Translate na saída:

OLT4840E(config)#vlan-translate egress table 101 102 501

OLT4840E(config)#vlan-translate egress table 201 202 502

OLT4840E(config)#vlan-translate egress table 301 302 503

OLT4840E(config)#interface ethernet 0/8

OLT4840E(config-if-ethernet-0/8)#vlan-translate egress

» Validação de resultado:

» Capture os pacotes de saída no dispositivo 1 (e0/4), você pode capturar o pacote com as tags VLAN 101, VLAN 201, VLAN 301, VLAN 202, VLAN 302.

» Capture os pacotes de saída no dispositivo 2 (e0/8), você pode capturar o pacote com as tags VLAN 501, VLAN 502, VLAN 503.

4.6. Configuração de VLAN baseada em MAC Address

Visão geral da VLAN baseada em MAC Address

Conforme mencionado anteriormente, uma única porta na rede do campus possui vários serviços e cada serviço pertence a diferentes VLANs. Portanto, a configuração flexível sob uma única porta tornou-se uma questão chave para o gerenciamento de rede.

Para resolver este problema, a VLAN baseada em MAC é proposta. O endereço MAC (Media Access Control) é gravado em uma placa de interface de rede (NIC), também conhecido como o endereço de hardware. Ele é composto de 48 bits de comprimento (6 bytes), 16 dígitos hexadecimais.

Na VLAN baseada em MAC, a tag da VLAN é adicionada ao pacote de acordo com o seu endereço MAC de origem. Isso geralmente é combinado com outras tecnologias de segurança (como 802.1X) para alcançar uma maior segurança do terminal, mesmo com um acesso flexível.

Configuração de VLAN baseada em MAC

» Requisitos de rede:

Conforme exibido a seguir, as portas 1 do dispositivo 1 e dispositivo 2 conectam duas salas de reunião, respectivamente; PC1 e PC2 são os laptops que serão usados durante a reunião.

PC1 e PC2 pertencem respectivamente a dois departamentos, e esses dois departamentos são isolados pela VLAN 100 e pela VLAN 200. O requisito é que, independentemente da sala de reunião em que estes dois laptops sejam utilizados, eles só podem acessar os servidores de seus próprios departamentos, que são o servidor 1 e o servidor 2. O endereço MAC do PC1 é 00:00:00:11:22 e o endereço Mac do PC2 é 00:00:00:00:11:33.

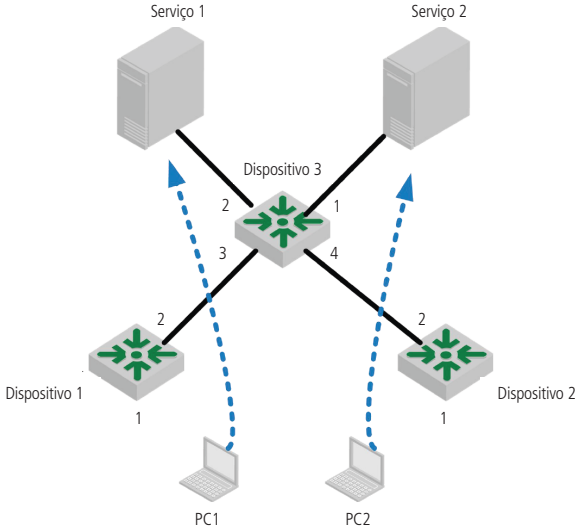


Diagrama de rede para VLAN baseada em MAC

» Passos de configuração:
  » Configuração do dispositivo 1:
    » Crie a VLAN 100 e a VLAN 200, então configure a porta 2 como trunk, para permitir que os pacotes de VLAN 100 e VLAN 200 possam ser transmitidos:

```
OLT4840E>enable
OLT4840E#configure terminal
OLT4840E(config)#
OLT4840E(config)#vlan 100,200
OLT4840E(config-if-vlan)#exit
OLT4840E(config)#interface ethernet 0/2
OLT4840E(config-if-ethernet-0/2)#switchport mode trunk
OLT4840E(config-if-ethernet-0/2)#switchport trunk allowed vlan 100,200
```

» Configure a porta 1 como hybrid e remova a tag VLAN quando pacotes das VLAN 100 e VLAN 200 forem encaminhados:

OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#switchport mode hybrid

OLT4840E(config-if-ethernet-0/1)#switchport hybrid untagged vlan 100,200

» Associe o endereço MAC do PC1 a VLAN 100 e o endereço MAC do PC2 a VLAN 200, habilite a MAC-VLAN:

OLT4840E(config)#vlan-mac-table 00:00:00:00:11:22 100 0

OLT4840E(config)#vlan-mac-table 00:00:00:00:11:33 200 0

» Configuração do Dispositivo 2:

A configuração do dispositivo 2 é totalmente igual à configuração do dispositivo 1, de modo que não será exibido aqui novamente.

» Configuração do Dispositivo 3:

» Crie a VLAN 100 e a VLAN 200 e adicione as portas 3 e 4 nestas duas VLANs:

OLT4840E(config)#vlan 100,200

OLT4840E(config-if-vlan)#switchport ethernet 0/3 ethernet 0/4

» Configure as portas 1 e 2 como trunk para permitir que os pacotes VLAN 100 e VLAN 200 sejam transmitidos:

OLT4840E(config)#interface range ethernet 0/1 ethernet 0/12

OLT4840E(config-if-range)#switchport mode trunk

OLT4840E(config-if-range)#switchport trunk allowed vlan 100,200

» Validação dos resultados.

Não importa em qual sala de reuniões estes dois laptops são utilizados, eles só podem acessar os servidores de seus próprios departamentos.

4.7. VLAN Baseada em protocolo

Configuração da VLAN baseada em protocolo

VLAN baseada em protocolo: o pacote distribui um ID de VLAN diferente de acordo com os tipos de protocolo e os formatos de encapsulamento. Os *tipos de protocolo + formatos de encapsulamento* também são chamados de *modelo de acordo*. Um protocolo VLAN pode ser capaz de vincular vários *modelos de acordos*, assim os pacotes recebidos/enviados podem ser modificados para carregar a tag da VLAN referente ao seu serviço.

Processamento de pacotes untagged (sem tag VLAN)

1. Se os tipos de protocolo de pacotes e os formatos de encapsulamento estiverem em conformidade com os *modelos de acordos*, ele será marcado com o VLAN-ID;
2. Se os tipos de protocolo de pacotes e os formatos de encapsulamento não estiverem em conformidade com os *modelos de acordos*, ele será marcado com a ID da VLAN padrão da porta.

Processamento de pacotes tagged (com tag VLAN)

1. Se os tipos de protocolo de pacotes e os formatos de encapsulamento estiverem em conformidade com os *modelos de acordos*, a informação da SVLAN será modificada para o VLAN-ID;
2. Se os tipos de protocolo de pacotes e os formatos de encapsulamento não estiverem em conformidade com os *modelos de acordos*, o modo de processamento será o mesmo que do VLAN baseado em porta.

Esse recurso é aplicado principalmente para vincular o tipo de serviço com uma VLAN, proporcionando gerenciamento e manutenção conveniente.

Existem modos de configuração de dois tipos de VLAN baseada em protocolo. Escolha o adequado de acordo com o tipo de equipamento.

Configuração de VLAN baseado em protocolo (método um)

» Configuração de VLAN baseado protocolo:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de modelo de protocolo	**vlan-protocol table** index index **ethertype** etype-id **protocol** {ethernetv2|non-snap-llc|snap-llc}	Obrigatório, não há nenhum protocolo por padrão
Remover modelo de protocolo	**no vlan-protocol table [index** index**]**	Opcional
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	Obrigatório
Configuração para associar o modelo de protocolo e configuração da VLAN por protocolo	**vlan-protocol** table **index index vlan** v-id	Obrigatório

Operação	Comando	Obrigatório/ opcional
Desassociar o modelo de protocolo	**no vlan-protocol table [index** index**]**	Opcional
Visualização da configuração do modelo de protocolo	**show vlan-protocol {table | interface [{ethernet | pon}** port-number**]}**	Opcional

Configuração de VLAN baseado em protocolo (método dois)

» Configuração de VLAN baseado protocolo:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de modelo de protocolo	**vlan-protocol frametype {8023-llc-snap|8023-llc|ethernet2}** ethertype **interface {ethernet | pon}** port-number vlan-id	Obrigatório
Remover modelo de protocolo	**no vlan-protocol [frametype {8023-llc-snap|8023-llc|ethernet2}** ethertype **interface {ethernet | pon}** port-number**]**	Opcional
Visualização da configuração do modelo de protocolo	**show vlan-protocol [frametype {8023-llc-snap|8023-llc|ethernet2}** ethertype **interface {ethernet | pon}** port-number vlan-id]	Opcional

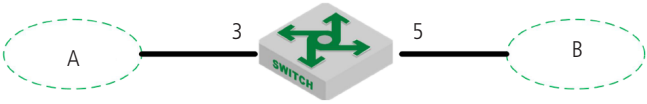
Exemplo de VLAN baseado em protocolo (método um)

» Requisitos de rede.

Crie a VLAN 10 e em seguida configure o modelo do protocolo, o valor do índice do modelo é 1, o tipo de protocolo é 0×0800, com o encapsulamento Ethernet v2.

Ele requer fluxo de dados IP com encapsulamento Ethernet v2 da porta 3, adicione a tag de VLAN 10.

O diagrama de rede é o seguinte:



Dispositivo A

Diagrama de rede para VLAN baseada em protocolo

» Passos de configuração:
  » Crie a VLAN 10 e o adicione a todas as portas
    OLT4840E(config)#vlan 10
    OLT4840E(config-if-vlan)#switchport all
    Add VLAN port successfully.
  » Configure a porta 5 para inserir a tag VLAN 10 em sua saída:
    OLT4840E(config)#interface ethernet 0/5
    OLT4840E(config-if-ethernet-0/5)#switchport hybrid tagged vlan 10
    OLT4840E(config-if-ethernet-0/5)#exit
  » Crie o modelo de protocolo, tipo de protocolo 0×0800 com encapsulamento ethernetv2:
    OLT4840E(config)#vlan-protocol table index 1 ethertype 0800 protocol ethernetv2
  » Configurar a entrada para habilitar a função de protocolo VLAN em primeiro lugar. Em seguida, vincule o índice do modelo de protocolo e configure o protocolo VLAN 10.
    OLT4840E(config)#interface ethernet 0/3
    OLT4840E(config-if-ethernet-0/3)#vlan-protocol
    OLT4840E(config-if-ethernet-0/3)#vlan-protocol table index 1 vlan 10
» Visualização de resultados e validação:
  OLT4840E(config)#show vlan-protocol table
  index ethertype protocol
  1 0x0800 EthernetV2
  OLT4840E(config)#show vlan-protocol interface ethernet 0/3
  e0/3: : enable
  global protocol-vlan table index 1 vlan 10
  Resultado: todo o fluxo de dados IP ethernetv2 que entra da porta 3 deve adicionar a tag VLAN 10 antes de transmitir.

4.8. VLAN baseado em sub-rede IP

Visão geral de VLAN baseada em sub-rede IP

O VLAN baseado em sub-rede IP é dividido de acordo com o endereço IP da fonte do pacote e a máscara de sub-rede. Depois que o dispositivo recebeu pacotes da interface, ele confirmará os pacotes pertencentes à VLAN e em seguida dividirá esses pacotes automaticamente entre VLANs específicas para transmitir.

Esse recurso é usado principalmente para o endereço de IP ou a transmissão de mensagens de segmento de rede na VLAN específica.

Configuração de VLAN baseada em sub-rede IP

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
(Des)Habilite a VLAN baseada em sub-rede IP	**[no]vlan-subnet precede**	Obrigatório
Configuração da tabela de VLAN baseada em sub-rede IP	**ip-subnet-vlan ipaddress** *mask vlan-id priority*	Obrigatório
Remover a tabela de sub-rede IP	**no ip-subnet-vlan** *ipaddress mask*	Opcional
Visualização da tabela de sub-rede	**show ip-subnet-vlan [***ipaddress*| *mask***]**	Pode ser executada em qualquer modo

Exemplo da configuração

» Requisitos de rede:

Uma rede empresarial aloca cada sub-rede IP de acordo com o tipo de serviço. O requisito é que diferentes usuários de sub-rede adotem diferentes caminhos de transmissão para acessar o servidor upstream.

Como exibido a seguir:

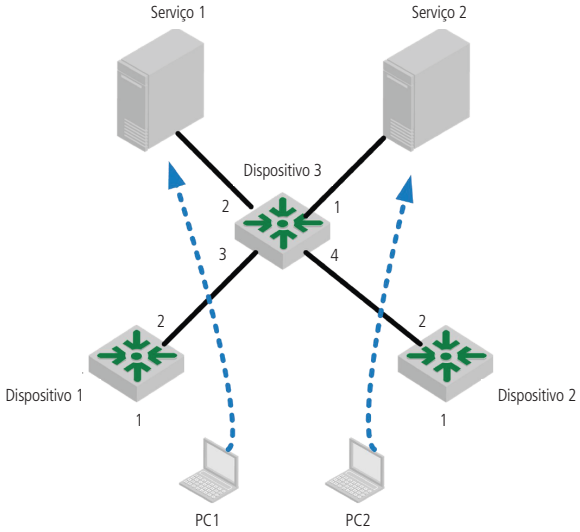


Diagrama de VLANs baseadas em sub-redes IP

Os pacotes do Dispositivo 1 incluem dados, IPTV, voz e assim por diante. Os seus endereços IP são diferentes uns dos outros. Configure a VLAN baseada em sub-rede IP no Dispositivo 1. Depois de receber os pacotes de serviço, o dispositivo dividirá automaticamente esse pacote em VLANs de acordo com o IP de origem diferente.

Além disso, o dispositivo encaminhará esses pacotes para o servidor superior.

» Passos de configuração:

  » Crie a VLAN e inclua as interfaces:

  OLT4840E(config)#vlan 100,200,300

  OLT4840E(config-if-vlan)#switchport ethernet 0/1 ethernet 0/2 ethernet 0/3

» Habilite a VLAN baseada em sub-rede IP e configure a tabela de sub-rede IP
OLT4840E(config)#vlan-subnet precede
OLT4840E(config)#ip-subnet-vlan 192.168.1.1 255.255.255.0 100 0
OLT4840E(config)#ip-subnet-vlan 192.168.1.2 255.255.255.0 200 0
OLT4840E(config)#ip-subnet-vlan 192.168.1.3 255.255.255.0 300 0
OLT4840E(config)#

Obs.: *garanta que a interface de uplink possua as VLANs 100, 200, 300 com tag.*

» Validação de resultado:
OLT4840E(config)#show run garp
![GARP]
vlan-subnet precede
ip-subnet-vlan 192.168.1.1 255.255.255.0 100 0

4.9. Configuração de VLAN-Trunking

Visão geral de VLAN-Trunking

VLAN-Trunking é usado para transmitir de forma transparente mensagens desconhecidas. Explicação:

» Cada OLT configura apenas um conjunto de VLAN-Trunking.
» Cada VLAN-Trunking inclui duas interfaces: uplink e downlink.
» Transmite a mensagem desconhecida e não realiza nenhuma alteração.
» Não aprende o endereço MAC da mensagem desconhecida.
» O mecanismo da mensagem conhecida é o mesmo que a VLAN 802.1Q.

Configuração de VLAN-Trunking

» Configuração de VLAN-Trunking:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da table de VLAN-Trunking	**vlan-trunking {ethernet | pon} port-number{ethernet | pon} port-number**	Obrigatório
Desabilite o VLAN-Trunking	**no vlan-trunking**	Opcional
Visualização da tabela de VLAN-Trunking	**show vlan-trunking**	Opcional

Exemplo de configuração de VLAN-Trunking

» Requisitos de rede:

As configurações padrão do equipamento exigem o fluxo de serviço de qualquer porta (o pacote não precisa ter tag) sendo encaminhado com sucesso.

» Passos de configuração:

Habilite o VLAN-Trunking, e depois especifique a porta e então especifique a porta de uplink do pacote que entra na interface 0/4 seja encaminhado para interface 0/8.

OLT4840E(config)#vlan-trunking ethernet 0/4 ethernet 0/8

Create VLAN Trunking successfully.

OLT4840E(config)#show vlan 100

The VLAN does not exist.

» Validação de resultado:

O pacote não carrega VLAN na interface 0/4, e o pacote pode sair na interface 0/8, ou seja, o equipamento pode ser capaz de transmitir pacote sem VLAN.

5. Configuração de tabela de endereço MAC

5.1. Configuração da tabela de endereços MAC

O sistema mantém uma tabela para encaminhamento de pacotes. Um item desta tabela contém o endereço MAC do dispositivo, a ID da VLAN e o número da porta do OLT que os pacotes entraram. Quando um pacote entra no OLT, é feita uma procura na tabela com base no endereço MAC de destino e na ID da VLAN do pacote. Se for encontrado, eles serão enviados para as portas especificadas.

Se o endereço de origem de um pacote recebido não existir na tabela, o sistema irá adicioná-lo juntamente da ID da VLAN e o número da porta do pacote recebido como uma nova entrada.

O administrador pode configurar a tabela de endereços MAC manualmente com base na condição real da rede, ou seja, o administrador pode adicionar ou modificar entradas estáticas, permanentes, de balckhole e dinâmicas.

O sistema fornece a função de validade do endereço MAC. Se um dispositivo não enviar pacotes em um determinado período de tempo, o sistema exclui as entradas associadas ao dispositivo. O envelhecimento só produz efeitos no endereço MAC aprendido ou nas entradas que podem ser envelhecidas (as entradas de endereço MAC dinâmicas que são configuradas pelo usuário).

Configuração do tempo de validade da tabela de endereços MAC

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
-	**mac-address-table age-time {**second| **disable}**	Unidade de tempo de envelhecimento é segundos; desativar significa que o endereço MAC nunca será excluído da tabela.
Visualização o tempo de validade da tabela MAC	**show mac-address-table age-time**	Opcional

Adicionar um endereço na tabela MAC manualmente

Além das entradas aprendidas dinamicamente, a tabela de endereços MAC pode ser adicionada manualmente.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar entrada manual	**mac-address-table { static | permanent | dynamic } H:H:H:H:H:H interface Ethernet** interface-num **vlan** vlan-id	Obrigatório
Visualização da tabela MAC	**show mac-address-table { static| permanent| dynamic| blackhole|vlan|interface {ethernet | pon}** port-number **}**	Opcional

- **Stactic:** endereço MAC estático, não será envelhecido.
- **Permanent:** endereço MAC permanente. Será descartado da tabela após um certo período de tempo. Se você salvar as configurações, as entradas continuarão a existir depois que o dispositivo for desligado.
- **Dynamic:** endereço MAC dinâmico e será descartado da tabela após um certo período de tempo.

Adicionar endereço MAC blackholes

É possível adicionar MACs a blackhole, ou seja, quando o endereço de origem ou o endereço de destino do pacote é um endereço que foi cadastrado, o OLT descarta o pacote.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
-	**mac-address-table blackhole** H:H:H:H:H:H vlan vlan-id	Obrigatório

Modificar o tipo da tabela MAC

Existem dois tipos de tabelas MAC:

- **IVL:** aprendizagem de VLAN independente. Cada VLAN possui uma tabela de mapeamento MAC-port; um MAC pode aparecer em múltiplas tabelas de mapeamento.
- **SVL:** aprendizagem de VLAN compartilhada. SVL refere-se a uma tabela grande no OLT. Todas as VLANs compartilham esta tabela e um MAC pertence apenas a uma VLAN, ou seja, um endereço só pode aparecer em uma tabela de mapeamento.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Modificar o tipo de tabela MAC	**mac-address-table learning mode {ivl | svl}**	Valor padrão é *IVL*. Para a modificação ocorrer, é necessário reiniciar o equipamento.

Habilitar/desabilitar o aprendizado da tabela de endereços MAC

Você pode configurar se o dispositivo aprende os endereços MAC dinamicamente ou não.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
(Des)Habilitar o aprendizado da tabela MAC	**[no] mac-address-table learning**	Habilitado por padrão
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
(Des)Habilitar o aprendizado da tabela MAC	**(no) mac-address-table learning**	Obrigatório
Visualização do estado de aprendizado da tabela MAC (habilitado/desabilitado)	**show mac-address learning [interface [interface-num]]**	Opcional

Obs.: *se a aprendizagem do endereço MAC estiver desativada no modo de configuração global, todas as portas não poderão aprender o endereço MAC; se você deseja desabilitar o aprendizado em algumas portas, ative o aprendizado no modo de configuração global e desative na porta.*

Limitação da quantidade de endereços na tabela MAC

Sob o modo de configuração da porta, você pode configurar o número máximo de endereços MAC aprendidos em uma porta. Por padrão, o número de tabela de aprendizado de endereços MAC é ilimitado.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Ativar limitação de quantidade de aprendizado na tabela de endereços MAC do grupo de agregação	**mac-address-table max-mac-count** integer **channel-group** id	Funciona apenas em grupos de agregação
Desativar limitação de quantidade de aprendizado na tabela de endereços MAC do grupo de agregação	**no mac-address-table max-mac-count** integer **channel-group** id	Opcional

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
Ativar limitação de quantidade de aprendizado na tabela de endereço MAC	**mac-address-table max-mac-count** integer	Funciona para apenas uma porta
Desativar limitação de quantidade de aprendizado na tabela de endereço MAC	**no mac-address-table max-mac-count**	Opcional
Visualizar o número máximo de endereços na tabela	**show mac-address max-mac-count [interface [interface-num]]**	Opcional

5.2. Função de switch local

Normalmente o OLT não encaminha os pacotes recebidos da porta. No entanto, você pode precisar encaminhar os pacotes que vêm da porta. Neste caso, você pode usar o switch local.

Configuração de switch local

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de encaminhamento local	**[no] local-switch**	Opcional
Visualização das configurações	**show local-switch [interface {ethernet | pon}** port-number**]**	Opcional

Exemplo de configuração de switch local

» Requisitos de rede:
Habilitar o encaminhamento na porta 0/1.

» Passos de configuração:
OLT4840E(config)#show local-switch interface ethernet 0/1

port local-switch-state

e0/1 disable

Total entries: 1 .

OLT4840E(config)#interface ethernet 0/1
OLT4840E(config-if-ethernet-0/1)#local-switch
Setting successfully! local-switch is enable

OLT4840E(config)#interface ethernet 0/1
OLT4840E(config-if-ethernet-0/1)#show local-switch interface ethernet 0/1
port local-switch-state
e0/1 enable
Total entries: 1 .

OLT4840E(config-if-ethernet-0/1)#no local-switch
Setting successfully! local-switch is disable

OLT4840E(config-if-ethernet-0/1)#show local-switch interface ethernet 0/1
port local-switch-state
e0/1 disable
Total entries: 1 .

5.3. Função *SLF-control*

Por padrão o OLT encaminha pacotes de origem desconhecidas sem precisar ser gerenciado pelo administrador da rede de acordo com a política de segurança. Você pode desativar a função de encaminhamento de pacotes de origem desconhecida usando um comando especificado, nesse caso, quando o dispositivo recebe um pacote, ele verifica se o MAC de origem existe na tabela MAC ou não. Se não existir, ele descarta o pacote. Assim ele só pode encaminhar o pacote cujo endereço de origem é conhecido.

Configuração do SLF-control

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	Obrigatório

Operação	Comando	Obrigatório/ opcional
Desabilitar a função de encaminhar pacotes com endereço MAC desconhecido	**[no] src_dlf_forward**	Obrigatório
Habilitar a função de encaminhar pacotes com endereço MAC desconhecido	**src_dlf_forward**	Obrigatório
Visualização da configuração	**show src_dlf_forward interface [ethernet** port-number**]**	Opcional

Esta função geralmente é combinada com a função de aprendizagem ou limite endereço MAC da porta.

Exemplo de configuração de SLF-control

» Requisitos de rede:
Desabilite a função de encaminhamento de pacotes com origem desconhecida na porta 0/9.

» Passos de configuração:

```
OLT4840E(config)#show src_dlf_forward interface ethernet 0/9
Port    src_dlf_forward status
0/9     enable
OLT4840E(config)#interface ethernet 0/9
OLT4840E(config-if-ethernet-0/9)#no src_dlf_forward
OLT4840E(config-if-ethernet-0/9)#no mac-address-table learning
OLT4840E(config-if-ethernet-0/9)#show src_dlf_forward interface ethernet 0/9
Port    src_dlf_forward status
0/9     disable
```

5.4. Visão geral de DLF-control

Os pacotes desconhecidos são classificados em pacotes unicast e multicast desconhecidos.

Os pacotes unicast desconhecidos são pacotes em que não foi possível encontrar o endereço MAC de destino na tabela MAC.

Os pacotes multicast desconhecidos são pacotes em que não foi possível encontrar endereço MAC de destino dos pacotes multicast na tabela MAC multicast.

Configuração de DLF-control

» Se habilitado, com base na configuração global este comando entrará em vigor em pacotes de saída de todas as portas.

» Se for habilitado, com base na configuração da interface este comando entrará em vigor nos pacotes de saída da porta em questão.

Por padrão, pacotes desconhecidos podem ser encaminhados.

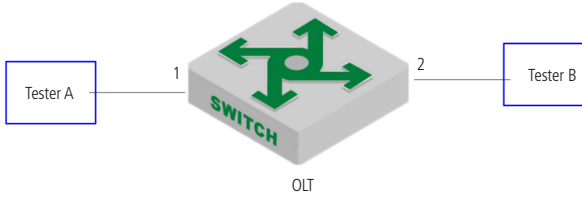
» Configuração de encaminhamento DLF:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar a função de encaminhamento de pacotes unicast desconhecidos	**[no]dlf-forward unicast**	Opcional, habilitado por padrão
Habilitar a função de encaminhamento de pacotes multicast desconhecidos	**[no]dlf-forward multicast**	Opcional, habilitado por padrão
Acesse o modo de configuração de interface	**{ethernet | pon}** port-number	-
Habilitar a função de encaminhamento de pacotes unicast desconhecidos	**[no]dlf-forward unicast**	Opcional, habilitado por padrão
Habilitar a função de encaminhamento de pacotes multicast desconhecidos	**[no]dlf-forward multicast**	Opcional, habilitado por padrão
Visualização de configuração do encaminhamento DLF	**show dlf-forward interface [{ethernet | pon}** port-number**]**	Opcional

Exemplo de configuração de DLF-control

» Requisitos de rede:

Configure a saída da porta 2 para não encaminhar pacotes de unicast desconhecidos.



Esboço de mapa de DLF-control

» Desativar a função de encaminhamento da porta 2 de pacotes de unicast desconhecidos:

OLT4840E(config-if-ethernet-0/1)#no dlf-forward unicast

» Exiba as configurações:

OLT4840E(config-if-ethernet-0/1)#show dlf-forward interface ethernet 0/2

Forwarding unknown unicast packets global status: enable

Forwarding unknown multicast packets global status: enable

Port	Forwarding Unknown Unicast	Forwarding Unknown Multicast
e0/1	disable	enable

» Validação de resultados:

(1) O tester A envia um pacote desconhecido e o tester B não recebe o pacote.

(2) O tester A envia um pacote conhecido e o tester B recebe o pacote.

6. Configuração de multicast

6.1. Configuração de IGMP-Snooping

Visão geral de IGMP-Snooping

IGMP (*Internet Group Management Protocol*) é uma parte do protocolo IP usado para suportar e gerenciar o multicast entre host e roteador multicast. Esta função permite a transferência de dados para uma coleção de hosts formada pelo grupo multicast. A relação do membro do grupo é dinâmica e o host pode entrar ou sair dele para reduzir a carga da rede ao mínimo, deixanto a transmissão de dados na rede mais efetiva.

O IGMP-Snooping é usado para monitorar o pacote IGMP entre host e roteadores. Ele pode criar, manter e excluir dinamicamente uma tabela de endereço multicast de acordo com a entrada e saída dos membros do grupo. Assim, o quadro multicast pode transferir o pacote de acordo com a sua própria tabela de endereço multicast.

Habilitar IGMP-Snooping

» Configuração do IGMP-Snooping:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o IGMP-Snooping	**imgp-snooping**	Obrigatório
Desligar o IGMP-Snooping	**no igmp-snooping**	Opcional

Configuração do controle de tempo do IGMP-Snooping

» Configuração do controle de tempo do IGMP-Snooping:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o tempo de envelhecimento dos membros multicast dinâmicos	**imgp-snooping host-aging-time** time	Opcional, por padrão o tempo de envelhecimento é de *300s*

Operação	Comando	Obrigatório/ opcional
Desativar o envelhecimento dos membros multicast dinâmicos	**no igmp-snooping** host-aging-time	Opcional
Configuração do tempo máximo de resposta do IGMP-Snooping	**igmp-snooping max-response-time** time	Opcional. Configure o tempo máximo de espera para que as portas do grupo sejam removidas depois de receber mensagens de saída. A configuração padrão é *10* segundos.
Desabilitar o tempo máximo de resposta do IGMP-Snooping	**no igmp-snooping max-response-time**	Opcional

Configuração de fast-leave (saída rápida)

Geralmente, depois de receber uma mensagem IGMP de saída (leave), IGMP-Snooping não exclui a porta diretamente do grupo multicast, ele aguarda um período de tempo antes de executar esta ação.

Se você habilitar o fast-leave, o IGMP-Snooping remove a porta diretamente do grupo multicast ao receber uma mensagem IGMP de saída. Quando existe apenas um usuário sob a porta, o fast-leave pode economizar a largura de banda.

» Configuração do fast-leave:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	

Operação	Comando	Obrigatório/ opcional
Configuração do fast-leave	**igmp-snooping fast-leave**	Opcional, por padrão esta função está desabilitada
Remover a configuração de fast-leave	**no igmp-snooping fast-leave**	Opcional

Configuração de número máximo de aprendizagem de grupos multicast

Use os seguintes comandos para configurar o número máximo de aprendizado de grupos multicast.

» Configuração de número máximo de aprendizagem de grupos multicast

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
Configuração de número máximo de aprendizagem de grupos multicast	**igmp-snooping group-limit** number	Opcional
Desabilitar a configuração de número máximo de aprendizagem de grupos multicast	**no igmp-snooping group-limit**	Opcional
Configure a ação quando a porta estiver cheia de grupos multicast	**igmp-snooping group-limit action** {replace | drop}	Opcional

Obs.: *o limite de grupo de IGMP-Snooping não se refere apenas ao número máximo de multicast que a porta pode aprender, mas também refere-se ao número máximo de multicast que a máquina pode aprender.*

Configuração da estratégia de aprendizado de multicast do IGMP-Snooping

Depois que uma estratégia de aprendizagem multicast for configurada, o administrador pode controlar o roteador para aprender apenas um grupo multicast específico. Se um grupo for adicionado à blacklist (lista negra), o roteador não aprenderá o grupo multicast; se um grupo multicast for adicionado à whitelist (lista branca), o roteador irá aprender este grupo multicast.

» Configuração da estratégia de aprendizado de multicast do IGMP-Snooping:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da regra padrão de grupos multicast fora da blacklist ou whitelist	**igmp-snooping** { permit | deny } **{ group all | vlan** vid **}**	Opcional, por padrão, a regra de aprendizagem de um grupo multicast é aprender todos os grupos multicast
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
Configuração de blacklist e whitelist dos grupos multicast	**igmp-snooping { permit | deny }** group-range MAC **multi-count** num **vlan** vid	Opcional
	igmp-snooping { permit | deny } group MAC **vlan** vid	Opcional, por padrão, nenhum grupo multicast será adicionado a blacklist ou whitelist

Configuração do IGMP-Snooping querier

Em uma rede multicast que executa IGMP, um roteador multicast é responsável pelo envio de consultas IGMP. Portanto, a função de consulta não pode ser implementada e a consulta de grupo comum não pode ser realizada.

Você pode configurar um Querier de IGMP-Snooping para habilitar o OLT para enviar ativamente uma mensagem de consulta geral para estabelecer e manter entradas de encaminhamento multicast. Você também pode configurar a VLAN, o endereço de origem, o tempo de resposta máximo e o intervalo de consulta para este querier enviar mensagens de consulta gerais.

» Configuração do IGMP-Snooping querier:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o IGMP-Snooping querier	**igmp-snooping querier**	Obrigatório
Desabilitar o IGMP-Snooping querier	**no igmp-snooping querier**	Opcional
Configuração da versão da consulta	**igmp-snooping querier version id**	Opcional, *Versão2* por padrão
Configuração das VLANs para pacotes de consulta gerais	**igmp-snooping querier-vlan** vid	Opcional
Remover configuração das VLANs para pacotes de consulta gerais	**no igmp-snooping querier-vlan** vid	Opcional
Configuração do intervalo de envio de pacotes de consulta geral	**igmp-snooping query-interval** interval	Opcional
Remover o intervalo de envio de pacotes de consulta geral	**no igmp-snooping query-interval**	Opcional
Configuração do tempo de resposta máximo para consulta gerais	**igmp-snooping query-max-respond** time	Opcional
Desabilitar o tempo de resposta máximo para consulta gerais	**no igmp-snooping query-max-respond**	Opcional
Configuração do IP de origem para envio de consulta geral	**igmp-snooping general-query source-ip ip**	Opcional
Desabilitar o IP de origem para envio de consulta geral	**no igmp-snooping general-query source-ip**	Opcional

Configuração de VLAN multicast

Depois que a função *VLAN multicast* estiver ativada em uma porta, o OLT altera o pacote IGMP para uma VLAN multicast, independentemente da VLAN à qual o pacote IGMP recebido pertence.

» Configuração de VLAN multicast:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	
Configuração da VLAN multicast na porta	**igmp-snooping multicast vlan** vid	Opcional
Desabilitar a VLAN multicast na porta	**no igmp-snooping multicast vlan**	Opcional

Configure a porta para armazenar o endereço MAC do host

Quando esta função está ativada na porta, o OLT grava o endereço de MAC da origem do pacote de relatório IGMP.

» Configure a porta para armazenar o endereço MAC do host:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	
Configure a porta para armazenar o endereço MAC do host	**igmp-snooping record-host**	Opcional
Desabilitar a porta para armazenar o endereço MAC do host	**no igmp-snooping record-host**	Opcional

Configuração da supressão de relatórios multicast

Depois de ativar a supressão de relatório de IGMP-Snooping:

1. Cada grupo enviará apenas um relatório para a porta Mroute (quando o primeiro relatório é recebido, o MAC da fonte é substituído pelo MAC do OLT e enviado para a porta do Mroute) e ele não será encaminhado. Se receber um relatório do mesmo grupo mais tarde, somente as informações do membro local ou do timer serão atualizadas e ele não será enviado para a porta mroute;

2. Depois de receber uma consulta geral, o OLT encapsula todos os pacotes no pacote de relatório para a porta mroute e em seguida, encaminha esta consulta para todos os clientes. Ao receber uma consulta específica, o OLT encapsula o grupo especificado em um pacote de relatório e o envia para a porta Mroute. Se o grupo especificado não estiver na tabela do OLT, ele descartará diretamente a consulta;
3. Depois de receber um relatório de saída, se houver outros membros no grupo, o OLT apaga o membro recebido, e não envia um relatório de saída para a porta de comando; se for o último membro, basta substituir o MAC da fonte com o MAC da OLT e depois enviá-lo para a porta Mroute.

» Configuração da supressão de relatórios multicast:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da supressão de relatórios multicast	**igmp-snooping report-suppression**	Opcional
Desabilitar a supressão de relatórios multicast	**no igmp-snooping report-suppression**	Opcional

Configuração de descarte de pacotes de consultas/relatórios

Quando esta função está habilitada na porta, o dispositivo descarta pacotes de consulta / relatório IGMP. A porta padrão recebe todas as mensagens IGMP.

» Configuração de descarte de pacotes de consultas/relatórios:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	
Configure a porta para descartar pacotes de consulta/ relatório	**igmp-snooping drop {query|report}**	Opcional
Configure a porta para receber pacotes de consulta/relatório	**no igmp-snooping drop {query|report}**	Opcional

Configuração da função de pré-visualização multicast

IGMP-Snooping fornece a função de pré-visualização multicast. Você pode configurar o canal, duração, intervalo, duração da reposição e os tempos de pré-visualização permitidos.

» Configuração da função de pré-visualização multicast:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da função de pré-visualização multicast	**igmp-snooping preview**	Opcional
Desabilitar a função de pré-visualização multicast	**no igmp-snooping preview**	Opcional
Configuração do canal de pré-visualização multicast	**igmp-snooping preview group-ip** IP **vlan** vid **interface ethernet** interface-num	Opcional
Desabilitar o canal de pré-visualização multicast	**no igmp-snooping preview group-ip** IP **vlan** vid **interface ethernet** interface-num	Opcional
Configuração da duração da pré-visualização, o intervalo de pré-visualização, a duração da reposição da pré-visualização e os tempos de pré-visualização permitidos	**igmp-snooping preview { time-once** time-once **time-interval** time-interval **time-reset** time-reset **permit-times** preview-times **}**	Opcional
Desabilitar a duração da pré-visualização única, o intervalo de pré-visualização, a duração da reposição da pré-visualização e os tempos de pré-visualização permitidos	**no igmp-snooping preview { time-once** time-once **time-interval** time-interval **time-reset** time-reset **permit-times** preview-times **}**	Opcional

Configuração do perfil de blacklist e whitelist

O IGMP-Snooping fornece o perfil de blacklist (lista negra) e whitelist (lista branca). Ele cria vários perfis no modo de configuração global e em seguida configura a lista referenciada por cada porta no modo de configuração da interface.

Você pode configurar o tipo e o intervalo do perfil de IGMP-Snooping, onde o tipo é permitido / recusado e o intervalo pode ser configurado para usar o endereço IP multicast ou o endereço MAC. O perfil de IGMP-Snooping só é ativado quando é referenciado por uma porta e uma porta pode se referir apenas um tipo (permitir ou negar).

Quando uma porta faz referência ao perfil de permissão, ela só pode aprender o grupo de multicast definido pelo perfil. Quando uma porta faz referência a um perfil de negação, ela pode aprender todos os grupos de multicast, exceto a definição do perfil.

» Configuração do perfil de Blacklist e Whitelist:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Crie um perfil e acesse o modo de configuração de perfil	**igmp-snooping profile** profile-id	-
Desabilitar a configuração de perfil	**no igmp-snooping profile** profile-id	Opcional
Configuração do tipo de perfil	**profile limit { permit | deny }**	Opcional
Configuração do intervalo do perfil IP	**ip range** start-ip end-ip **[vlan** vlan-id **]**	Opcional
Configuração do intervalo do perfil MAC	**mac range** start-mac end-mac **[vlan** vlan-id **]**	Opcional
Acesse o modo de configuração de interface	**interface ethernet** interface-num	-
Configuração de perfil de referência da porta	**igmp-snooping profile refer** profile-list	Opcional
Desabilitar o perfil de referência da porta	**no igmp-snooping profile refer** profile-list	Opcional

Visualização e manutenção do IGMP-Snooping

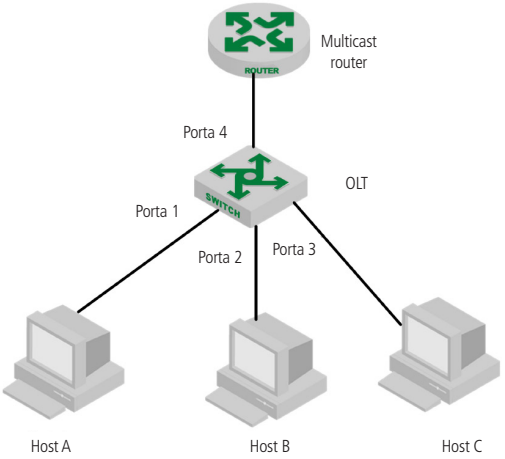
Depois de concluir a configuração acima, você pode usar os seguintes comandos para visualizar as configurações.

» Visualização das configurações de IGMP-Snooping:

Operação	Comando	Obrigatório/ opcional
Visualização das configurações de IGMP-Snooping	**show igmp-snooping**	Opcional, executável em todos os modos.
Visualização das estatísticas de pacotes de IGMP-Snooping	**show igmp-snooping statistics {interface |** vlan**}**	
Visualização do MAC do host do relatório	**show igmp-snooping record-host [interface]**	
Visualização das informações de pré-visualização multicast	**show igmp-snooping preview**	
Visualização do status do canal de pré-visualização multicast	**show igmp-snooping preview status**	
Visualização das configurações de perfil	**show igmp-snooping profile**	
Visualização resumida da tabela multicast	**show multicast**	
Visualização detalhada da tabela multicast	**show multicast igmp-snooping interface**	-

Exemplo de configuração

» Requisitos de rede:



Exemplo de configuração de IGMP-Snooping

Conforme exibido acima, Host-A, Host-B e Host-C pertencem a VLAN 2, VLAN 3 e VLAN 4, respectivamente. Os três hosts estão configurados para receber os dados do grupo multicast com os endereços de grupo 224.0.1.1 a 224.0.1.3, respectivamente.

» Etapas de configuração:

1. Habilite o IGMP-Snooping;
2. Adicionar portas diferentes a diferentes VLANs;
3. O host envia um pacote de relatório para o OLT e o OLT aprende o grupo multicast;
4. O roteador de origem multicast envia um pacote de consulta ao OLT e o OLT aprende as entradas da porta de roteamento;
5. O roteador de origem multicast envia o fluxo de dados do serviço multicast para o OLT e o OLT os distribui para o host correspondente.

» Validação de resultados:

» Habilitar IGMP:

OLT4840E(config)#igmp-snooping

» # Configure VLAN 2, VLAN 3 e VLAN 4 e, em seguida, adicione Ethernet0 / 1, Ethernet0 / 2 e Ethernet0 / 3 para VLAN 2, VLAN 3 e VLAN 4, respectivamente.

OLT4840E(config)#vlan 2

OLT4840E(config-if-vlan)#switchport ethernet 0/1

OLT4840E(config-if-vlan)#exit

OLT4840E(config)#vlan 3

OLT4840E(config-if-vlan)#switchport ethernet 0/2

OLT4840E(config-if-vlan)#exit

OLT4840E(config)#vlan 4

OLT4840E(config-if-vlan)#switchport ethernet 0/3

OLT4840E(config-if-vlan)#exit

Quando Host-A, Host-B e Host-C enviam relatórios IGMP para o OLT, ele irá aprender a entrada de grupo multicast correspondente. Quando o roteador de origem multicast envia pacotes de consulta IGMP para o OLT, ele aprenderá as entradas da porta de roteamento correspondentes.

» Exibir os grupos multicast aprendidos pelo OLT

OLT4840E(config)#show multicast

show multicast table information

MAC Address : 01:00:5e:00:01:01

VLAN ID : 2

Static port list : .

IGMP port list : e0/1

Dynamic port list :

MAC Address : 01:00:5e:00:01:02

VLAN ID : 3

Static port list : .

IGMP port list : e0/2

Dynamic port list :

MAC Address : 01:00:5e:00:01:03

VLAN ID : 4

Static port list :

IGMP port list : e0/3.

Dynamic port list :

Total entries: 3 .

OLT4840E(config)#show igmp-snooping router-dynamic

Port	VID	Age	Type
e0/4	2	284	{ STATIC }
e0/4	3	284	{ STATIC }s
e0/4	4	284	{ STATIC }

Total Record: 3

Quando o roteador de origem de multicast envia tráfego multicast de 224.0.1.1 ~ 224.0.1.3, o OLT distribuirá o fluxo de tráfego correspondente para Host-A, Host-B e Host-C.

6.2. Configuração de MLD-Snooping

Visão geral de MLD-Snooping

MLD (Multicast Listener Discovery) faz parte do protocolo IPv6, usando para suportar e gerenciar o multicast IP entre o host e o roteador multicast. O multicast IP permite que os datagramas sejam transmitidos para um conjunto de hosts que compõem um grupo multicast. As relações entre os membros do grupo multicast são dinâmicas, ou seja, os hosts podem entrar ou sair deles para minimizar a carga da rede, de modo a obter a efetiva transmissão de dados.

O snooping MLD é usado para monitorar os pacotes MLD entre o host e o roteador. Ele dinamicamente cria, mantém e exclui a tabela de endereços multicast com base na entrada e saída dos membros do grupo multicast. Nesse caso, os quadros multicast são encaminhados de acordo com a tabela de endereço multicast.

Habilitar o MLD-Snooping

» Habilitar o MLD-Snooping:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o MLD-Snooping	**mld-snooping**	Obrigatório

Configuração do timer do MLD-Snooping

» Configuração do timer do MLD-Snooping:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do tempo de envelhecimento dos membros dinâmicos	**mld-snooping host-aging-time** time	Opcional, por padrão, o tempo de envelhecimento das portas do membro multicast dinâmico é de *300 segundos*
Configure o tempo máximo de resposta dos pacotes de licença	**mld-snooping max-response-time** time	Opcional, por padrão, o tempo de resposta máximo é de *10 segundos*

Configuração de fast-leave

Normalmente, ao receber uma mensagem de MLD leave, MLD-Snooping não excluirá a porta diretamente do grupo de multicast. Em vez disso, aguarda um período de tempo para executar esta ação.

Após o fast-leave ser ativado, o MLD-Snooping remove a porta do grupo multicast diretamente quando recebido o pacote de licença MLD. Quando há apenas um usuário sob a porta, o fast-leave pode economizar a largura de banda.

» Configuração do fast-leave:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface ethernet** interface-num	-
Configuração do fast-leave	**mld-snooping fast-leave**	Opcional, por padrão o fast-leave está desabilitado

Configuração do número máximo de grupos multicast

Você pode usar os seguintes comandos para definir o número máximo de grupos multicast que podem ser aprendidos em cada porta.

» Configuração do número máximo de grupos multicast:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	configure terminal	-
Acesse o modo de configuração de interface	**interface ethernet** interface-num	-
Configuração do número máximo de grupos multicast	**mld-snooping group-limit** number	Opcional

Configuração da estratégia de aprendizado de multicast MLD-Snooping

Depois que uma estratégia de aprendizagem multicast for configurada, o administrador pode controlar o roteador para aprender apenas um grupo multicast específico. Se um grupo multicast for adicionado à blacklist, o roteador não o aprenderá; pelo contrário, o roteador no grupo multicast na whitelist pode ser aprendido.

» Configuração da estratégia de aprendizado de multicast MLD-Snooping:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-

Operação	Comando	Obrigatório/ opcional
Configure a regra de aprendizado padrão para grupos de multicast que não estão na blacklist ou whitelist	**mld-snooping { permit | deny } { group all | vlan** vid **}**	Opcional, por padrão, a regra de aprendizagem de um grupo multicast que não está na blacklist ou na whitelist é aprender todos os grupos multicast.
Acesse o modo de configuração de interface	**interface ethernet** interface-num	-
Configuração de blacklist e whitelist para a porta multicast	**mld-snooping { permit | deny } group-range** MAC **multi-count** num **vlan** vid	Opcional
	mld-snooping { permit | deny } group MAC **vlan** vid	Opcional, por padrão, nenhum grupo de multicast será adicionado à blacklist e whitelist

Configuração do MLD-Snoooping querier

Em uma rede multicast executando o protocolo MLD, um roteador multicast é responsável pelo envio de consultas MLD.

Mas você pode configurar o MLD-Snooping querier para que o OLT possa enviar ativamente uma mensagem de consulta de grupo geral para estabelecer e manter uma entrada de encaminhamento multicast.

Os usuários também podem configurar o MLD-Snooping querier para encaminhar em um endereço de origem especifico, o tempo de resposta máximo e o intervalo de consulta para o envio de mensagens de consulta geral.

» Configuração do MLD-Snoooping querier:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar MLD-Snooping querier	**mld-snooping querier**	Obrigatório
Configuração do intervalo de envio de pacotes de consulta geral	**mld-snooping query-interval** interval	Opcional
Configuração do tempo de resposta máximo para consulta gerais	**mld-snooping query-max-respond** time	Opcional

Configuração da porta de roteamento

A porta roteador pode ser identificada dinamicamente pelo MLD. Quando um OLT recebe um relatório de associação de um host, o OLT encaminha o relatório para a porta de roteamento.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da função de porta de roteamento híbrida	**mld-snooping route-port forward**	Opcional
Configure o tempo de envelhecimento da porta de roteamento dinâmico	**mld-snooping router-port-age { on | off |** age-time }	Opcional
Configuração da porta de rota estática	**mld-snooping route-port vlan** vid **interface { all | * thernet** interface-num }	Opcional

Configuração de VLAN multicast

Depois de habilitar a função de VLAN multicast em uma porta, o OLT altera os pacotes para uma VLAN multicast, independentemente da VLAN à qual pertençam as mensagens MLD.

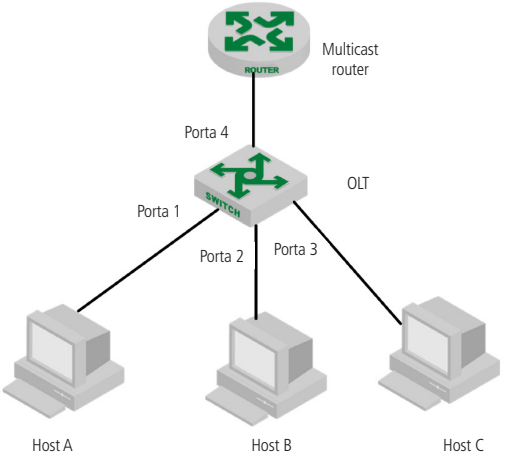
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de interface	**interface {ethernet | pon}** port-number	-
Configuração da VLAN multicast na porta	**mld-snooping multicast vlan** vid	Opcional

Visualização e manutenção de MLD-Snooping

Depois de completar as configurações acima, você pode usar o seguinte comando para visualizar as configurações.

Operação	Comando	Obrigatório/ opcional
Visualização das configurações do MLD-Snooping	**show mld-snooping**	Opcional, executável em todos os modos.
Visualização da porta de rota dinâmica	**show mld-snooping router-dynamic**	
Visualização da configuração de rota estática	**show mld-snooping router-static**	
Visualização do grupo multicast	**show multicast mld-snooping**	

Exemplo de configuração MLD-Snooping



» Requisitos de rede:

Conforme exibido na figura anterior, os hosts Host-A, Host-B e Host-C pertencem à VLAN 2, VLAN 3 e VLAN 4, respectivamente. Os hosts estão configurados para receber os dados do grupo multicast com o endereço FF02::01::0101, FF02::01::0102 e FF02::01::0103, respectivamente.

» Etapas de configuração

» Configurar OLT

» Configure VLAN 2, VLAN 3 e VLAN 4 e em seguida adicione Ethernet 0/1, Ethernet 0/2 e Ethernet 0/3 a VLAN 2, VLAN 3 e VLAN 4, respectivamente.

```
OLT4840E(config)#vlan 2
OLT4840E(config-if-vlan)#switchport ethernet 0/1
OLT4840E(config-if-vlan)#exit
OLT4840E(config)#vlan 3
OLT4840E(config-if-vlan)#switchport ethernet 0/2
OLT4840E(config-if-vlan)#exit
OLT4840E(config)#vlan 4
```

OLT4840E(config-if-vlan)#switchport ethernet 0/3

OLT4840E(config-if-vlan)#exit

» Habilitar MLD-Snooping

OLT4840E(config)#mld-snooping

Quando Host-A, Host-B e Host-C enviam pacotes de relatório MLD para o OLT4840E, ele aprenderá as entradas de grupo multicast correspondentes. Quando o roteador multicast IPV6 envia pacotes de consulta MLD, o OLT irá aprender as entradas da porta de roteamento correspondente.

Exibir os grupos multicast aprendidos pelo OLT

OLT4840E(config)#show mld-snooping group

show multicast table information

MAC Address : 33:33:00:01:00:01

VLAN ID : 2

port list : e0/1.

MAC Address : 33:33:00:01:00:02

VLAN ID : 3

port list : e0/2.

MAC Address : 33:33:00:01:00:03

VLAN ID : 4

port list : e0/2.

Total entries: 3 .

OLT4840E(config)#show mld-snooping router-dynamic

Port	VID	Age	Type
e0/4	2	284	{ QUERY }
e0/4	3	284	{ QUERY }
e0/4	4	284	{ QUERY }

Total Record: 3

Quando o roteador multicast envia o fluxo de dados multicast FF02::01::0101, FF02::01::0102 e FF02::01::0103, o OLT distribuirá o fluxo de dados correspondente para Host-A, Host-B E Host-C.

6.3. GMRP

Visão geral de GMRP

GMRP (*GARP Multicast Registration Protocol*) baseia-se no mecanismo de trabalho do GARP (*Generic Attribute Registration Protocol*) e mantém as informações de registro multicast dinâmico no roteador. Todos os roteadores que suportam o recurso GMRP podem receber dados de registro multicast de outros roteadores e atualizar dinamicamente as informações locais de cadastro multicast. Ao mesmo tempo, o roteador também pode enviá-las para outros roteadores para que todos os dispositivos estejam consistentes.

Quando um host quer se juntar a um grupo de multicast IP, ele precisa enviar uma mensagem de IGMP *join*, que é derivada do GMRP. Ao receber esta mensagem, o OLT adiciona a porta ao grupo multicast apropriado e envia as informações para todos os outros hosts na VLAN, com um host atuando como a fonte de multicast.

Quando esta fonte de multicast envia informações de multicast, o OLT envia tais informações somente através da porta que foi adicionada anteriormente ao grupo de multicast. Além disso, o OLT envia periodicamente uma consulta GMRP, se o host quiser permanecer no grupo multicast, ele deve responder à consulta GMRP.

Se um host não quer ficar em um grupo multicast, ele pode enviar uma mensagem de saída (leave) ou não responder a uma consulta GMRP periódica. Uma vez que o OLT recebe uma mensagem de saída ou não recebe uma resposta durante a configuração de todas as temporizações, ele exclui o host do grupo multicast.

Habilitar/desabilitar GMRP

O GMRP pode ser ativado no modo de configuração global ou no modo de configuração da porta. Por padrão, o GMRP está desabilitado.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Habilite o GMRP no modo *Global*	**gmrp**	Obrigatório

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de portas	**interface ethernet** interface-num	Obrigatório
Habilite o GMRP no modo de interface	**gmrp**	Obrigatório, para habilitar este modo, a porta deve estar em modo *Trunk*
Desabilite o GMRP	**no gmrp**	O GMRP pode ser desabilitado em modo *Global* ou modo de interface

Configuração de multicast release por GMRP

Depois que o GMRP é ativado, o sistema propaga automaticamente os grupos de multicast aprendidos através do GMRP, mas para propagar grupos de configuração por ele, você precisa executar as seguintes configurações:

» Configuração de Multicast Release por GMRP

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de Multicast Release por GMRP	**[no] garp permit multicast mac-address** mac **vlan** vid	Obrigatório, o multicast estático correspondente deve ser criado em primeiro lugar; usando o comando "no" para excluir a configuração

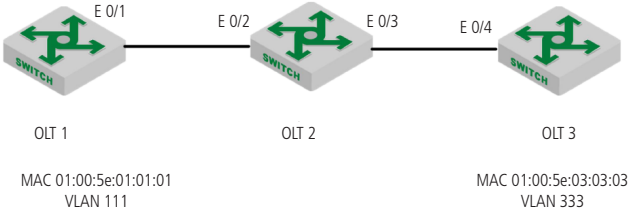
Obs.: *no GMRP, se não for a VLAN padrão, a VLAN correspondente deve ser combinada com o gvrp para produzir efeitos. Todos os recursos geralmente são usados em conjunto com o gvrp. Para a configuração do gvrp, consulte a seção 4.4. Configuração de GVRP.*

Visualização e manutenção do GMRP

Depois de completar a configuração acima, você pode usar o seguinte comando para visualizar a configuração.

Operação	Comando	Obrigatório/ opcional
Visualização do status global do GVRP	**show gmrp**	Opcional, executável em todos os modos.
Visualização do status do GMRP	**show gmrp interface [ethernet** interface-num**]**	
Visualização do GMRP	**show garp permit multicast**	
Visualização dos grupos de multicast locais (incluindo grupos multicast estáticos e grupos multicast aprendidos via GMRP)	**show multicast**	

Exemplo de configuração GMRP



Exemplo de configuração de serviço GMRP

» Requisitos de rede:

Na rede exibida acima, OLT 1 e OLT 3 anunciam suas informações de multicast estático para o OLT 2 via pacotes GMRP e o OLT 2 anuncia as informações multicast aprendidas através do GMRP. Eventualmente, as informações de multicast da OLT 1, OLT 2 e OLT 3 são sincronizadas.

» Roteiro de configuração:

1. Ative o GMRP no OLT 1 e anuncie as informações do multicast;
2. Ative o GMRP no OLT 2 e anuncie as informações do multicast;
3. Ative o GMRP no OLT 3 e anuncie as informações do multicast.

» Passos de configuração:

» Configuração do OLT1

OLT4840E(config)#vlan 111,333

OLT4840E(config-if-vlan)#switchport ethernet 0/1 to ethernet 0/10

Add VLAN port successfully.

OLT4840E(config)#multicast mac-address 01:00:5e:01:01:01 vlan 111

adding multicast group successfully !

OLT4840E(config)#multicast mac-address 01:00:5e:01:01:01 vlan 111 interface ethernet 0/1

to ethernet 0/10

adding multicast group port successfully !

OLT4840E(config-if-vlan)#interface e 0/1

OLT4840E(config-if-ethernet-0/1)#switchport mode trunk

OLT4840E(config-if-ethernet-0/1)#exit

OLT4840E(config)#gvrp

Turn on GVRP successfully.

OLT4840E(config)#gmrp // Configuração de GMRP

Turn on GMRP successfully.

OLT4840E(config)#garp permit vlan 111,333

OLT4840E(config)#garp permit multicast mac-address 01:00:5e:01:01:01 vlan 111

OLT4840E(config)#interface e 0/1

OLT4840E(config-if-ethernet-0/1)#gvrp

OLT4840E(config-if-ethernet-0/1)#gmrp

OLT4840E(config-if-ethernet-0/1)#exit

OLT4840E(config)#show gmrp // Verifique as configurações GMRP

GMRP status : enable

OLT4840E(config)#show gmrp interface ethernet 0/1

port GMRP status

e0/1 enable

Total entries: 1.

OLT4840E(config)#show garp permit multicast

GARP permit multicast:

vlan 111, mac 01:00:5e:01:01:01

» Configuração do OLT2

OLT4840E(config)#interface range ethernet 0/2 to ethernet 0/3

OLT4840E(config-if-range)#switchport mode trunk

OLT4840E(config-if-range)#exit

OLT4840E(config)#gvrp

Turn on GVRP successfully

OLT4840E(config)#gmrp // Configuração do GMRP

Turn on GMRP successfully.

OLT4840E(config)#interface range ethernet 0/2 to ethernet 0/3

OLT4840E(config-if-range)#gvrp

OLT4840E(config-if-range)#gmrp

OLT4840E(config-if-range)#exit

OLT4840E(config)#show gmrp // Verifique as configurações GMRP

GMRP state : enable

OLT4840E(config)#show gmrp interface ethernet 0/2 ethernet 0/3

port GMRP status

e0/2 enable

e0/3 enable

Total entries: 2.

» Configurações OLT3

OLT4840E(config)#vlan 111,333

OLT4840E(config-if-vlan)#switchport ethernet 0/1 to ethernet 0/10

Add VLAN port successfully.

OLT4840E(config)#multicast mac-address 01:00:5e:03:03:03 vlan 333

adding multicast group successfully !

OLT4840E(config)#multicast mac-address 01:00:5e:03:03:03 vlan 333 interface ethernet 0/1 to ethernet 0/10

adding multicast group port successfully !

OLT4840E(config-if-vlan)#interface e 0/4

OLT4840E(config-if-ethernet-0/4)#switchport mode trunk

OLT4840E(config-if-ethernet-0/4)#exit

OLT4840E(config)#gvrp

Turn on GVRP successfully.

OLT4840E(config)#gmrp // Configuração do GMRP

Turn on GMRP successfully.

OLT4840E(config)#garp permit vlan 111,333

OLT4840E(config)#garp permit multicast mac-address 01:00:5e:03:03:03 vlan 333

OLT4840E(config)#interface e 0/4

OLT4840E(config-if-ethernet-0/4)#gvrp

OLT4840E(config-if-ethernet-0/4)#gmrp

OLT4840E(config-if-ethernet-0/4)#exit

OLT4840E(config)#show gmrp // // Verifique as configurações de GMRP

GMRP status : enable

OLT4840E(config)#show gmrp interface ethernet 0/4

port GMRP status

e0/4 enable

Total entries: 1.

OLT4840E(config)#show garp permit multicast

GARP permit multicast:

vlan 333, mac 01:00:5e:03:03:03

Após a conclusão da configuração, você pode usar o comando show multicast para visualizar as informações de registro multicast aprendidas pela função *GMRP*.

OLT4840E(config)#show multicast

show multicast table information

MAC Address : 01:00:5e:01:01:01

VLAN ID : 111

Static port list : e0/1-e0/10.

IGMP port list :

Dynamic port list :

MAC Address : 01:00:5e:03:03:03

VLAN ID : 333

Static port list :

IGMP port list :

Dynamic port list : e0/1.

Total entries: 2 .

As informações de multicast no OLT2 mostram que os MACs 01:00:5e:01:01:01 e 01:00:5e:03:03:03 são aprendidas através do GMRP.

OLT4840E(config)#show multicast

show multicast table information

MAC Address : 01:00:5e:01:01:01

VLAN ID : 111

Static port list :

IGMP port list :

Dynamic port list : e0/2.

MAC Address : 01:00:5e:03:03:03

VLAN ID : 333

Static port list :

IGMP port list :

Dynamic port list : e0/3.

Total entries: 2 .

As informações de multicast no OLT3 exibem que 01:00:5e:01:01:01 são pacotes multicast aprendidos via GMRP.

OLT4840E (config)#show multicast

show multicast table information

MAC Address : 01:00:5e:01:01:01

VLAN ID : 111

Static port list :

IGMP port list :

Dynamic port list : e0/4.

MAC Address : 01:00:5e:03:03:03

VLAN ID : 333

Static port list : e0/1-e0/10.

IGMP port list :

Dynamic port list :

Total entries: 2 .

6.4. Configuração da tabela multicast estática

Visão geral da tabela multicast estática

Além do aprendizado dinâmico, as tabelas multicast podem ser configuradas manualmente e neste caso são chamadas de tabela multicast estática. A tabela MAC multicast estática não será envelhecida e não pode ser perdida depois de ser salva.

Apenas a tabela multicast IPv4 pode ser configurada como estática e não é possível fazer na tabela IPV6.

Criação de uma tabela multicast estática

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Criação de uma tabela multicast estática	**multicast {mac-address** mac **| ip-address** ip **} vlan** vlan-id	Obrigatório

O parâmetro MAC refere-se ao endereço MAC do grupo multicast. É necessário usar o formato de endereço multicast, por exemplo: 01:00:5e:**:**:**, IP refere-se a IP multicast, por exemplo, 224.0.1.1, VLAN-ID refere-se a ID de VLAN, com O intervalo de 1 a 4094 (deve ser uma VLAN existente). Quando o grupo de multicast estático não existe, o grupo de multicast não pode ser adicionado.

Por exemplo:

» ! Crie um grupo multicast com o endereço MAC de 01:00:5e:01:02:03 e a VLAN ID 1
OLT4840E(config)#multicast mac-address 01:00:5e:01:02:03 vlan 1

! Crie um grupo multicast com o endereço IP de 224.0.1.1 e VLAN ID 1

OLT4840E(config)#multicast ip-address 224.0.1.1 vlan 1

Adicionar uma porta a um grupo multicast

Adicionar uma porta a um grupo multicast

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Adicionar uma porta a um grupo multicast estático	**multicast {mac-address** mac **| ip-address** ip **} vlan** vlan-id **interface { all | interface-list }**	Obrigatório

Por exemplo:

» ! Adicionar as portas Ethernet 2, 3, e 8 no multicast criado
OLT4840E(config)#multicast mac-address 01:00:5e:01:02:03 vlan 1 interface ethernet 0/2 to

ethernet 0/4 ethernet 0/8

Configuração da porta de proxy

Quando um OLT é configurado com uma tabela de multicast estático, se o OLT estiver configurado com uma porta de proxy, ele pode enviar o relatório para a fonte de multicast anunciando a informação do membro.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Criar uma porta proxy para um grupo multicast estático	**multicast {mac-address** mac **| ip-address** ip **} vlan** vlan-id **proxy-port ethernet interface-list**	Obrigatório
Configurar intervalo de envio de pacotes de relatório para a origem multicast pela porta de proxy	**multicas proxy-interval** second	Opcional

7. Configuração de endereço de IP

7.1. Endereço de IP da interface do OLT

Introdução ao IP da interface do OLT

O IP do OLT pode ser usado como endereço de gerenciamento ou gateway. O IP deve ser configurado nas interfaces *interface VLAN* e *interface super-VLAN*. A SuperVLAN inclui muitas sub-VLANs.

Configuração da interface VLAN

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	configure terminal	-
Criar a VLAN	vlan id	Opcional
Adicionar a porta na VLAN	**switchport ethernet** port	Opcional
Criar interface VLAN	interface **vlan-interface** vid	Opcional
Configuração de endereço de IP da interface	**ip address** {ipaddress|primary} mask override	Opcional
Remover endereço de IP da interface	**no ip address** ipaddress *mask*	Opcional
Configuração do intervalo de controle de acesso de IP	**ip addres range** start ipaddress end ipaddress	Opcional
Remover intervalo de controle de acesso de IP	**no ip addres range** start ipaddress end ipaddress	Opcional

Obs.: *uma interface pode configurar 32 IPs em diferentes redes.*

» **Controle de intervalo de acesso IP:** todas as interfaces VLAN ou superVLAN podem ser configuradas com até oito intervalos de acesso. Depois que o intervalo de acesso é configurado, o usuário ARP deve estar dentro desses intervalos para aprender e, assim, limitar o acesso do usuário.

Configuração da interface SuperVLAN

Configuração de interface SuperVLAN

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Criar interface SuperVLAN	interface **supervlan-interface** vid	Opcional
Adicionar uma sub-VLAN na SuperVLAN	**subvlan** {vid| VLAN list }	Opcional
Configuração da IP da interface SuperVLAN	**ip address {**ipaddress| **primary}** mask	Opcional
Remover endereço de IP da interface	**no ip address** ipaddress mask	Opcional
Configuração do intervalo de controle de acesso de IP	**ip addres range** start ipaddress end ipaddress	Opcional
Remover intervalo de controle de acesso de IP	**no ip addres range** start ipaddress end ipaddress	Opcional

Configuração override IP

Ao configurar o IP, adicione o comando de override na parte de trás, usado para revisar o IP no mesmo segmento de rede.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	configure terminal	-
Acesse o modo de configuração de interface	interface vlan-interface vid /supervlan-interface id	Opcional
Configuração	ip address ipaddress mask override	Opcional

Configuração de interface de loopback

A interface VLAN e a interface SuperVLAN conectam as portas diretamente enquanto a interface de loopback conecta as portas através delas. No caso, a interface de loopback não será influenciada pelo status da porta e sempre ficará no estado de linkup.

» Configuração de interface de loopback:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Criar a interface de loopback	**interface loopback-interface <0-1>**	Opcional
Configuração IP da interface	**ip address** ipaddress mask	Opcional

Configuração dos parâmetros de interface

» Configuração do IP do sistema na interface VLAN:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Habilitar o pacote de resposta da máscara de endereço ICMP	**ip icmp** mask-reply	Opcional
Acesse a interface de configuração de VLAN	**interface vlan-interface** vid	-
Habilitar o envio de pacotes inacessíveis de destino icmp	**ip icmp unreachable**	Opcional
Configuração de descrição de interface IP	**description** interface-name	Opcional
Remover descrição de interface IP	**no description**	Opcional

Desligar uma interface

Você não pode gerenciar um dispositivo após sua interface ser desligada.

» Desligar interface:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse a interface de configuração de VLAN	**interface vlan-interface** vid	Obrigatório
Desligar a interface	**shutdown**	Opcional
Acesse a interface de configuração de SuperVLAN	**interface supervlan-interface** vid	Obrigatório
Desligar a interface	**shutdown**	Opcional
Reativar interface	**no shutdown**	Opcional

Visualização e manutenção de interface IP

Depois de concluir a configuração acima, você pode usar o seguinte comando para visualizar a configuração.

» Visualização de interface IP:

Operação	Comando	Obrigatório/ opcional
Visualizar configuração IP das Interfaces de VLAN	**show ip interface {loopback-interface | supervlan-interface | vlan-interface }**	Opcional, pode ser executado em qualquer modo

8. Configuração de endereço IPv6

8.1. Informações básicas de IPv6

IPv6 (Internet Protocol Version 6) é o protocolo de camada de rede padrão de segunda geração, também conhecido como IPng (IP Next Generation), que foi projetado pela IETF (Internet Engineering Task Force), superior ao IPv4. A maior diferença entre IPv6 e IPv4 é que o comprimento do endereço IP aumenta de 32 bits para 128 bits.

8.2. Padrão do endereço IPv6

O endereço IPv6 é um número hexadecimal de série de 16 bits isolado por (:). Cada endereço IPv6 é dividido em 8 grupos, representado por 4 números hexadecimais (16bits). Dois pontos (:) separam diferentes grupos, por exemplo:

2001:0000:130F:0000:0000:09C0:876A:130B

Para simplificar o padrão, o *0* pode ser tratado conforme a seguir:

- » A frente *0* pode ser omitida em cada grupo. O endereço acima pode ser exibido como 2001:0:130F:0:0:9C0:876A:130B.
- » Se houver *0* consecutivamente em dois ou mais grupos, *::* dois pontos duplos podem substituí-lo. Por exemplo: 2001:0:130F::9C0:876A:130B.

Existem duas partes no endereço IPv6: prefixo do endereço e identificação da interface. O prefixo de endereço é semelhante ao número de rede no IPv4, enquanto a identificação da interface é semelhante ao número do mainframe.

Prefixo de endereço: endereço IPv6 / comprimento do prefixo. O endereço IPv6 pode estar em qualquer forma das listadas acima, mas o comprimento do prefixo é um número decimal, mostrando em que local da esquerda seria o prefixo.

8.3. Protocolo de descoberta de vizinhos IPv6

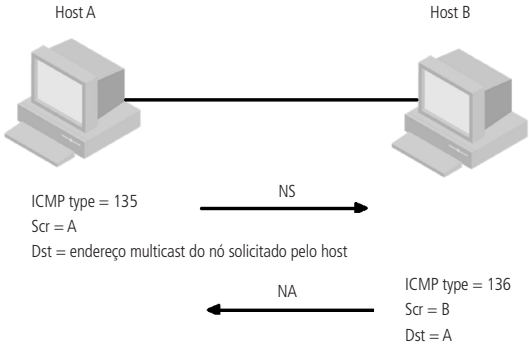
IPv6 Neighbor Discovery Protocol (Protocolo de descoberta de vizinhos IPv6) adota 5 tipos de mensagem ICMPv6 para realizar as atividades: resolução de endereço, verificação de acessibilidade de vizinhança, detecção de endereço duplicado, descoberta de roteador / descoberta de prefixo, autoconfiguração de endereço, redirecionamento.

Os tipos e funções de mensagem ICMPv6 no protocolo de descoberta vizinha são exibidos a seguir:

ICMPv6	Descrição
Router Solicitation	A mensagem Router Solicitation é enviada por um dispositivo para requisitar aos roteadores o envio de mensagens Router Advertisement. Sua importância provém da necessidade da descoberta imediata, por um nó, de informações (como rotas, MTU, Hot Limit e outras) que estão dispostas no roteador.
Router Avertisement	A mensagem Router Avertisement é enviada periodicamente ou em resposta à mensagem Router Solicitation por um roteador para anunciar sua presença no enlace. Sua importância provém do caráter informativo dessa mensagem. Além de anunciar o roteador como alternativa para rota de tráfego no enlace, ela também transmiti dados com prefixos, MTU, DNS e outros.
Neighbor Solicitation	A mensagem Neighbor Solicitation é enviada por um dispositivo para requisitar a um determinado vizinho o envio de mensagens Neighbor Advertisement. Por causa dessa funcionalidade, ela é utilizada para suprir três necessidades básicas de comunicação em redes IPv6. A primeira consiste na descoberta de um endereço físico associado a um endereço lógico. Nesse caso a resposta ao Neighbor Solicitation conterá o endereço requisitado. No IPv4, o Adress Resolution Protocol realiza a mesma função. A segunda consiste no teste de acessibilidade de nós vizinhos no enlace. Nesse caso, a mensagem pode ser enviada para se verificar se determinado endereço lógico existe ou se ainda está respondendo. A terceira é sobre a detecção de endereços IPv6 duplicados na vizinhança.
Neighbor Adverstisement	A mensagem Neighbor Advertisement é enviada em resposta a uma mensagem Neighbor Solicitation ou espontaneamente para anunciar a mudança de alguma característica do dispositivo na rede de maneira rápida. Igual a mensagem Neighbor Solicitation, essa mensagem também é utilizada para auxiliar nas funcionalidades de resolução de endereços físicos, no teste de acessibilidade de um nó vizinho e na detecção de endereços duplicados.
Redirect	A mensagem Redirect é enviada por roteadores para informar ao nó solicitante de uma comunicação, uma melhor opção de caminho para ser utilizada. Em outras palavras, ele envia o endereço do próximo salto que deve ser usado para encaminhar pacotes quando se comunicar com aquele determinado desttino.

- Funções no protocolo de descoberta vizinha (Neighbor Solicitation):
  - Resolução do endereço:

    Obter o endereço MAC do nó vizinho, no mesmo link (mesma função do ARP no IPv4) através de NS e NA. Conforme exibido a seguir, o host A recebe o endereço MAC do host B.



1. O host A envia NS por meio de multicast. O endereço de origem de NS é o endereço IPv6 da interface do host A. O endereço de destino é o endereço multicast do nó solicitado pelo host B e a mensagem também inclui o endereço MAC do host A;
2. Quando o host B recebe NS, se o endereço de destino corresponde ao endereço de multicast do nó. Se sim, o host B pode aprender o endereço do host A e responder a mensagem NA por modo *Unicast*, com o seu endereço IPv6 e MAC;
3. O host A recebe NA e obtém o endereço MAC do host B. Portanto, o host A pode se comunicar com o host B.

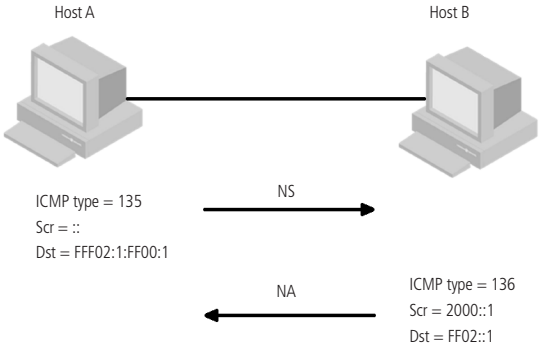
» Verificação a acessibilidade do vizinho:

Depois de obter o endereço do nó vizinho, as mensagens Neighbor Solicitation (NS) e Neighbor Advertisement (NA) podem ser usadas para verificar se o nó vizinho está acessível.

1. O nó envia NS, onde o endereço de destino é o endereço IPv6 do nó vizinho;
2. Se a mensagem de confirmação for recebida, considera-se o vizinho como acessível. Caso contrário, considera que o vizinho está inacessível.

» Detecção de endereço duplicado:

» Quando o nó recebe um endereço IPv6, a detecção de endereço duplicado é reativa para garantir que este endereço seja ocupado por outros nós por meio de NS e NA (o mesmo que o ARP livre IPv4). Exibido como a seguir.



1. O host A envia o endereço de origem da mensagem NS, NS é um endereço desconhecido ::, o endereço de destino é o endereço IPv6 solicitado e a mensagem inclui o endereço IPv6 a ser detectado;
2. Se o host B já ocupa esse endereço, a mensagem NA será retornada e a mensagem também incluirá o endereço IPv6 próprio;
3. Se o host A recebe NA do host B, isto é, o endereço IPv6 é tomado. Caso contrário, o endereço está disponível para o anfitrião A.

8.4. Configuração de IPv6

Configuração de endereço IPv6 unicast

Ao acessar a rede IPv6, o endereço IPv6 deve ser configurado, e temos que escolher um dos endereços unicast global, endereço local, endereço local do link.

Ao acessar a rede, o endereço unicast IPv6 deve ser configurado.

- O endereço local do site IPv6 e o endereço unicast global podem ser configurados pelas seguintes 4 maneiras:
  - **EUI-64:** quando adota EUI-64 formando IPv6, o prefixo do endereço IPv6 da interface é o prefixo configurado. O identificador da interface é traduzido a partir do endereço da camada de ligação da interface.
  - **Modo *Manual*:** configure o endereço local do local IPv6 ou o endereço unicast global por modo *Manual*.
  - **DHCP:** suporta obter o endereço local do site IPv6 ou o endereço unicast global ou algumas informações relacionadas através do servidor DHCP.

- **Configuração automática:** IPv6 e informações relacionadas são configuradas automaticamente com base em seu próprio endereço de camada de link e as informações de prefixo anunciadas pelo roteador.

» Obtenha o endereço local do link IPv6 por duas maneiras:

- **Geração automática:** gera automaticamente o endereço local do link para a interface com base no prefixo do endereço local do link (FE80 :: / 64) e no endereço da camada da ligação da interface.
- **Atribuição manual:** configure manualmente o endereço local do link IPv6.

» Configuração de endereço IPv6:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Acesse o modo de interface VLAN/ interface SuperVLAN	**interface { vlan-interface** vid **| supervlan-interface** interface-number **}**	Obrigatório
Configurar o endereço do site local e o endereço unicast global no formato EUI-64	**ipv6 address** ipv6-address/prefix-length **eui-64**	Opcional
Excluir o endereço local do site e o endereço unicast global configurado no formato EUI-64	**no ipv6 address** ipv6-address/prefix-length **eui-64**	Opcional
Especificar manualmente o endereço local do site e o endereço unicast global	**ipv6 address** ipv6-address/prefix-length	Opcional
Excluir endereços local-local especificados manualmente e endereços unicast globais	**no ipv6 address** ipv6-address/prefix-length	Opcional
Configurar automaticamente o endereço local do site e o endereço unicast global	**ipv6 address autoconfig**	Opcional
Excluir o endereço local-global configurado automaticamente e o endereço unicast global	**no ipv6 address autoconfig**	Opcional

Operação	Comando	Obrigatório/ opcional
Especificar o endereço local do link manualmente	**ipv6 address** ipv6-address **link-local**	Opcional, por padrão, um endereço local de link é automaticamente formado
Excluir o link-endereço local especificado manualmente	**no ipv6 address** ipv6-address **link-local**	Opcional
Obter endereço ipv6 pelo DHCP	**ipv6 address dhcpc6**	Opcional
Desativar a função de obter o endereço ipv6 pelo DHCP	**no ipv6 address dhcpc6**	Opcional
Visualização da configuração do endereço ipv6	**show ipv6**	Opcional
Visualização a situação de obter o endereço IPv6 pelo DHCP	**show ipv6 address dhcpc6**	Opcional

Configuração da lista de vizinhança estática

Envie NS & NA ou configure a lista de vizinhança estática por linha de comando para resolver o endereço IPv6 do nó vizinho.

A lista estática de vizinhos inclui lista de vizinhança estática longa ou lista de vizinhança estática curta.

Para uma lista estática de vizinhança longa, deve-se configurar o endereço IPv6, MAC, VLAN e a lista de porta de vizinhos. Ela pode ser usada diretamente para encaminhamento de pacotes.

Ao configurar a lista de vizinhança estática curta, basta configurar o endereço IPv6 e o endereço MAC. Esta não pode ser usada para o encaminhamento de pacotes, o pedido de vizinho é enviado em primeiro lugar. Se o endereço IPv6 configurado e o endereço MAC forem iguais aos do pacote de resposta, completa-se a lista e ela pode ser usada no encaminhamento do pacote IPv6.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de interface VLAN/ interface SuperVLAN	**interface { vlan-interface** vid **| supervlan-interface** interface-number **}**	-
Configuração de lista de vizinhança estática longa	**ipv6 neighbor** ipv6-address mac-address vlan-id device/slot/port	Obrigatório
Configuração de lista de vizinhança estática curta	**ipv6 neighbor** ipv6-address mac-address	Obrigatório
Excluir a lista de vizinhança	**no ipv6 neighbor {dynamic | static | all | }**	Opcional
Excluir a lista de vizinhança na interface VLAN	**no ipv6 neighbor** ipv6-address **interface { vlan-interface** vid **| supervlan-interface interface**-number }	Opcional
Visualização da lista de vizinhança	**show ipv6 neighbors {** ipv6-addres **|all | dynamic| static|mac** mac-address}	Opcional

Configuração de número máximo de vizinhos

Se o número de vizinhos for muito grande, isso pode afetar desempenho da transmissão. Podemos limitar o número máximo de vizinhos por configuração.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do número de envio de NS para detecção de endereço duplicado	**ipv6 nd dad attempts** value	Opcional, por padrão, o número de envio de NS na detecção de endereço duplicado é *1*. Quando o valor é *0*, significa que a detecção de endereço duplicado está desativada.

Operação	Comando	Obrigatório/ opcional
Recupere o valor padrão de retrans-time	**no ipv6 nd ns retrans-time**	Opcional
Visualização do número de envio de NS para detecção de endereço duplicado	**show ipv6 nd dad attemps**	Opcional
Visualização do intervalo para enviar mensagem NS	**show ipv6 nd ns retrans-time**	Opcional

Configuração do tempo para manter o vizinho acessível

Quando a acessibilidade do vizinho é determinada por detecção, o dispositivo considera o vizinho acessível dentro do tempo de alcance da configuração. Depois que ele é executado durante o tempo de ajuste, se um pacote precisa ser enviado para o vizinho, ele é reconhecido.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do tempo para manter o vizinho acessível	**ipv6 nd reachable-time** value	Opcional, unidades em segundos. O tempo acessível é *30 segundos* por padrão.
Recupere o valor padrão de reachable-time	**no ipv6 nd reachable-time**	Opcional

Configuração de rota estática IPv6

Operação	Comando	Obrigatório/ Opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de rota estática IPv6	**ipv6 route** [ipv6-address mask| ipv6-address/ prefix-length] nexthop-address	Obrigatório, por padrão, nenhuma rota estática ipv6 está configurada.

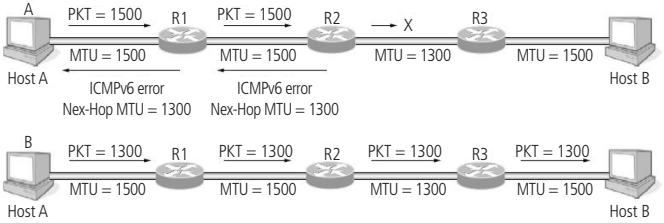
Operação	Comando	Obrigatório/ Opcional
Remover a rota estática IPv6	**no ipv6 route** [ipv6-address mask| ipv6-address/prefix-length] nexthop-addres	Opcional
Visualização da lista de rota	**show ipv6 route**	Opcional

Configurar interface MAX de transmissão (MTU)

A unidade de transmissão MAX do caminho da interface IPv6 pode ser ajustada na faixa de 1280-1510 bytes. O pacote IPv6 deve ser menor que 1280 bytes, devendo ser fragmentado e encapsulado. Pacotes maiores que a configuração do MTU serão descartados.

» Passos para obter Interface MTU

1. O nó de envio assume que o caminho MTU é o link de saída de encaminhamento;
2. O nó de envio envia pacotes de acordo com a MTU do caminho assumido;
3. Se o roteador não puder encaminhar este pacote devido ao MTU transmissor ser menor que o MTU assumido, o roteador descarta o pacote e retorna o pacote sobrecarregado ICMPv6 ao nó de envio. O pacote sobrecarregado carrega o MTU de falha de transmissão;
4. O nó de envio define o caminho MTU para o valor MTU no pacote sobrecarregado ICMPv6.



Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de interface VLAN / interface SuperVLAN	**interface { vlan-interface** vid **| supervlan-interface** interface-number **}**	-

Operação	Comando	Obrigatório/ opcional
Configuração da interface MTU	**ipv6 pathmtu** value	Opcional, por padrão o valor é *1500*
Restaurar configurações padrão	**no ipv6 pathmtu**	Opcional

Dispositivo que recebe pedido multicast de eco responde com pacote de resposta eco

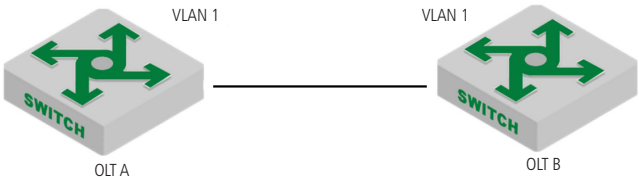
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Ativar a resposta de pacote multicast	**ipv6 icmpv6 multicast-echo-reply enable**	Obrigatório, por padrão está desativado
Desativar a resposta de pacote multicast	**no ipv6 icmpv6 multicast-echo-reply**	Opcional

8.5. Exemplo de configuração de endereço unicast IPv6

Requisitos de rede

Dois OLTs estão interligados através de portas Ethernet. Configure o endereço IPv6 para ambos os OLTs, para verificar sua interconexão. OLT A global unicast endereço é 2001::1/64, OLTB global unicast endereço é 2001::2/64.

Diagrama de rede



» Configuração do OLT A:
SwitchA(config)#interface vlan-interface 1

SwitchA(config-if-vlanInterface-1)#ipv6 address 2001::1/64

SwitchA(config-if-vlanInterface-1)#ipv6 address fe80:12::1 link-local

» (2) Configuração do OLT B:
SwitchB(config)# interface vlan-interface 1

SwitchB(config-if-vlanInterface-1)#ipv6 address 2001::2/64

SwitchB(config-if-vlanInterface-1)#ipv6 address fe80:12::2 link-local

Verificação de configuração

» Exiba as informações ipv6 do OLT A
OLT A(config)#show ipv6 interface vlan-interface 1

Show informations of ipv6 interface

VLAN-IF1:

sw0 Link type:Ethernet HWaddr 00:00:00:09:99:99 Queue:none

IPv6 forwarding is disabled

inet6 unicast 2001::1 prefixlen 64

inet6 unicast FE80::200:FF:FE09:9999%sw0 prefixlen 64 automatic

inet6 unicast 2001:: prefixlen 64 anycast

inet6 multicast FF02::1%sw0 prefixlen 16 automatic

inet6 multicast FF02::1:FF09:9999%sw0 prefixlen 16

inet6 multicast FF02::1:FF00:1%sw0 prefixlen 16

inet6 multicast FF02::1:FF00:0%sw0 prefixlen 16

UP RUNNING SIMPLEX BROADCAST MULTICAST PROMISC

MTU:1500 metric:1 VR:0 ifindex:2

RX packets:150 mcast:35 errors:0 dropped:0

TX packets:1216 mcast:33 errors:0

collisions:0 unsupported proto:0

RX bytes:13k TX bytes:55k

» Exiba as informações ipv6 do OLTB
OLT A(config)#show ipv6 interface vlan-interface 1

Show informations of ipv6 interface

VLAN-IF1:

sw0 Link type:Ethernet HWaddr 00:01:7a:e9:68:58 Queue:none
IPv6 forwarding is disabled
inet6 unicast FE80:12::2%sw0 prefixlen 64
inet6 unicast 2001::2 prefixlen 64
inet6 unicast FE80::201:7AFF:FEE9:6858%sw0 prefixlen 64 automatic
inet6 multicast FF02::1%sw0 prefixlen 16 automatic
inet6 multicast FF02::1:FFE9:6858%sw0 prefixlen 16
inet6 multicast FF02::1:FF00:2%sw0 prefixlen 16
UP RUNNING SIMPLEX BROADCAST MULTICAST PROMISC
MTU:1500 metric:1 VR:0 ifindex:2
RX packets:21912 mcast:7990 errors:0 dropped:73
TX packets:8300 mcast:8023 errors:0
collisions:0 unsupported proto:0
RX bytes:1858k TX bytes:714k

Total entries: 1 interface.

» Faça o ping do OLT A para o OLTB no endereço local e no endereço unicast global. Se a configuração for correta, os dois tipos de endereços IPv6 podem ser pingados com sucesso.

OLT A(config)#ping6 FE80:12::2%sw0

Pinging FE80:12::2%sw0 (FE80:12::2%sw0) with 56 bytes of data:

Reply from FE80:12::2%sw0 bytes=56 time=10ms hlim=64
Reply from FE80:12::2%sw0 bytes=56 time=10ms hlim=64
Reply from FE80:12::2%sw0 bytes=56 time=10ms hlim=64
Reply from FE80:12::2%sw0 bytes=56 time=10ms hlim=64

--- FE80:12::2%sw0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4840 ms
rtt min/avg/max = 10/10/10 ms

OLTA(config)#ping6 2001::2

Pinging 2001::2 (2001::2) with 56 bytes of data:
Reply from 2001::2 bytes=56 time=10ms hlim=64
Reply from 2001::2 bytes=56 time=10ms hlim=64
Reply from 2001::2 bytes=56 time=10ms hlim=64
Reply from 2001::2 bytes=56 time=10ms hlim=64

--- 2001::2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4840 ms
rtt min/avg/max = 10/10/10 ms

» Visualizar a tabela de vizinhança do OLT A
OLT A(config)#show ipv6 neighbors all
Information of neighbor cache

Neighbor	Status	Mac_ Address	VLAN	Port	Type	Expire
2001::2	00:01:7a:e9:68:58	1	1	Dynamic	941 s	stale
FE80:12::2%sw0	00:01:7a:e9:68:58	1	1	Dynamic	941 s	stale

Total entries:2

9. Configuração de ONU

9.1. Descoberta e autenticação de ONU

Visão geral de descoberta e autenticação de ONU

O OLT gera periodicamente mensagens *Discover Time Windows* para a descoberta de ONUs recém conectadas ou que não estão ativas, mas que acessam o PON. É encaminhada uma mensagem de descoberta para todas ONUs notificando o período de descoberta. Uma vez recebida, a ONU aguarda o início do período e encaminha uma mensagem REGISTER_REQ em resposta, onde é informado seu identificador físico (MAC) e/ou lógico (LOID + password). O OLT recebe a mensagem REGISTER_REQ e verifica a validade da identificação da ONU de acordo com a lista de autenticação configurada. Se a autenticação for bem-sucedida, a mensagem REGISTER é encaminhada para a ONU e o estado dela atualizado para *autorizado*. O LLID é atribuído à ONU e o OLT encaminha uma mensagem GATE padrão unicast para a ONU autorizada. Após sua chegada, a ONU encaminha uma mensagem REGISTER_ACK para confirmar o LLID e o tempo de sincronização na mensagem GATE. Quando o OLT receber o REGISTER_ACK, o processo de autenticação de descoberta da ONU é concluído.

Se a autenticação da ONU falhar, o estado *não autorizado* será mantido, o OLT encaminhará a mensagem REGISTER (Flag = 0x02: Deregister) para ela cancelar o seu registro.

Nosso equipamento EPON suporta três métodos de autenticação da ONU:

- **Autenticação baseada na identificação física:** a autenticação baseada em MAC é dividida em dois modos: autenticação de whitelist (lista de MAC permitidos) e autenticação de blacklist (lista de MAC bloqueados). Quando a autenticação MAC é habilitada, o MAC da ONU correspondente deve ser configurado no OLT para determinar se a ela deve completar o seu registro ou não.
- **Autenticação baseada em identificação lógica:** a identificação lógica usa LOID + Senha. Quando você habilita a autenticação da ONU com base na ID lógica, você precisa configurá-la no OLT para determinar se a ONU deve completar o registro ou não.
- **Híbrido:** a autenticação da ONU baseada no endereço físico e na ID lógica são compatíveis. O OLT usa um dos dois modos de autenticação para ONUs diferentes. Desta forma, autentica-se primeiro baseado no endereço MAC. Se falhar, inicia-se a autenticação com base na ID lógica da ONU.

Por padrão nenhum modo de autenticação vem habilitado, ou seja, toda ONU pode se conectar ao sistema EPON e não precisa ser autenticada.

Configuração da descoberta e autenticação de ONU

» Configuração da descoberta e autenticação de ONU:

Configuração da atividade		Obrigatório/ opcional	Informação detalhada
-	Configuração do modo sem autenticação	Opcional	1.3
Configurações básicas de autenticação de ONU	Configuração do modo de autenticação por MAC	Opcional	1.4
	Configuração do modo de autenticação baseado em identificação lógica	Opcional	1.5
	Configuração do modo de autenticação híbrida	Opcional	1.6

Modo sem autenticação

Configuração do modo sem autenticação

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Visualização das configurações de autenticação de ONU	**show onu-authenticate mode slot** slot_id	Opcional
Acesse o modo de configuração de porta PON	**interface pon** port_id	Opcional
Visualização do modo de autenticação de porta PON padrão	**show onu-authenticate mode**	Opcional
Configuração do modo de autenticação de porta PON para sem autenticação	**onu-authenticate mode disable**	Opcional

Obs.: *este é o modo* Padrão *da OLT.*

Exemplo de configuração de modo sem autenticação

» Requisitos de rede:

» Explicação da rede: por padrão a ONU pode estar conectada:

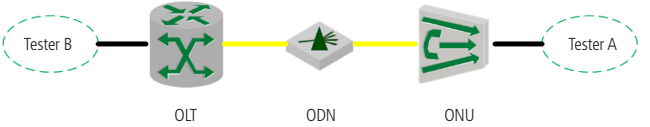


Diagrama de configuração para o modo sem autenticação

» Passos de configuração:

» Exiba o modo de autenticação ONU da porta PON no OLT no modo de configuração vazio:

» Exiba a configuração de autenticação da ONU na porta PON (no modo *Global*):

OLT4840E(config)#show onu-authenticate mode slot 0

slot : 0

pon 0/1 onu-authentication mode: disable

pon 0/2 onu-authentication mode: disable

pon 0/3 onu-authentication mode: disable

pon 0/4 onu-authentication mode: disable

» Exiba a configuração de autenticação da porta PON 0/1 (no modo de configuração de porta);

OLT4840E(config)#interface pon 0/1

OLT4840E(config-if-pon-0/1)#show onu-authenticate mode

slot : 0

pon 0/1 onu-authentication mode: disable

» Verifique os resultados:

As ONUs conectadas podem ser registradas.

Modo de autenticação por MAC

Configuração do modo de autenticação por MAC

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta PON	**interface pon** port_id	-
Configuração do modo de autenticação de ONU por MAC	**onu-authenticate mode mac-auth** {white-list| black-list }	Opcional
Adicionar um registro na *whitelist* (lista de permissão) da porta PON	**white-list add** onu_mac	Opcional
Remover um registro na *whitelist* (lista de permissão) da porta PON	**white-list del** { onu_mac | all}	Opcional
Adicionar um registro na *blacklist* (lista de bloqueio) da porta PON	**black-list add** onu_mac	Opcional
Remover um registro na *blacklist* (lista de bloqueio) da porta PON	**black-list del** { onu_mac | all}	Opcional
Visualização da whitelist da porta PON	**show white-list**	Opcional
Visualização da blacklist da porta PON	**show black-list**	Opcional

Obs.: *a autenticação MAC inclui autenticação de whitelist e autenticação de blacklist. Na whitelist, o endereço MAC da ONU pode ser registrado apenas quando está presente na lista; no modo* Blacklist, *o endereço MAC da ONU presente na lista não pode ser registrado.*

Exemplo de configuração da autenticação por MAC

- Requisitos de rede:
  - Explicação da rede: configure o modo de autenticação da ONU como autenticação por MAC e acesse a ONU para verificar se a ONU pode estar online ou não.

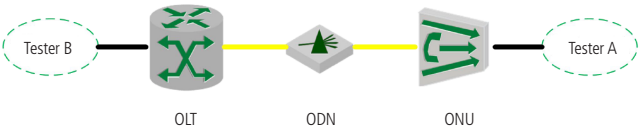


Diagrama de configuração da autenticação por MAC

» Passos de configuração:

» Configure o modo de autenticação de PON 0/1 para autenticação de whitelist:
OLT4840E(config)#int pon 0/1

OLT4840E(config-if-pon-0/1)#onu-authenticate mode mac-auth white-list

OLT4840E(config-if-pon-0/1)#white-list add mac 00:0a:5a:00:01:01

» Adicione um registro da whitelist com o ONU_id para ser 1 e o endereço MAC: 00:0a:5a:00:01:01 para PON 0/1.
OLT4840E(config-if-pon-0/1)#white-list add mac 00:0a:5a:00:01:01

» Exiba a whitelist configurada na porta PON 0/1:
OLT4840E(config-if-pon-0/1)#show white-list

WHITE LIST:

Port Index Mac Address

pon-0/1 1 00:0a:5a:00:01:01

Total white-list entries: 1 .

» Verifique os resultados:
OLT4840E(config-if-pon-0/1)#show onu-status

ONU Mac Address Rtt RegisterTime Type Software State

0/1/1 00:0a:5a:00:01:01 14 16/11/09 09:56:15 2400 B01D004P2 Up

0/1/2 00:0a:5a:ff:ff:69 - - - - Down

Total onu entries: 2 .

onu online : 1 .

» A ONU que acessou com o endereço MAC 00: 0a: 5a: 00: 01: 01 pode ser registrada normalmente.

» (A ONU que não acessou com o endereço MAC 00:0a:5a:00:01:01 não pode ser registrada normalmente.

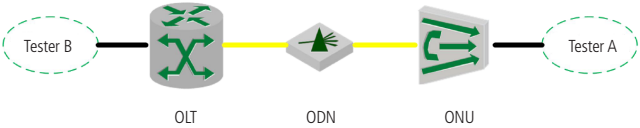
Autenticação baseada em identificador lógico

Configuração da autenticação baseada em identificador lógico

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta PON	**Interface pon** port_id	Opcional
Configuração do modo de autenticação de ONU por identificador lógico	**onu-authenticate mode loid-auth**	Opcional
Adicionar um ID lógico na porta PON	**loid-list add loid** loid_id **password** password_id	Opcional
Remover um ID lógico na porta PON	**loid-list del** {loid loid _id| all}	Opcional
Visualização da lista de IDs lógicos da porta PON	**show loid-list**	Opcional

Exemplo de configuração de autenticação baseado em identificador lógico

- Requisitos de rede:
  - Explicação da rede: configure o modo de autenticação da ONU como identificação lógica e, em seguida, acesse a ONU para verificar se a ONU pode estar online ou não.



- Passos de configuração:
  - Configure o modo de autenticação de ONU na PON 0/1 para autenticação com base na identificação lógica:
    OLT4840E(config-if-pon-0/1)#onu-authenticate mode loid-auth
  - Adicione uma ID com LOID 000a5a000101 e senha de 1111 na PON 0/1:
    OLT4840E(config-if-pon-0/1)#loid-list add loid 000a5a000101 password 1111

» Exiba a lista de ID lógicos na porta PON 0/1:

OLT4840E(config-if-pon-0/1)#show loid-list

LOID LIST:

Index Loid Password

1 000a5a000101 1111

Total loid entries: 1 .

» Verifique o resultado:

OLT4840E(config-if-pon-0/1)#show onu-status

ONU Mac Address Rtt RegisterTime Type Software State

0/1/1 00:0a:5a:00:01:01 13 16/11/09 10:06:53 2400 B01D004P2 Up

0/1/2 00:0a:5a:ff:ff:69 - - - - Down

Total onu entries: 2 .

onu online : 1 .

(1) A ONU que acessou com a LOID 000a5a000101 e senha 1111 pôde ser registrada normalmente.

(2) A ONU que não acessou com o LOID 000a5a000101 e senha 1111 não pôde ser registrada normalmente.

Modo de autenticação híbrida

Configuração do modo de autenticação híbrida

» Modo de autenticação híbrida:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta PON	**Interface pon** port_id	Opcional
Configuração do modo de autenticação de ONU híbrido	**onu-authenticate mode hybrid-auth**	Opcional
Adicionar um registro de interface PON híbrida	**hybrid-list add** { loid|mac } {[loid loid_id password password_id] | [onu-mac]}	Opcional
Remover um registro de interface PON híbrida	**hybrid-list del {loid** loid_id **| mac** onu_mac **| all}**	Opcional

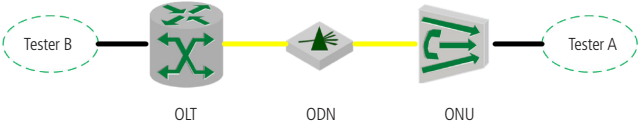
Operação	Comando	Obrigatório/ opcional
Visualização da lista registros de interface PON híbrida	**show hybrid-list**	Opcional

Obs.: *desta forma, o OLT se autentica com base no endereço MAC da ONU. Se a autenticação falhar, o OLT inicia a autenticação com base na ID lógica da ONU.*

Exemplo de configuração para o modo de autenticação híbrida

» Requisitos de rede:

» Explicação da rede: configure o modo de autenticação da ONU como modo de autenticação híbrida, em seguida, acesse a ONU para verificar se pode estar online ou não.



» Passos de configuração:

» Configure o modo de autenticação ONU da PON 0/1 como modo de autenticação híbrida:

OLT4840E(config-if-pon-0/1)#onu-authenticate mode hybrid-auth

» Adicione o registro de autenticação LOID com o LOID 000a5a000101 e a senha 1111 na PON 0/1:

OLT4840E(config-if-pon-0/1)#hybrid-list add LOID 000a5a000101 password 1111

» Adicione a entrada de autenticação MAC com o endereço MAC 00:0a:5a:04:05:06 na PON 0/1.

OLT4840E(config-if-pon-0/1)#hybrid-list add mac 00:0a:5a:04:05:06

» Exibir a lista de autenticação híbridas no PON 0/1

OLT4840E(config-if-pon-0/1)#show hybrid-list

Hybrid LIST:

Index Loid/Mac Address Password

1 000a5a000101 1111

2 00:0a:5a:04:05:06

Total hybrid entries: 2 .

» Verifique os resultados:

OLT4840E(config-if-pon-0/1)#show onu-status

ONU Mac Address Rtt RegisterTime Type Software State

0/1/1 00:0a:5a:00:01:01 14 16/11/09 10:19:38 2400 B01D004P2 Up

0/1/2 00:0a:5a:ff:ff:69 - - - - Down

Total onu entries: 2 .

onu online : 1 .

» A ONU com MAC ou LOID na lista de autenticação híbrida pode ser registrada online normalmente.

» A ONU sem MAC ou LOID na lista de autenticação híbrida não pode ser registrada online normalmente.

9.2. ONU Ranging

Visão geral de ONU Ranging

Uma vez que o canal de upstream do EPON adota o modo *TDMA*, o acesso multiponto leva a diferentes atrasos do quadro de dados de cada ONU. Portanto, é necessário introduzir as técnicas de compensação de atraso e de intervalo para evitar a colisão de dados no domínio do tempo. Assim, é importante medir com precisão a distância entre cada ONU e o OLT, e ajustar com precisão o atraso da transmissão de cada ONU para alcançar a sincronização do sistema.

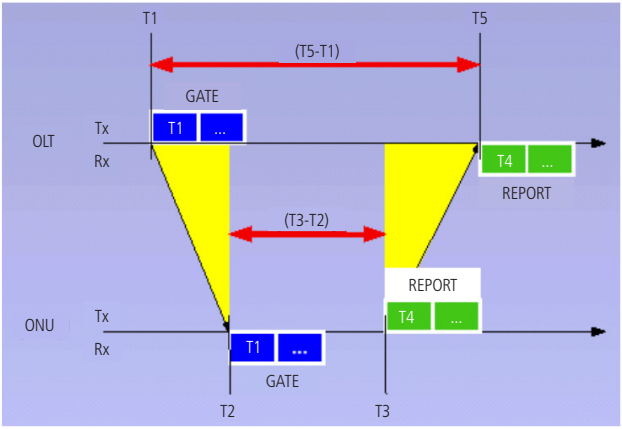
» **Sincronização do sistema:** como cada sistema EPON adota o modo de divisão do tempo, o OLT e as ONUs devem alcançar a sincronização antes de iniciarem a comunicação para garantir a transmissão correta das informações. Para isso, é necessário um tempo de referência comum, no EPON, ele é o relógio do OLT. Periodicamente são transmitidas as informações de sincronização para que as ONUs possam ajustar seus próprios relógios.

Como a distância entre cada ONU e o OLT é diferente, o atraso da transmissão deve ser diferente. Para isso, o relógio da ONU deve estar adiantado em relação ao relógio do OLT. Esta diferença é o atraso da transmissão do uplink. Ou seja, se o OLT encaminha um bit no momento 0, a ONU deve recebê-lo no tempo RTT (atraso de transmissão de ida e volta). RTT é igual ao atraso de transmissão de ligação downlink mais atraso de transmissão de ligação uplink, ele deve ser calculado e enviado para a ONU. O processo de aquisição do RTT é variável. Quando o sistema EPON atinge a sincronização, as informações encaminhadas pelas diferentes ONUs sob o mesmo OLT não entrarão em colisão.

» **Ranging e atraso de compensação:** medindo com precisão a distância de cada ONU para o OLT e ajustando o atraso de transmissão, os intervalos entre as janelas de transmissão da ONU podem ser reduzidos, melhorando assim a taxa de utilização do canal upstream e reduzindo o tempo de atraso. Além disso, o processo de ranging deve levar plenamente em conta a configuração do EPON. Por exemplo, se uma nova ONU for adicionada enquanto o sistema estiver funcionando, o ranging não deve ter um impacto significativo em outras ONUs. O ranging do EPON é iniciado e completado pelo OLT, que monitora o plug and play da ONU através da data / hora (Timestamp).

O processo básico é o seguinte:

O OLT transmite o sinal de sincronização do slot e o indicador do intervalo de tempo ocioso através do canal downstream no momento T1; quando a ONU detecta uma marca de intervalo de tempo ocioso em T2, ela reinicia o temporizador local em T1; no momento T3, ela encaminha um quadro de dados de resposta online que contém os parâmetros da ONU (endereço, nível de serviço, etc.). Nesse caso, o carimbo de data / hora local no quadro de dados é T4; o OLT recebe o quadro de resposta no momento T5. Através deste quadro de resposta, o OLT não só obtém parâmetros da ONU, mas também calcula o atraso do canal entre o OLT e a ONU (RTT = T2-T1 + T5-T3 = T5-T4).



RTT = (T5 - T1) - (T3 - T2) = (T5 - T1) - (T4 - T1) = T5 - T4

Diagrama para o ranging e o atraso de compensação

» **Compensação RTT:** a compensação de atraso é realizada no lado do OLT. A autorização encaminhada para a ONU reflete a hora de chegada em função da compensação RTT. Por exemplo, se o OLT receber dados no tempo T, o OLT envia um GATE = T-RTT incluindo o início do slot. De fato, o atraso mínimo definido entre o timestamp e a hora de início é o tempo de processamento permitido. O atraso máximo definido entre o timestamp e o tempo de início é definido para manter a rede sincronizada.

Visão geral de configuração de ONU Ranging

» Visão geral de configuração de ONU Ranging:

Configuração da atividade		Obrigatório/ opcional	Informação detalhada
Configuração básica do registro e gerenciamento de ONU	Configuração de ONU Ranging	Opcional	2.3

ONU Ranging

Configuração de ONU Ranging

» Configuração de ONU Ranging:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Acesse o modo de configuração de porta PON	**Interface pon** port_id	Opcional
Obter a distância da conexão entre ONU e OLT	**onu-rtt** onu_id	Opcional

Obs.: *Rtt é o tempo de ida e volta, 1tq é 16ns, a velocidade da luz na velocidade da fibra é cerca de 200.000 km / segundo (C / índice de refração 1.5), 1tq é equivalente a 1.5 m; no entanto, o RTT também inclui LaserON, LaserOn Delay, AGC e tempo de CDR do laser OLT e do laser ONU, portanto, o real 1 tq = 1.500 ~ 3.180 m.*

Configuração exemplo do ONU Ranging

» Requisitos de rede:

» Explicação da rede: conecte a fibra de 4KM entre a ONU e o OLT, você precisa medir a distância da ligação óptica física entre a ONU e o OLT.

OLT ODN ONU

» Passos de configuração:

» Leia a distância de ligação física (em unidades de tq) da ONU com o ONU-ID 1 na PON 0/1.

OLT4840E(config-if-pon-0/1)#onu-rtt 1

onu 0/1/1 rtt is 14 tq.

» Exibir a informação de estado da ONU 0/1/1 e a distância de ligação física (m)

OLT4840E(config)#show onu-status 0/1/1

ONU Mac Address Rtt RegisterTime Type Software State

0/1/1 00:0a:5a:00:01:01 14 16/11/09 10:23:31 2400 B01D004P2 Up

Total onu entries: 1 .

onu online : 1 .\

OLT4840E(config)#show onu-status mac 00:0a:5a:00:01:01

ONU Mac Address Rtt RegisterTime Type Software State

0/1/1 00:0a:5a:00:01:01 14 16/11/09 10:23:31 2400 B01D004P2 Up

Total onu entries: 1 .

onu online : 1 .

» Verifique os resultados:

Os três métodos podem ler com precisão a distância real do link óptico físico.

9.3. ONU-VLAN

Visão geral de ONU-VLAN

As regras específicas para cada modo *VLAN* são definidas da seguinte forma:

» **Modo de transmissão transparente de VLAN:** neste modo, o dispositivo (OLT / ONU) recebe o quadro Ethernet de uplink/downlink sem qualquer processamento (independentemente de o quadro Ethernet possui tag VLAN ou não) e o encaminhará para outra interface. A tabela a seguir exibe como um OLT / ONU manipula pacotes de dados no modo de transmissão transparente de VLAN.

» O modo de processamento do dispositivo em modos de transmissão transparentes de VLAN:

Direção	tag/untag	Modo de processamento
Uplink	Com tag VLAN	Sem qualquer processamento para o pacote Ethernet; encaminha
	Sem tag VLAN	Sem qualquer processamento para o pacote Ethernet; encaminha
Downlink	Com tag VLAN	Sem qualquer processamento para o pacote Ethernet; encaminha
	Sem tag VLAN	Sem qualquer processamento para o pacote Ethernet; encaminha

» **Modo de tag VLAN:** neste modo, o dispositivo OLT / ONU processa o quadro Ethernet de uplink recebido adicionando uma tag VLAN; para um quadro Ethernet downlink, a tag VLAN é removida. A tabela a seguir exibe como um OLT / ONU manipula pacotes de dados no modo de tag VLAN.

» O modo de processamento do dispositivo no modo *Tag VLAN*:

Direção	Tag/untag	Modo de processamento
Uplink	Com tag VLAN	Descarta
	Sem tag VLAN	Marcado com a nova tag VLAN (o parâmetro principal é VID), encaminha.
Downlink	Com tag VLAN	Reencaminha para a porta correspondente de acordo com o VID, e descartar a Tag; se a ID de VLAN do pacote marcado do downlink não for o VID da porta, o pacote será descartado.
	Sem tag VLAN	Descarta

» **Modo de tradução de VLAN:** neste modo, o dispositivo (OLT ou ONU) converte a tag VLAN marcada pelo usuário no uplink em uma tag VLAN da rede exclusiva (a tag VLAN marcada pelo usuário pode não ser única na rede, podendo haver outros usuários no mesmo sistema com o mesmo VID) e faz o inverso para o downlink. Quando o dispositivo suporta a tradução de VLAN, ele deve suportar o valor EtherType 0×8100 e possuir a opção para utilização de outros valores EtherType. A tabela a seguir exibe como um OLT ou ONU manipula pacotes de dados no modo de tradução VLAN.

Direção	Tag/untag	Modo de processamento
Uplink	Com tag VLAN	Se o VID da tag original tiver uma entrada correspondente na lista de conversão da porta, o VID é convertido para o correspondente e encaminhado.
		Se o VID não tiver entrada correspondente na lista de tradução da porta correspondente, o pacote será descartado. Atualmente, apenas o equipamento é necessário para converter VID. A conversão em outros campos (como TPID, CFI e Pri) não é necessária no momento. O dispositivo deve configurar o TPID convertido para o valor padrão (TPID = 0×8100) e Pri permanece no valor original.
	Sem tag VLAN	A VLAN untagged é marcada com a VLAN padrão e é encaminhado.

Direção	Tag/untag	Modo de processamento
Downlink	Com tag VLAN	Se o VID da tag original tiver uma entrada correspondente na lista de tradução da porta, o VID é convertido para o correspondente (entrada) e encaminhado.
		Se o VID da tag original é o VID padrão, a etiqueta é removida e o pacote será encaminhado.
		Se o VID não tiver entrada correspondente na lista de conversão da porta, o pacote será descartado. Atualmente, apenas o equipamento é necessário para converter VID. Além disso, ele deve definir o TPID convertido para o valor padrão (TPID = 0×8100) e Pri permanece no valor original.
	Sem tag VLAN	Descarta

» **Modo *VLAN-Trunk*:** a tabela a seguir exibe como um OLT ou ONU manipula pacotes de dados no modo *VLAN-Trunk*.

Direção	Tag/untag	Modo de processamento
Uplink	Com tag VLAN	Se a ID da VLAN do pacote pertence à VLAN que é permitida para passar pela porta, o pacote será encaminhado para uplink; se a ID da VLAN do pacote não pertence à VLAN que é permitida para passar pela porta, o pacote será descartado.
	Sem tag VLAN	A VLAN untagged é marcada com a VLAN padrão e pode ser encaminhada.
Downklin	Com tag VLAN	Se o ID da VLAN do pacote pertence à VLAN que é permitida para passar pela porta, o pacote será encaminhado para downlink; se o pacote carregar uma ID de VLAN de "VLAN padrão", a tag será removida e em seguida, o pacote será encaminhado para downlink; se a ID da VLAN do pacote não pertence à VLAN que é permitida para passar pela porta, o pacote será descartado.
	Sem tag VLAN	Descarta

Visão geral da configuração de CTC-VLAN

Visão geral de configuração de CTC-VLAN

Configuração da atividade		Obrigatório/ opcional	Informação detalhada
Configurações básicas de autenticação de ONU	Modo de transmissão transparente	Obrigatório	1.3
	Modo *VLAN* com tag	Obrigatório	1.4
	Modo de tradução de VLAN	Obrigatório	1.5
	Modo *Trunk*	Obrigatório	1.6

Modo de transmissão transparente

Configuração do modo de transmissão transparente

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de ONU	**onu** onu_id	Obrigatório
Configuração o modo de transmissão transparente	**onu-vlan-mode transparent**	Obrigatório
Visualização do modo de VLAN da ONU	**show onu-vlan-mode**	Opcional

Obs.: *a ONU no modo* Global *funciona em todas as portas da ONU. No modo de porta ONU, a configuração só se aplica à porta especificada. Da mesma forma, o comando view.*

Exemplo de configuração de modo Transparente de transmissão

» Requisitos de rede:

O diagrama de rede é o seguinte.

» **Requisitos:** o frame Ethernet de uplink do tester A pode ser encaminhado de forma transparente para o tester B, independentemente de o pacote ter ou não uma tag; ao mesmo tempo, a estrutura Ethernet downlink do tester B pode ser encaminhada de forma transparente para o tester A, independentemente de o pacote ter ou não tag.

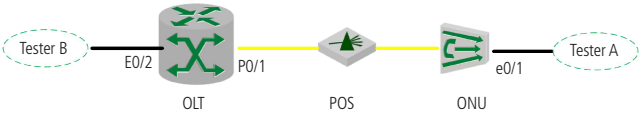


Diagrama de VLAN transparente

» Passos de configuração:

» Acesse o modo de configuração de ONU:

OLT4840E(config)#onu 0/1/1

» Configure a ONU para operar em modo de transmissão transparente:

OLT4840E(onu-0/1/1)#onu-vlan-mode transparent

» Verifique o resultado:

» Display the ONU VLAN mode:

OLT4840E(onu-0/1/1)#show onu-vlan-mode

onu 0/1/1 :

port ID : 1 ctc vlan mode : transparent

port ID : 2 ctc vlan mode : transparent

port ID : 3 ctc vlan mode : transparent

port ID : 4 ctc vlan mode : transparent

O frame Ethernet de uplink do tester A pode ser encaminhado de forma transparente para o tester B, independentemente de o pacote ter ou não uma tag; ao mesmo tempo, a estrutura Ethernet downlink do tester B pode ser encaminhada de forma transparente para o tester A, independentemente de o pacote ter ou não tag.

Modo *VLAN com tag*

Configuração do modo VLAN com tag

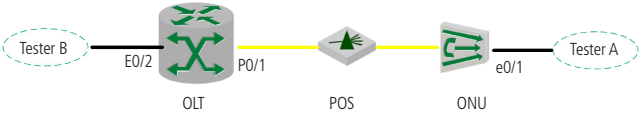
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de ONU	**onu** *onu_id*	Obrigatório
Configuração o modo de VLAN com tag	**onu-vlan-mode tag vlan** vlan-id	Obrigatório
Visualização do modo de VLAN da ONU	**show onu-vlan-mode**	Opcional

Exemplo de configuração do modo VLAN com tag

- Requisitos de rede:

  O diagrama de rede é o seguinte.

  - **Requisitos:** os pacotes de uplink não marcados do tester A são encaminhados para o tester B a passar pela ONU e com a tag VLAN 10, enquanto os pacotes de uplink marcados do tester A serão descartados; os pacotes marcados com VLAN 10 do tester B terão suas tags de VLAN removidas e serão encaminhados para o tester A.



- Passos de configuração:
  - Acesse o modo de configuração de ONU:

    OLT4840E(config)#onu 0/1/1
  - Configure a ONU para operar em modo *VLAN com tag*:

    OLT4840E(onu-0/1/1)#onu-vlan-mode tag vlan 10
- Verifique o resultado:
  - Display ONU VLAN mode

    OLT4840E(onu-0/1/1)#show onu-vlan-mode

onu 0/1/1 :

port ID : 1 ctc vlan mode : tag default vlan : 10

port ID : 2 ctc vlan mode : tag default vlan : 10

port ID : 3 ctc vlan mode : tag default vlan : 10

port ID : 4 ctc vlan mode : tag default vlan : 10

Os pacotes de uplink não marcados do tester A são encaminhados para o tester B, com a tag VLAN 10. Enquanto os pacotes de uplink marcados do tester A serão descartados; os pacotes marcados com VLAN 10 do tester B terão suas tags de VLAN removidas e serão encaminhados para o tester A.

Modo de tradução de VLAN

Configuração do modo de tradução de VLAN

» Configuração do modo de tradução de VLAN:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Acesse o modo de configuração de ONU	**onu** onu_id	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** port_id	É necessário acessar o modo de configuração de ONU antes de acessar este modo
Configuração de tabela de tradução de VLAN	**onu-vlan-mode translation vlan** default-vlan **old_vlan** old_vlan **new_vlan** new_vlan	Obrigatório
Remover tabela de tradução de VLAN	**onu-vlan-mode translation delete old_ vlan** old_vlan **new_vlan** new vlan	Opcional
Visualização do modo de VLAN da ONU	**show onu-vlan-mode**	Opcional

Obs.: *» O modo de tradução VLAN precisa ser configurado no modo de porta ONU.*

» Se a tabela de tradução VLAN tiver apenas uma entrada, você não poderá excluí-la através do comando de ONU-VLAN-mode translation delete.

Exemplo de configuração do modo de tradução de VLAN

» Requisitos de rede:

» Direção de Uplink:

O tester A encaminha um pacote não marcado para a ONU. O tester B recebe o pacote com a etiqueta VLAN 10.

O tester A encaminha um pacote com VLAN 20 para a ONU e o pacote é encaminhado para o tester B com a etiqueta VLAN 30.

O tester A envia pacotes de outras VLAN para a ONU. Os pacotes não podem ser encaminhados para o tester B.

» Direção Downlink:

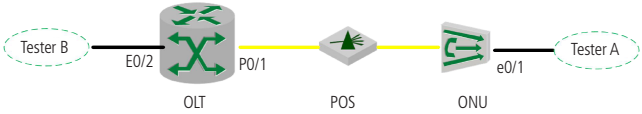
O pacote de downlink do tester B não é marcado com o VLAN depois de passar pela porta OLT PON. O pacote não pode ser transferido para o tester A.

O pacote downlink do tester B é marcado com o VLAN 10 depois de passar pela porta OLT PON. O pacote é transferido para o tester A mas não carrega a tag VLAN.

O pacote de downlink do tester B é marcado com o VLAN 30 depois de passar pela porta OLT PON. O pacote é transferido para o tester A e ele carrega a VLAN 20.

O pacote downlink do tester B é marcado com outras tags VLAN depois de passar pela porta OLT PON. O pacote não pode ser transferido para o tester A.

O diagrama de rede é o seguinte:



» Passos de configuração:

» Acesse o modo de configuração da porta ONU:

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#int ethernet 0/1

» Configure a lista de tradução de VLAN:

OLT4840E(onu-0/1/1-reth-0/1)#onu-vlan-mode translation vlan 10 old_vlan 20 new_vlan 30.

» Verifique o resultado:

» Exiba o modo de VLAN da ONU:

OLT4840E(onu-0/1/1-reth-0/1)#show onu-vlan-mode

onu 0/1/1 :

port ID : 1 ctc vlan mode : translation default vlan : 10

translation list : old vlan new vlan

1 20 30

Os resultados estão de acordo com o esperado.

Modo *Trunk*

Configuração do modo Trunk

» Configuração do modo *Trunk*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de ONU	**onu** onu_id	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** port_id	É necessário acessar o modo de configuração de ONU antes de acessar este modo
Configuração de registros de VLAN-Trunk	**onu-vlan-mode trunk vlan** default-vlan **allow-vlan** vlan-list	Obrigatório
Remover registros de VLAN-Trunk	**onu-vlan-mode trunk delete allow-vlan** vlan-list	Opcional
Visualização do modo de VLAN da ONU	**show onu-vlan-mode**	Opcional

Exemplo de configuração de VLAN-Trunk

» Requisitos de rede:

» Direção de Uplink:

O uplink do tester A encaminha um pacote não marcado. Ao passar pela ONU, o pacote será encaminhado com a tag VLAN 10 para o tester B.

O uplink do tester A encaminha pacotes com VLAN 20-27, e os pacotes são transmitidos de forma transparente para o tester B depois de passar pela ONU.

O uplink do tester A encaminha pacotes com outras tags VLAN, e os pacotes são descartados ao passar pela ONU.

» Direção de downlink:

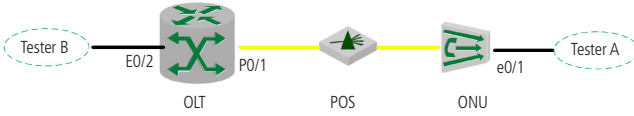
O pacote downlink do tester B não carrega a tag VLAN depois de passar pela porta OLT PON, o pacote não pode ser transferido para o tester A.

O pacote downlink do tester B carrega o VLAN 10 depois de passar pela porta OLT PON, o pacote é transferido para o tester A, mas ele não carrega a tag VLAN.

O pacote downlink do tester B carrega VLAN 20-27 depois de passar pela porta OLT PON, o pacote é transferido para o tester A.

O pacote downlink do tester B carrega outras tags VLAN depois de passar pela porta OLT PON, o pacote não pode ser transferido para o tester A.

O diagrama de rede é o seguinte:



» Passos de configuração:

» Acesse o modo de configuração de portas da ONU:

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#interface ethernet 0/1

» Configure a ONU para operar no modo *Trunk*:

OLT4840E(onu-0/1/1-reth-0/1)#onu-vlan-mode trunk vlan 10 allow-vlan 20-27

» Verifique o resultado:

» Display ONU vlan mode:

OLT4840E(onu-0/1/1-reth-0/1)#show onu-vlan-mode

onu 0/1/1 :

port ID : 1 ctc vlan mode : trunk default vlan : 10

trunk allow-vlan list : 20 21 22 23 24 25 26 27

Os resultados estão de acordo com o esperado.

9.4. Configuração de portas da ONU

Visão geral da configuração de portas da ONU

Configuração de portas da ONU via OLT. Os conteúdos de configuração incluem controle de fluxo de porta, modo de negociação automática e limitação de velocidade.

Visão geral da configuração de porta da ONU

Configuração de task		Obrigatório / opcional	Detalhes de configuração
Configuração de portas da ONU	Configuração do estado de link da porta	Opcional	1.3
	Habilitar/desabilitar a porta	Opcional	1.4
	Configuração do controle de fluxo da porta	Opcional	1.5
	Configuração de auto-negociação da porta	Opcional	1.6
	Limitação de velocidade da porta	Opcional	1.7

Estado da conexão (link) da porta

Configuração do estado do link da porta

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório

Operação	Comando	Obrigatório / opcional
Visualização do estado da conexão	show **onu-interface** [ethernet port_id]	Pode ser executado para todas as portas, ou apenas para a porta especificada no comando.

Exemplo de visualização do estado do link da porta da ONU

» Visualização do estado do link da porta e0/1:

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#show onu-interface ethernet 0/1

ONU 0/1/1

ONU port 1 is Enable, port link is LINK DOWN

ONU auto negotiate ability :

ability value[1] : Half duplex 10BASE-T

ability value[2] : Full duplex 10BASE-T

ability value[3] : Half duplex 100BASE-T4

ability value[4] : Half duplex 100BASE-TX

ability value[5] : Full duplex 100BASE-TX

ability value[6] : Full duplex PAUSE

ability value[7] : Full duplex Symmetric PAUSE

ability value[8] : Half duplex 100BASE-T2

ability value[9] : Full duplex 100BASE-T2

ability value[10] : Half duplex 1000BASE-T

ability value[11] : Full duplex 1000BASE-T

speed auto is Enable, Flow control is Disable

bandwidth ingress is Disable

bandwidth egress is Disable

Habilitar/desabilitar a porta da ONU

Habilitar/desabilitar a porta da ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** port_id	Obrigatório
Habilitar a porta	no **onu-shutdown**	Por padrão da porta da ONU está habilitada
Desabilitar a porta	**onu-shutdown**	Opcional

Exemplo de habilitar e desabilitar as portas

» Desabilite a porta 1 da ONU 0/1/1:
OLT4840E(onu-0/1/1-reth-0/1)#onu-shutdown

Habilite a porta 1 da ONU 0/1/1

OLT4840E(onu-0/1/1-reth-0/1)#no onu-shutdown

Controle de fluxo da porta da ONU

Quando a porta da ONU permite esta função, a ONU transmitirá o frame de controle de fluxo para o remetente de origem se ocorrer um bloqueio de porta. E então a extremidade oposta diminuirá a velocidade quando encaminhar pacotes.

Configuração do controle de fluxo para a porta da ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** port_id	Obrigatório

Operação	Comando	Obrigatório / opcional
Habilitar o controle de fluxo	**onu-flow-control**	Opcional
Desabilitar o controle de fluxo	no **onu-flow-control**	Opcional

Exemplo de configuração de controle de fluxo para a porta da ONU

» Habilite o controle de fluxo para a porta 1 da ONU 0/1/1:
OLT4840E(onu-0/1/1-reth-0/1)#onu-flow-control

» Desabilite o controle de fluxo para a porta 1 da ONU 0/1/1:
OLT4840E(onu-0/1/1-reth-0/1)#no onu-flow-control

Auto-negociação da porta da ONU

A porta da ONU possui o modo de auto-negociação e o modo de não auto-negociação. A velocidade da porta será full duplex e half duplex em cada caso, respectivamente.

Configuração do modo de auto-negociação para a porta

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** port_id	Obrigatório
Configuração do modo de auto-negociação da porta da ONU	**onu-speed auto**	Por padrão, este modo estará ativo
Configuração do modo de não auto-negociação da porta da ONU	no **onu-speed auto**	Opcional

Exemplo de auto-negociação da porta da ONU

» Configuração da velocidade da porta ONU para auto-negociação:
OLT4840E(onu-0/1/1-reth-0/1)#onu-speed auto

» Configuração da velocidade da porta ONU para não auto-negociação:
OLT4840E(onu-0/1/1-reth-0/1)#no onu-speed auto

Limitação de velocidade da porta da ONU

Limitação de velocidade da porta da ONU na entrada e na saída para evitar a perda de pacotes de uplink e de downlink.

Configuração da limitação de velocidade da porta

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** port_id	Obrigatório
Configurar a limitação de velocidade de entrada da porta	**onu-bandwith ingress cir** cir-number **cbs** cbs-number **ebs** ebs-number	Opcional
Desabilitar a limitação de velocidade de entrada	no **onu-bandwith ingress**	Opcional
Configurar a limitação de velocidade de saída da porta	**onu-bandwith egress cir** cir-number **pir** pir-number	Opcional
Desabilitar a limitação de velocidade de entrada	no **onu-bandwith egress**	Opcional

Obs.: » *Descrição de parâmetros de velocidade de entrada:*
- » ***cir-number:*** *Commited Burst Size: 64 - 1024000 kbps.*
- » ***cbs-number:*** *Commited Information Rate: 1523 - 1000000 Byte.*
- » ***ebs-number:*** *Excess Burst Size: 0 - 1522 Byte.*

» *Parâmetros de descrição de velocidade de saída:*
- » ***cir-number:*** *(Committed Information Rate: 64 - 1024000 kbps.*
- » ***pir-number:*** *Peak Information Rate: 64 - 1024000 kbps.*

Exemplo de limitação de velocidade de porta da ONU

» Configuração da largura de banda de entrada para a porta 1 da ONU 0/1/1:
OLT4840E(onu-0/1/1-reth-0/1)#onu-bandwidth ingress cir 1024 cbs 1600 ebs 2

» Configuração da largura de banda de saída para a porta 1 da ONU 0/1/1:
OLT4840E(onu-0/1/1-reth-0/1)#onu-bandwidth egress cir 1024 pir 4096

9.5. Informações básicas da ONU

É possível verificar informações básicas da ONU através do OLT, incluindo a versão ONU, desempenho, chipset, firmware, número de série, entre outras:

- **Informações de versão:** incluindo versão atual de software, plataforma de software, versão de hardware, BOOTROM versão e assim por diante.
- **Informações de desempenho:** incluindo as configurações suportadas pela ONU e os parâmetros relacionados.
- **Informações do chipset:** incluindo ID do fornecedor do chipset, MODEL ID e assim por diante.
- **Informações de firmware:** incluindo o número de firmware da ONU.
- **Informações de número de série:** incluindo ID de fornecedor da ONU, ID do MODELO, endereço MAC, versão do software e versão do hardware e mais.

Visualização de informações básicas da ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Visualização da versão da ONU	**show onu-version**	Opcional
Visualização de informações de desempenho da ONU	**show onu-capabitilies** **show onu-capabitilies-2**	*onu-capabilities-2* é a extensão de *onu-capabilities*
Visualização de informações de chipset da ONU	**show onu-pon-chip**	Opcional
Visualização de informações de firmware da ONU	**show onu-firmware**	Opcional
Visualização do número de série da ONU	**show onu-sn**	Opcional

Exemplo de visualização de informações básicas da ONU

- Exibir informações de desempenho da ONU 0/1/1:
  OLT4840E(onu-0/1/1)#show onu-capability

onu 0/1/1 :
onu capability: serviceSupported 2
onu capability: numGEPorts 0
onu capability: geBitmap 0x0
onu capability: numFEPorts 4
onu capability: feBitmap 0xf
onu capability: numPOTSPorts 0
onu capability: numE1Ports 0
onu capability: numUSQueues 1
onu capability: maxQueueUSPort 32
onu capability: numDSQueues 1
onu capability: maxQueueDSPort 20
onu capability: BatteryBackup 0

» OLT4840E(onu-0/1/1)#show onu-capabilities-2
onu 0/1/1 :
onu capability-2: OnuType SFU
onu capability-2: MultiLLID Not Support
onu capability-2: ProtectionType Not Support
onu capability-2: NumOfPon 1
onu capability-2: NumOfSlot 0
onu capability-2: NumOfInterfaceType 1
onu capability-2: InterfaceType GE
onu capability-2: NumOfPort 4
onu capability-2: BatteryBackup Not Support

» Exibir a informação do chipset da onu 0/1/1:
OLT4840E(onu-0/1/1)#show onu-pon-chip
Chipset of onu 0/1/1 :
Vendor id :
Model Id :0x0 0xa0
Revision :0x00
IC_Version/Date :19/04/21

» Exibir as informações de firmware da ONU 0/1/1:

OLT4840E(onu-0/1/1)#show onu-firmware

firmware of onu 0/1/1 :

» Exibir o número de série da ONU 0/1/1:
OLT4840E(onu-0/1/1)#show onu-sn

SN of Onu 0/1/1:

Vendor ID : 0T4R (HEX: 30 54 34 52)

Model : 6838 (HEX: 36 38 33 38)

OnuID(MAC) : 78:30:3b:b0:88:00

HW : CM.1.1.6

SW : OT04R68.1.2.0

9.6. Descrição de ONU

Visão geral da descrição de ONUs

O gerente de rede pode adicionar uma etiqueta de descrição na ONU para distinguir o serviço provido em cada porta da ONU, de modo a localizar os serviços das portas da ONU.

Configuração da descrição de ONUs

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Configuração da descrição da porta da ONU	**onu-description** description	Opcional
Visualização da descrição da porta da ONU	**show onu-description**	Opcional

Exemplo para descrição de portas da ONU

» Configure a descrição de portas da ONU:
OLT4840E(onu-0/1/1)#onu-description aa

Display ONU port description configuration

OLT4840E(onu-0/1/1)#show onu-description

The name of ONU 0/1/1: aa

9.7. Isolamento de portas da ONU

Funcionamento do isolamento de portas

O isolamento de portas da ONU significa adicionar sua porta a um grupo de isolamento para separá-la de outras evitando o vazamento de mensagens.

Uma ONU pode definir apenas um grupo de isolamento. Um grupo de isolamento só pode trocar mensagens com a porta de uplink (no caso da ONU a porta PON é a porta uplink).

Configuração do isolamento de portas da ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu_id	Obrigatório
Adicionar o grupo de isolamento de portas	**onu-port-isolation** {all | ethernet port_id}	É possível adicionar múltiplas portas de no grupo de isolamento no mesmo comando
Visualização do grupo de isolamento de portas	**show onu-port-isolation**	Opcional

Exemplo de isolamento de portas

» Configure o isolamento de portas da ONU:
OLT4840E(onu-0/1/1)#onu-port-isolation ethernet 0/1 ethernet 0/4

» Exiba as configurações de isolamento de portas da ONU.
OLT4840E(onu-0/1/1)#show onu-port-isolation

ONU 0/1/1

onu isolation port :e0/1,e0/4.

9.8. ONU-Multicast

Modo de IGMP distribuido

Visão geral do modo de IGMP distribuido

O modo distribuído *IGMP* refere-se à utilização do IGMP-Snooping para alcançar o gerenciamento em membros do grupo multicast pela ONU. É usado principalmente para a entrada/saída dinâmica e manutenção dos membros do grupo através das mensagens IGMP Report / Leave e IGMP Query. O sistema EPON controla as permissões de usuário simples através da VLAN multicast da porta Ethernet.

Processo de implementação do modo IGMP distribuído

A ONU monitora o modo como o terminal do aplicativo (como um set-top box) encaminha as mensagens IGMP para o roteador multicast para formar uma relação de mapeamento entre os membros do grupo e as interfaces do switch. A ONU encaminha o pacote multicast de downlink recebido com o membro do grupo, de acordo com a tabela de encaminhamento multicast. Ela controla os direitos de acesso multicast de cada porta Ethernet com base em cada porta da VLAN multicast.

Se o IGMP-Snooping ou IGMP proxy estiver habilitado no OLT, ele intercepta todas as solicitações IGMP encaminhadas e as envia para o roteador de multicast de camada superior, configurando a associação entre o membro do grupo e a interface PON (ele também é uma tabela de encaminhamento multicast). O OLT encaminha o pacote multicast para cada interface PON de acordo com a tabela de encaminhamento.

Multicast controlável

Visão geral de multicast controlável

A idéia central do multicast dinâmico controlável é que o OLT execute a autenticação de usuário com base nas informações de identificação carregadas na mensagem IGMP e ajuste a ONU para controlar o encaminhamento dos pacotes multicast, estendendo a mensagem OAM. Os principais princípios são os seguintes:

» O OLT mantém uma tabela de controle de privilégios de usuários para gerenciar de forma centralizada o acesso ao serviço de multicast. O OLT usa o LLID do usuário e a ID da VLAN carregada para identificar a porta (do usuário) e determinar se ela possui o direito de acesso e os parâmetros do serviço multicast solicitado com base na tabela. Ele distribui a permissão de acesso da porta para a ONU através do pacote OAM de controle de multicast estendido, e ela executa o encaminhamento ou o desligamento do fluxo de serviço na porta. O OLT é o principal ente do gerenciamento de direitos de multicast e a ONU é o executor deste gerenciamento de direitos de multicast.

» A ONU mantém uma tabela de encaminhamento de endereço multicast. Comparado com a tabela de controle multicast do OLT, esta tabela tem uma capacidade pequena. Ela só processa a função de controle de fluxo do serviço multicast atual e se atualiza dinamicamente de acordo com o atributo Multicast Control emitido pelo OLT. A ONU transmite de forma transparente o pacote IGMP Report / Leave para o OLT com a etiqueta VLAN da porta (usuário). Ela recebe os pacotes OAM de controle de multicast estendido (incluindo uma série de entradas de controle de multicast) encaminhadas pelo OLT e adiciona ou elimina as entradas de encaminhamento de endereço de grupo local e encaminhamento multicast de acordo com os pacotes, executando o encaminhamento e o desligamento no fluxo de serviço multicast correspondente.

Processo de implementação do multicast controlável

Quando um terminal de aplicação multicast (como um set-top box) solicita um canal multicast específico (por exemplo, o endereço IP XX.XX.XX.XX), ele encaminhará uma mensagem de Report IGMP para o uplink. Este pacote entra na interface de usuário Ethernet da ONU, que adiciona a etiqueta VLAN à mensagem. Esta VLAN tem um valor TPID de 0×8100, um valor CFI de 0 e um valor Pri de 0. O VID é o número da porta Ethernet que recebeu o pacote de controle IGMP. Se uma mensagem do Relatório IGMP já possui uma marca VLAN, o VID é substituído pela etiqueta VLAN que identifica a porta do usuário. Então, a ONU transmite mensagens de relatório IGMP para o OLT, ele consulta os direitos de acesso e os parâmetros da porta (usuário) para o canal de acordo com a identificação da porta (usuário), o endereço IP multicast e o endereço IP da fonte do pacote Report (Somente para IGMP V3, opcional). De acordo com os diferentes direitos de acesso dos usuários, o sistema EPON pode ser dividido nos seguintes processos:

» Quando a porta (usuário) tem acesso ao canal como "permitir", o OLT usa um pacote OAM de controle multicast estendido para notificar a ONU para adicionar uma entrada de encaminhamento multicast. Ela indica que a porta do usuário tem permissão para acessar o canal. A ONU estabelece uma tabela de encaminhamento multicast local com base nos pacotes de OAM recebidos e encaminha o fluxo de serviço de dados multicast do canal para a porta de usuário correspondente.

» Quando a tabela de consulta OLT exibe que o acesso do usuário ao canal é "proibido", o OLT e a ONU não realizam nenhuma ação. Quando um terminal de aplicação multicast não recebe mensagens IGMP e tráfego multicast por um determinado período de tempo, a aplicação é encerrada.

» Quando a tabela de consulta OLT exibe que o acesso do usuário ao canal é "preview", o OLT notifica a ONU para adicionar um item de tabela de encaminhamento multicast (temporário) através de um pacote OAM de multicast estendida. Ao mesmo tempo, ele inicia um temporizador ou um contador, usado para controlar a duração da visualização, o número de pré-visualização, o intervalo de pré-visualização e outros parâmetros.

Configuração básica de ONU-IGMP-Snooping

Visão geral da configuração de ONU-IGMP-Snooping

Configuração de task		Obrigatório / opcional	Detalhes de configuração
Configuração básica de ONU-IGMP-Snooping	Habilitar/desabilitar o onu-gmp-snooping	Obrigatório	1.3.2
Afinar e otimizar o ONU-IGMP-Snooping	Configuração da ONU-Multicast fast leave (saída rápida do multicast da ONU)	Opcional	1.3.3
	Configuração do número máximo de multicast na porta da ONU	Opcional	1.3.4
	Configuração da VLAN multicast para a porta da ONU	Opcional	1.3.5
	Configuração do modo de tag os pacotes multicast da porta da ONU	Opcional	1.3.6

Habilitar/desabilitar o ONU-IGMP-Snooping

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Habilitar o ONU-IGMP-Snooping	**onu-multicast mode onu-igmp-snooping**	Habilitado por padrão
Visualização do modo do multicast da ONU	**show onu-multicast mode**	Deve ser executado no modo de configuração da onu

Obs.: *no padrão CTC, o IGMP-Snooping multicast da ONU é habilitado e não há nenhum comando de fechamento direto. Só é possível mudar para o modo* Multicast, *ou seja, IGMP-Snooping ou multicast controlável.*

Por exemplo:

» Defina o modo de multicast da ONU como ONU-IGMP-Snooping:
OLT4840E (onu-0/4/1)#onu-multicast mode ONU-IGMP-Snooping

ONU-Multicast mode is already igmp-snooping

Configuração o ONU-Multicast fast leave saída rápida do multicast da ONU)

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	-
Habilitar o ONU-Multicast fast leave	**onu-multicast fastleave {enable|disable}**	Obrigatório
Visualização do ONU-Multicast fast leave	**show onu-multicast fastleave**	Deve ser executado no modo de configuração da ONU

Por exemplo:

» Habilitar o ONU-Multicast fast leave:
OLT4840E (onu-0/4/1)#onu-multicast fastleave enable

» Desabilitar o ONU-Multicast fast leave:
OLT4840E (onu-0/4/1)#onu-multicast fastleave disable

Configuração do número máximo de multicast na porta da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta da ONU	**interface ethernet** slot/port	Você deve acessar o modo de configuração da ONU antes de acessar este modo
Configuração do número máximo de multicast na porta da ONU	**onu-igmp-snooping group-number** group-num	Obrigatório
Visualização do número máximo de multicast na porta da ONU	**show onu-igmp-snooping**	Deve ser executado no modo de configuração da ONU

Por exemplo:

» Defina o número máximo de pacotes multicast na porta 1 da ONU 0/4/1 para 7

OLT4840E(config)#onu 0/4/1

OLT4840E(onu-0/4/1)#int ethernet 0/1

OLT4840E(onu-0/4/1-reth-0/1)#onu-igmp-snooping group-number 10

OLT4840E(onu-0/4/1-reth-0/1)#show onu-igmp-snooping

ONU 0/4/1 interface 1

Multicast Vlan : no vlan

Group Number : 10

Configuração da VLAN multicast da porta da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta da ONU	**interface ethernet** slot/port	Você deve acessar o modo de configuração da ONU antes de acessar este modo
Configuração da VLAN multicast de entrada da porta da ONU	**onu-igmp-snooping vlan** vlan-list	Obrigatório
Remover a VLAN multicast de entrada da porta da ONU	**no onu-igmp-snooping vlan {**<1-256> **|all}**	Opcional
Visualização da VLAN multicast de entrada da porta da ONU	**show onu-igmp-snooping**	Deve ser executado no modo de configuração da ONU

Obs.: » *A VLAN multicast não pode ser a mesma que a VLAN padrão da porta da ONU e não pode ser VLAN 1.*

» *Cada ONU suporta VLAN multicast de forma diferente e as entradas configuradas podem ser diferentes. Para detalhes, consulte a tabela da ONU. O número máximo de entradas configuradas é de até 64.*

Por exemplo:

» Configure a VLAN multicast para a porta 1 da porta ONU 0 / 4/1 para ser 10-16

OLT4840E(config)#onu 0/4/1

OLT4840E(onu-0/4/1)#int ethernet 0/1

OLT4840E(onu-0/4/1-reth-0/1)#onu-igmp-snooping vlan 10-16

OLT4840E(onu-0/4/1-reth-0/1)#show onu-igmp-snooping

ONU 0/4/1 interface 1

Multicast Vlan : 10-16

Group Number : 10

Configuração do modo de tag os pacotes multicast da porta da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Acesse o modo de configuração de porta da ONU	**interface ethernet** slot/port	Você deve acessar o modo de configuração da ONU antes de acessar este modo
Configuração do modo de tag os pacotes multicast da porta da ONU	**onu-multicast {tag|untag}**	Obrigatório
Visualização do modo de tag os pacotes multicast da porta da ONU	**show onu-multicast tag**	Deve ser executado no modo de configuração da ONU

Obs.: » *O padrão é Tagged e Tagged nos pacotes Multicast. Os pacotes de VLAN não multicast não são controlados.*

» *Os pacotes de VLAN não multicast são controlados no modo* Unicast.

Por exemplo:

» Configure o modo de tag multicast na porta 1 da porta ONU 0 / 4/1 para ser tag:

OLT4840E(config)#onu 0/4/1

OLT4840E(onu-0/4/1)#int ethernet 0/1

OLT4840E(onu-0/4/1-reth-0/1)#onu-multicast tag

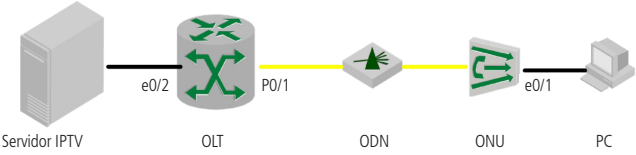
Exemplo de configuração do ONU-IGMP-Snooping

» Requisitos de rede:

» A rede é conforme:

O PC está conectado à porta e0/1 da ONU e o servidor multicast IPTV está conectado à porta OLT e0/2 e a ONU e0/1 é configurada com a VLAN 10 de multicast.

» **Requisitos de rede:** o PC usa o VLC para solicitar uma transmissão de um canal multicast. O endereço multicast correspondente é 224.1.1.1. O PC pode receber os pacotes de serviço multicast com o VLAN 10 do servidor multicast IPTV enquanto outros pacotes multicast não podem ser recebidos e o serviço unicast não pode ser afetado.



» Passos de configuração:
  » Configuração do OLT:
    » Crie a VLAN 10:
      OLT4840E (config)#vlan 10
    » Adicionar as portas e0/2 e p0/1 do OLT a VLAN 10:
      OLT4840E (config-if-vlan)#switchport ethernet 0/2
      OLT4840E (config-if-vlan)#switchport pon 0/1
    » Configure a porta p0/1 do OLT vlan 10 como atributo tag:
      OLT4840E (config)#interface pon 0/1
      OLT4840E (config-if-pon-0/1)#switchport hybrid tagged vlan 10
    » Configuração ONU (distribuída através do OLT), a ONU funciona no modo *Transparente*:
      OLT4840E (config)#onu 0/4/1
    » Configure a função de multidifusão da ONU no modo *Igobs-snooping*:
      OLT4840E (onu-0/4/1)#onu-multicast mode onu-igmp-snooping
    » Entre na porta ONU 1:
      OLT4840E (onu-0/4/1)#interface ethernet 0/1
    » Defina a VLAN multicast como sendo 10 na porta ONU 1:
      OLT4840E (onu-0/4/1-reth-0/1)#onu-igmp-snooping vlan 10
» Verificar resultados:
  » Exiba a VLAN multicast ONU:
    OLT4840E (config)#onu 0/4/1

OLT4840E (onu-0/4/1)#interface ethernet 0/1

OLT4840E (onu-0/4/1-reth-0/1)#show onu-igmp-snooping

ONU 0/4/1 interface 1

Multicast Vlan : 10 // A VLAN multicast é 10

Group Number :255

» A fonte de multicast IPTV encaminha pacotes de multicast com o VLAN 10, que o PC pode receber normalmente. O PC não pode receber os pacotes do serviço multicast com outras VLANs. O serviço unicast do PC não é afetado.

Configuração básica do ONU-Multicast-Ctrl

Visão geral da configuração básica do ONU-Multicast-Ctrl

Configuração de task		Obrigatório / opcional	Detalhes de configuração
Configuração básica de ONU-IGMP-Ctrl	Habilitar/desabilitar o ONU-GMP-Ctrl	Obrigatório	1.4.2
Afinar e otimizar o ONU-IGMP-Snooping	Configuração da ONU-Multicast fast leave (saída rápida do multicast da ONU)	Opcional	1.4.3
	Configuração do modo de tag os pacotes multicast da porta da ONU	Opcional	1.4.4
	Configuração da entrada controlada do multicast da ONU	Opcional	1.4.5
	Configuração do modelo de controle do multicast da ONU	Opcional	1.4.6
	Configuração dos parâmetros multicast controláveis	Opcional	1.4.7

Habilitar/desabilitar ONU-Multicast-Ctrl

Obs.: *o snooping IGMP deve ser ativado no OLT, porque o multicast controlável é controlado no OLT. Ative o IGMP-Snooping para habilitar o IGMP Report / Leave mensagens a serem processadas pela CPU OLT.*

Por exemplo:

EPON(onu-0/4/1)#onu-multicast mode onu-multicast-ctrl

Configuração do ONU-Multicast fast leave

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Habilitar o ONU-Multicast fast leave	**onu-multicast fastleave {enable|disable}**	Obrigatório
Visualização do ONU-Multicast fast leave	**show onu-multicast fastleave**	Deve ser executado no modo de configuração da ONU

Por exemplo:

» Habilitar o ONU-Multicast fast leave:

QptiWay (onu-0/4/1)#onu-multicast fastleave enable

» Desabilitar o ONU-Multicast fast leave:

OLT4840E (onu-0/4/1)#onu-multicast fastleave disable

Configuração do modo de tag dos pacotes multicast da porta da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	-
Acesse o modo de configuração de porta da ONU	**interface ethernet** slot/port	Você deve acessar o modo de configuração da ONU antes de acessar este modo
Configuração do modo de tag os pacotes multicast da porta da ONU	**onu-multicast {tag|untag}**	Obrigatório

Operação	Comando	Obrigatório/ opcional
Visualização do modo de tag os pacotes multicast da porta da ONU	**show onu-multicast tag**	Deve ser executado no modo de configuração da ONU

Obs.: *o padrão é Tagged e Tagged nos pacotes multicast. Os pacotes de VLAN não multicast não são controlados. Os pacotes de VLAN não multicast são controlados no modo* Unicast.

Configuração da entrada controlada do multicast da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Configuração da entrada controlada do multicast da ONU	**onu-multicast-ctrl {deny|permit|preview}** mac-address port-id vlan-id	Obrigatório
Remover o controle de entrada do multicast da ONU	**no onu-multicast-ctrl [mac** mac-address **|port-id** port-id **| vlan *vlan-id*]**	Opcional
Visualização do controle de entrada do multicast da ONU	**show onu-multicast-ctrl {interface |local-ctrl |}**	Deve ser executado no modo de configuração da ONU

Obs.: » *As entradas multicast controláveis têm três tipos de regras de autoridade, ou seja, proibir, permitir e visualizar. Quando configurado para ser proibido, o usuário não possui permissão para receber o pacote multicast. Se configurado para ser permitido, o usuário pode receber o fluxo multicast de forma contínua. Se configurado para ser pré-visualização, o usuário pode receber o fluxo multicast, mas o tempo de pré-visualização, o intervalo e o número de vezes são limitados.*

» *Quando a entrada controlável é excluída, a ordem de entrada de cada parâmetro não é restrita.*

Configuração dos parâmetros do multicast controlável

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do número máximo do multicast que pode ser controlado	**onu-multicast-ctrl channel-number** channel-num	Opcional, por padrão é *1024*
Configuração do tempo de envelhecimento do multicast controlável	**onu-multicast-ctrl live-time** live-time	Opcional, por padrão é *300s*
Configuração do número de pré-visualização de multicast	**onu-multicast-ctrl preview-times** preview-time	Opcional, por padrão é *5*
Configuração do intervalo de pré-visualização de multicast	**onu-multicast-ctrl time-interval** interval-time	Opcional, por padrão é *300s*
Configuração do tempo para uma pré-visualização de multicast	**onu-multicast-ctrl time-once** one-time	Opcional, por padrão é *180s*
Configuração do tempo de reposição da pré-visualização multicast	**onu-multicast-ctrl time-reset** reset-time	Opcional, por padrão é *3600s*
Restaurar os parâmetros padrão do multicast controlável	**no onu-multicast-ctrl {all |channel-number| live-time | preview-times | time-interval | time-once | time-reset }**	Opcional
Visualização dos parâmetros do multicast controlável	**show onu-multicast-ctrl**	Deve ser executado no modo *Global*

Por exemplo:

» Exiba os parâmetros de multicast controláveis:

QptiWay (config)#show onu-multicast-ctrl

the channel number at one time : 1024

the live time : 300(s)

preview time once : 180(s)

preview interval : 300(s)

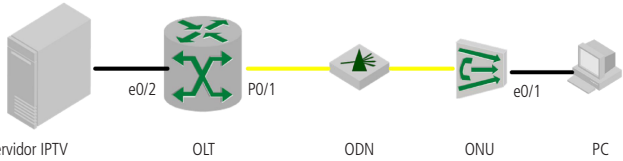
preview times : 5

preview reset : 3600(s)

Exemplo de configuração da ONU-Multicast-Ctrl

» Requisitos de rede:

O PC usa o VLC para solicitar uma transmissão de um canal. O endereço multicast correspondente é 224.1.1.2. O PC pode receber os pacotes de serviços multicast com o VLAN 100 do servidor dE IPTV enquanto outros pacotes multicast não podem ser recebidos e o serviço unicast não pode ser afetado.



» Etapas de configuração:

» Configuração OLT:

» Creat VLAN 10:

OLT4840E (config)#vlan 100

» Adicionar portas OLT e0 / 2 e p0 / 1 para VLAN 100

OLT4840E (config-if-vlan)#switchport ethernet 0/2

OLT4840E (config-if-vlan)#switchport pon 0/1

» # Configure OLT p0 / 1 port vlan 100 como o atributo tag

OLT4840E (config)#interface pon 0/1

OLT4840E (config-if-pon-0/1)#switchport hybrid tagged vlan 100

» # Configuração ONU (distribuída através do OLT), a ONU funciona em modo *Transparente*:

OLT4840E (config)#onu 0/4/1

» Configure a função de multidifusão da ONU no modo *Multicast-Ctrl*:

OLT4840E (onu-0/4/1)#onu-multicast mode onu-multicast-ctrl

OLT4840E(onu-0/4/1)#onu-multicast-ctrl permit 01:00:5e:01:01:02 0/1 100

» Verificação de resultados:

O testador encaminha uma mensagem de relatório multicast com o MAC de destino de 01:00:5e:01:01:02 para a porta ONU1. O OLT distribui uma tabela multicast controlável VLAN 100. Exibir as entradas controláveis no modo *ONU*.

OLT4840E(onu-0/4/1)#show onu-multicast-ctrl local-ctrl

Port MulticastMAC VLANID Type Online Channel Preview Profileflag

1 01:00:5e:01:01:02 100 permit Y 1 NULL 0

Total number of channels : 1 Total number of channels on-line : 1

O PC pode receber os pacotes de serviços multicast com o VLAN 100 e o MAC de destino como 01:00:5e:01:01:02 distribuídos pela fonte IPTV e os pacotes multicast de outras VLANs não podem ser recebidos.

9.9. Gerenciamento de atualização de ONU

Visão geral do gerenciamento de atualização de ONU

Para facilitar o gerenciamento de atualização remota do sistema da ONU, o OLT fornece o modo de atualização CTC. O arquivo de atualização é carregado no OLT e a operação de atualização é realizada no modo de configuração de ONU. Tanto o software da ONU e a atualização do firmware do chip podem ser completados simultaneamente. Seu firmware contém o arquivo de configuração e a validação CRC32.

A ONU suporta a função automática de reversão do processo de atualização, ou seja, quando uma falha da fonte de alimentação ou uma falha do link interrompem este processo e a ONU não funcionar normalmente, é possível reverter automaticamente para a versão original.

Atualização via CTC

Configuração da atualização via ONU-CTC

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Executar a atualização via CTC	**onu-ctc-upgrade**	Obrigatório
Confirmação da operação de atualização via CTC	**onu-ctc-upgrade-commit**	Opcional
Visualização da versão da ONU	**show** onu-sn	Opcional

Exemplo de atualização via ONU-CTC

A ONU 0/4/2 é atualizada de B01D004P1 para B01D004P2 por CTC.

» Carregue o arquivo de atualização da ONU B01D004P2 para o OLT:
OLT4840E#load onu-image tftp 1.1.1.1 4P2.mif
Downloading application via TFTP...
Download application via TFTP successfully.

» Verifique a versão ONU e execute a atualização:
OLT4840E(onu-0/4/2)#show onu-sn
Vendor ID : EPON
MODEL : 2400
ONUID(MAC) : 00:0a:5a:00:01:01
HW : V3.0
SW : B01D004P1
OLT4840E(onu-0/4/2)#onu-ctc-upgrade
CTC ONU(0/4/2) upgrade start ... WAIT PLEASE...
CTC ONU(0/4/2) upgrade complete.
CTC upgrade OK,please COMMIT after onu reboot!

» Confirmação da atualização. Se a atualização não for realizada, a ONU voltará a B01D004P1 após a reinicialização:
OLT4840E(onu-0/4/2)#onu-ctc-upgrade-commit
Commit image request/response successful

» Exibir a versão da ONU e deve mostrar que foi atualizada para o B01D004P2 com sucesso.
OLT4840E(onu-0/4/2)#show onu-sn
Vendor ID : EPON
MODEL : 2400
ONUID(MAC) : 00:0a:5a:00:01:01
HW : V3.0
SW : B01D004P2

9.10. Reinicialização da ONU

Visão geral da reinicialização da ONU

A função de reiniciar da ONU permite que você reinicie remotamente um dispositivo ONU sem ter que se deslocar para o ponto onde ela está.

Configuração da reinicialização da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Reinicializar a ONU	**onu-reboot**	Obrigatório

Exemplo de aplicação da reinicialização da ONU

» Reinicie a ONU 0/4/2:

OLT4840E(onu-0/4/2)#onu-reboot

Are you sure you want to proceed with the system reboot(y/n)?[n]y

OLT4840E(onu-0/4/2)#

2016/11/07 17:58:13

EVENT (onu status): Dereg 0/4/2 mac 00:0a:5a:00:01:01 reason: ONU TIMEOUT, type

1G/1G

Timeout: command_type 3; leaf ff; llid 0.

2016/11/07 17:58:21

EVENT (onu status): Reg 0/4/2 mac 00:0a:5a:00:01:01 reason: Auth passed, type 1G/1G

» Exiba o estatus de registro da ONU

OLT4840E(config)#show pon

ONU Mac Address LLID RTT REG-TYPE ONU-TYPE Description

0/4/1 00:0a:5a:ff:ff:69 0000 14 1G/1G other

0/4/2 00:0a:5a:00:01:01 0001 14 1G/1G 2400

Total onu entries: 2 .

9.11. Descrição do sistema da ONU

Visão geral da descrição do sistema da ONU

O papel principal da descrição do sistema da ONU é distinguir as ONUs de diferentes fabricantes ou identificar uma ONU. Uma vez que o usuário downstream está anormal, é possível localizar e analisar uma ONU específica rapidamente.

Configuração da descrição do sistema da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Descrição do sistema da ONU	**onu-description** onu-name	Obrigatório
Visualização da descrição do sistema da ONU	**show onu-description**	Opcional
Visualização das ONUs conectadas	**show pon**	Opcional

Exemplo de aplicação da descrição do sistema da ONU

Por exemplo:

» Configure a descrição da ONU 0/4/1 como intelbras:
OLT4840E(onu-0/4/1)#onu-description intelbras

» Exiba a descrição da ONU 0/4/1!
OLT4840E(onu-0/4/1)#show onu-description
The name of ONU 0/4/1: intelbras

OLT4840E(config)#show pon
ONU Mac Address LLID RTT REG-TYPE ONU-TYPE Description
0/4/1 00:0a:5a:ff:ff:69 0000 14 1G/1G other intelbras
0/4/2 00:0a:5a:00:01:01 0001 14 1G/1G 2400
Total onu entries: 2 .

9.12. Detecção de loop remoto de ONU

Visão geral da função da detecção de loop remoto de ONU

A ONU deve suportar a função de detecção de loop da porta Ethernet e da porta DSL. Além disso, ao detectá-lo, ela deve desativar a porta e, em seguida, disparar o alarme.

A interface Ethernet e a interface VDSL2 conectada à ONU devem ser capazes de suportar o protocolo Rapid Spanning Tree Protocol (RSTP) que atenda ao IEEE 802.1D.

Visão geral da configuração de detecção de loop remoto da ONU

Configuração de Task		Obrigatório / opcional	Detalhes de configuração
Configurações básicas da detecção de loop remoto da ONU	Detecção de loop remoto da ONU	Opcional	1.3
	Função de spanning tree da ONU	Opcional	1.4

Detecção de loop remoto da ONU

Configuração da detecção de loop remoto da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu-id	Obrigatório
Habilitar a detecção de loop da ONU	**onu-spanning-tree remote-loop-detect**	Por padrão está habilitado
Desabilitar a detecção de loop da ONU	**no onu-spanning-tree remote-loop-detect**	Opcional
Visualização da detecção de loop da ONU	**show onu-spanning-tree remote-loop-detect**	Opcional

Exemplo de configuração da detecção de loop remoto da ONU

» Requisito de rede:

Explicação de rede ----- conecte uma ONU à OLT e, em seguida, use um cabo para fazer um loop e por último desabilite o Spanning Tree.

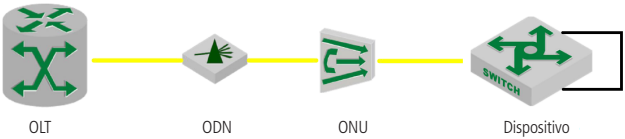


Diagrama esquemático da detecção de loop da ONU

» Passos de configuração:

» Acesse a ONU e habilite a detecção de loop remoto

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#onu-spanning-tree remote-loop-detect

» Verificação dos resultados:

» Depois que a detecção de loop remoto estiver ativada, os pacotes com o número de protocolo 0×5524 são enviados a cada 10 segundos.

Depois que a ONU detectar o loop, ele bloqueará a porta e imprimirá a mensagem de detecção de loop no OLT.

OLT4840E(onu-0/1/1)#

2016/11/10 09:34:33 EVENT (onu-port status): 0/1/2 Port 2 BLOCK_LOOP_DETECT

» Depois que o loop é removido, o status da porta da ONU é restaurado ao estad normal e a liberação do loop é impresso no prompt do OLT.

OLT4840E(onu-0/1/1)#

2016/11/10 09:35:18 EVENT (onu-port status): 0/1/2 Port 2 BLOCK_LOOP_CLEAR

Função de spanning tree da ONU

Configuração da função do spanning tree da ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** onu-id	Obrigatório

Operação	Comando	Obrigatório/ opcional
Habilitar o spanning tree da ONU	**onu-spanning-tree**	Para habilitar esta função, a detecção de loop da ONU deve estar desativada. Você deve escolher uma das duas funções e não poderá utilizar as duas ao mesmo tempo.
Desabilitar o spanning tree da ONU	**no onu-spanning-tree**	Opcional
Configuração do atraso de encaminhamento do spanning tree da ONU	**onu-spanning-tree forward-time** time	Opcional
Configuração do intervalo para a mensagem Hello do spanning tree da ONU	**onu-spanning-tree hello-time** time	Opcional
Configuração do tempo de envelhecimento do spanning tree da ONU	**onu-spanning-tree maxage** time	Opcional
Configuração da prioridade do spanning tree da ONU	**onu-spanning-tree priority** priority	Opcional
Visualização da configuração de spanning tree da ONU	**show onu-spanning-tree**	Opcional

Obs.: » *Ao configurar Forward Delay / Hello Time / Max Age, eles devem atender a essa expressão relacional:*

» *2 * (Forward Delay -1)> = Max Age> = 2 * (Hello Time + 1).*

Exemplo de configuração do spanning tree da ONU

» Requisito de rede:

Explicação de rede ----- conectando um switch na porta 2 e na porta 3 da ONU para fazer com que ele formasse um loop.

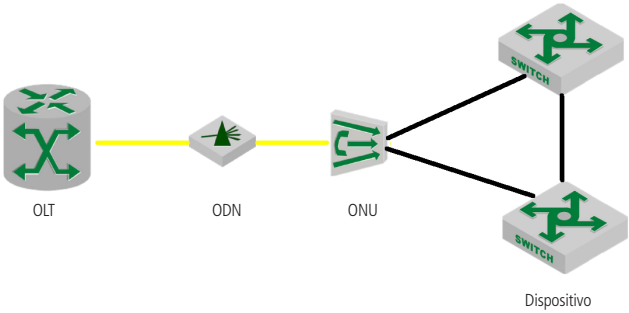


Diagrama esquemático da função de spanning tree da ONU

» Passos de configuração:

» Acesse a ONU e habilite a função de spanning tree:

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#onu-spanning-tree

Tanto o dispositivo 1 como o dispositivo 2 devem habilitar o RSTP. Além disso, configure a prioridade da bridge para tornar o dispositivo 1 como Bridge Root, o dispositivo 2 ocupando o segundo lugar e a prioridade da bridge da ONU para ser a mais baixa.

» 3. Verificação de resultados:

» A porta 2 da ONU sendo selecionada como porta root, a porta 3 é selecionada como a porta alternativa sendo bloqueada e as informações do loop detectado são impressas no prompt do OLT.

OLT4840E(onu-0/1/1)# 2016/11/10 10:49:24 EVENT (onu-port status): 0/1/1 Port 3

BLOCK_LOOP_DETECTED

» Depois de desconectar o cabo de rede entre a ONU e o Dispositivo 2, exibirá a informação de liberação do loop no OLT.

OLT4840E(onu-0/1/1)#2016/11/10 10:51:08 EVENT (onu-port status): 0/1/1 Port 3

BLOCK_LOOP_CLEAR

9.13. PSG

Visão geral da função *PSG*

Existem várias ONUs que compartilham uma largura de banda óptica no sistema EPON, por isso é necessário fornecer arquitetura de proteção para garantir sua comunicação e evitar perda de tráfego.

O PSG é uma sigla para o Grupo de Comutação de Proteção (protection switching group). É constituído por um par de fibras ópticas, adotando divisor ótico 2: N. Um dos links deve ser configurado como mestre, e o outro como backup. O fluxo de tráfego normal é transmitido pelo link óptico mestre, se a interrupção ocorrer, ele será transferido para o link óptico de backup.

Existem dois tipos de troca de link:

» **Troca automática:** causada por descoberta de falhas, por exemplo, LOS (perda de sinal) ou sinal degradado.

» **Troca forçada:** causado por um evento gerencial.

Tipos de troca de link óptico

A função de troca do OLT está em conformidade com o tipo A do padrão CTC3.0 de telecomunicações, ou seja, duas portas PON do OLT adotam um chipset PON MAC para realizar a proteção através de um link de chave elétrica 1: 2 que se conecta a dois módulos ópticos.

As informações de serviço da porta principal do OLT podem ser sincronizada com a porta de backup, para garantir que o serviço ONU permaneça o mesmo durante a troca.

Critérios de troca de link óptico

No sistema EPON, as condições de disparo da troca incluem:

» Perda de sinal de entrada (LoS).

Isso pode ser devido a perda do sinal físico perdido ou não recebimento do relatório MPCPDU pela ONU.

» Canal de entrada degradado.
  » O sinal óptico de entrada é muito alto ou muito baixo.
  » Taxa de erro acima do limite.
» Falha de hardware do dispositivo.
  » Falha do módulo óptico.
» Mecanismo de troca (camada lógica):
  » Troca automática:

  Após o OLT detectar os eventos de falha do link, ele determinará se ela está no tronco ou no ramo da rede. Se for o primeiro caso, ele iniciará a proteção PON imediatamente. Se for o segundo caso, ele não iniciará a troca de PON.

» Troca forçada:

  Depois que o OLT receber o comando da troca forçada do gerente de rede, ele irá desativar imediatamente o módulo óptico da interface óptica mestre, habilitando o módulo óptico da interface óptica de backup, trocando o tráfego da ONU para a porta PON de backup.

Visão geral da configuração do *PSG*

Configuração de task		**Obrigatório / opcional**	**Detalhes de configuração**
Configurações básicas do PSG	Desabilitar uma porta PON	Obrigatório	1.5
	Estabelecer um grupo PSG	Obrigatório	1.6
	Habilitar o grupo PSG	Obrigatório	1.7
	Executar a troca manual da porta mestra para a porta backup no grupo PSG	Opcional	1.8

Desabilitar uma porta PON

Desabilitar uma porta PON

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	-
Desabilitar uma pota PON	**no admin-enable-pon** slot slot_id **pon** port_id	Obrigatório

Operação	Comando	Obrigatório/ opcional
Habilitar uma pota PON	**admin-enable-pon slot** slot_id **pon** port_id	Por padrão está habilitado
Visualização das porta habilitadas	**show admin-enable-pon slot** slot_id	Opcional

Obs.: » *Somente quando a porta PON está desativada, você pode estabelecer o grupo PSG.*

» *Se você estiver usando essa abordagem para desativar a porta PON, você pode desabilitar a porta PON em vez da porta NNI.*

Exemplo para desabilitar uma porta PON

» Desabilite a porta PON 1 e a porta PON 3 do slot 4:

OLT4840E(config)#no admin-enable-pon slot 0 pon 3

OLT4840E(config)#no admin-enable-pon slot 0 pon 4

» Exiba o estado das portas PON do slot 4:

OLT4840E(config)#show admin-enable-pon slot 0

PON port administrative status

pon 0/1: admin-up

pon 0/2: admin-up

pon 0/3: admin-down

pon 0/4: admin-down

Estabelecer um grupo PSG

Estabelecer um grupo PSG

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Estabelecer um grupo PSG	**psg creat slot** slot_id **psg-id** psg-id **active-pon** pon-id **standby-pon** pon-id	Obrigatório
Remover um grupo PSG	**psg delete slot** slot_id **psg-id** psg-id	Opcional
Visualização das informações do grupo PSG	**show psg slot** slot_id	Opcional

Exemplo de configuração para estabelecer um grupo PSG

» O slot # OLT 4 cria o grupo PSG 1, com a porta PON 1 para ser a porta mestre e a porta PON 3 para ser a porta backup.

OLT4840E(config)#psg creat slot 0 psg-id 1 active-pon 3 standby-pon 4

#Exiba as informações do grupo PSG

OLT4840E(config)#show psg slot 0

psg id active pon standby pon administrative status

1 pon-0/3 pon-0/4 admin-up

Troca manual entre portas mestre e backup do grupo PSG

Troca manual entre portas mestre e backup do grupo PSG

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Troca manual entre portas mestre e backup do grupo PSG	**psg switch slot** slot_id **psg-id** psg_id	Obrigatório

***Obs.:** a troca manual é igual a um comando de troca forçada, que irá mudar da porta mestre para a porta de backup. Naquele momento, o módulo óptico da interface será desabilitado imediatamente e, em seguida, habilitará o seu backup.*

Exemplo de troca manual entre portas mestre e backup do grupo PSG

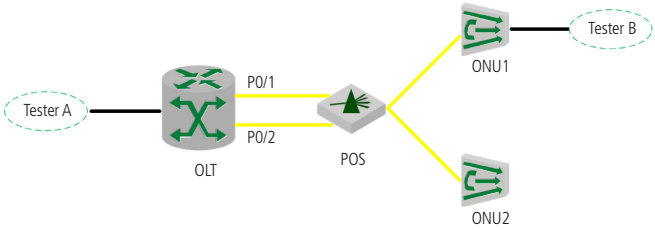
» Troque manualmente entre portas mestre e backup do grupo PSG 1 no slot 0:

OLT4840E(config)#psg switch slot 0 psg-id 1

Exemplo de configuração integrada do PSG

» Requisito de rede:

» **A rede é a seguinte:** o OLT se conecta com divisor óptico 2: N e múltiplas ONUs. Isso exige que, se houver algo errado em um link óptico de OLT PON, a porta ONU-PON pode ser alterada automaticamente para outra porta, e o serviço permanece o mesmo.



» Passos de configuração:
  » Disabilitar a porta PON:
    OLT4840E(config)#no admin-enable-pon slot 0 pon 1
    OLT4840E(config)#no admin-enable-pon slot 0 pon 2
  » Estabelecer um grupo PSG:
    OLT4840E(config)#psg creat slot 0 psg-id 1 active-pon 1 standby-pon 2
» Passos de teste:
  » Insira a fibra óptica da porta PON mestre para deixar a ONU on-line primeiro e, em seguida, insira a fibra óptica da porta PON de backup para verificar o estado das informações de logon da ONU e as informações de configuração da ONU.
  » A porta A e a porta B do testador com a porta da ONU e a porta OLT GE, respectivamente, e, em seguida, enviam o unicast conhecido para o outro; desconecte a fibra óptica da porta PON mestre para verificar a informação de logon da ONU e as informações de encaminhamento de pacotes.
» Verificação de resultados:
  » Registro da ONU como a porta PON mestre, ONU-ID é o ID da porta PON Mestre:
    OLT4840E(config)#show running-config onumnt
    ![ONUMNT]
    onu 0/1/1
    onu-binding mac 00:0a:5a:ff:ff:69
    onu-binding type other
    onu-description aa
    onu-port-isolation ethernet 0/1 ethernet 0/4

```
no onu-spanning-tree remote-loop-detect
onu-spanning-tree
interface pon 0/0
exit
interface ethernet 0/1
onu-bandwidth ingress cir 100 cbs 1600 ebs 2
onu-bandwidth egress cir 100 pir 300
exit
interface ethernet 0/2
exit
interface ethernet 0/3
exit
interface ethernet 0/4
exit
onu 0/3/2
onu-binding mac 00:0a:5a:00:01:01
onu-binding type 2400
onu-description weerv
onu-port-isolation ethernet 0/1 to ethernet 0/4
interface pon 0/0
exit
interface ethernet 0/1
exit
interface ethernet 0/2
exit
interface ethernet 0/3
exit
interface ethernet 0/4
exit
```

» Depois de desconectar a fibra óptica da porta Mestre PON, não ocorre o prompt off da ONU. Ao verificar a informação de logon da ONU, mostra que ONU-ID foi alterada para ser a identificação da porta PON de backup e o número de série do ONU-Index permanece o mesmo. Além disso, o envio e o envio de pacotes do testador não apresentam interrupção.

```
OLT4840E(config)#show running-config onumnt
![ONUMNT]
onu 0/2/1
onu-binding mac 00:0a:5a:ff:ff:69
onu-binding type other
onu-description aa
onu-port-isolation ethernet 0/1 ethernet 0/4
no onu-spanning-tree remote-loop-detect
onu-spanning-tree
interface pon 0/0
exit
interface ethernet 0/1
onu-bandwidth ingress cir 100 cbs 1600 ebs 2
onu-bandwidth egress cir 100 pir 300
exit
interface ethernet 0/2
exit
interface ethernet 0/3
exit
interface ethernet 0/4
exit
onu 0/4/2
onu-binding mac 00:0a:5a:00:01:01
onu-binding type 2400
onu-description weerv
onu-port-isolation ethernet 0/1 to ethernet 0/4
```

interface pon 0/0

exit

interface ethernet 0/1

exit

interface ethernet 0/2

exit

interface ethernet 0/3

exit

interface ethernet 0/4

exit

9.14. FEC

Visão geral de FEC

FEC é a sigla de Forward Error Correction (Encaminhamento de correção de erro), usando o byte de paridade para substituir uma parte do espaço entre pacotes com base na estrutura original do quadro, de modo a verificar os dados. O equipamento suporta a correção de erro de duas vias, ou seja, o equipamento da nossa empresa suporta na porta PON e na ONU, abrindo essa função.

Esta função pode efetivamente reduzir a taxa de erro de bits para satisfazer os requisitos do sistema de comunicação de fibra óptica de alto desempenho; ela pode reduzir o orçamento de energia de emissão laser e seu consumo de modo a aumentar a distância de transmissão máxima de sinais ópticos; existem também algumas deficiências da FEC, por exemplo, ela aumentará os custos, a complexidade do sistema e assim por diante. No entanto, no ponto de vista geral as vantagens da FEC superam em muito as suas desvantagens.

Habilitar/desabilitar o FEC na ONU

Habilitar/desabilitar o FEC na ONU

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório

Operação	Comando	Obrigatório/ opcional
Acesse o modo de interface PON	**onu** onu_id	Obrigatório
Habilitar o FEC na interface PON	**onu-fec mode enable**	Obrigatório
Desabilitar o FEC na interface PON	**onu-fec mode disable**	Opcional, por padrão está desabilitado
Visualização do estado do FEC na ONU	**show onu-fec**	Opcional, funciona apenas no modo de ONU

Exemplo de configuração do FEC na ONU:

» Requisitos de rede:

Registre ONU para OLT, então conecte a porta A e a porta B do testador à porta da ONU e à porta OLT GE. Habilite a função *FEC* da porta PON e em seguida a porta A e a porta B enviarão 100M de áudio unidos entre si. Em seguida, preste atenção aos pacotes que serão transmitidos.

» Rede será a seguinte:

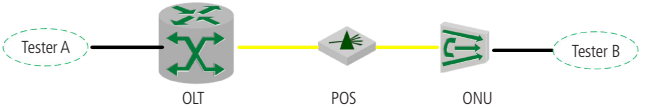


Diagrama esquemático para o FEC na ONU

» Etapas de configuração:

» Entre no modo de configuração da ONU e habilite o FEC.

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#onu-fec mode enable

» Verificação do resultado:

A velocidade de recepção da porta A permanece igual à anterior e a velocidade de recepção da porta B diminui pelo menos 30%.

9.15. Detecção dos parâmetros ópticos da ONU

Visão geral da detecção dos parâmetros ópticos da ONU

A ONU deve ser capaz de suportar a função de detecção de parâmetros do transceiver óptico com base no SFF-8472 / SFF-8077i, incluindo temperatura operacional, tensão de alimentação, corrente de polarização, potência transmitida, potência recebida e assim por diante. Além disso, ela deve ser capaz de suportar a calibração interna do valor de detecção dos indicadores acima (não requer módulo óptico para suportar a calibração interna do valor de detecção de indicadores, pois a ONU pode realizar a calibração interna do valor de detecção de indicadores no módulo óptico).

Os requisitos para a função de detecção de parâmetros da ONU do transceptor óptico são os seguintes:

- **Temperatura de operação do módulo óptico:** apresentada por 16 dígitos binários com os caracteres, e a unidade será 1/256 °C. Isso significa que o intervalo de valores é de -128 °C a + 128 °C, e a precisão da medição deve estar na faixa de ± 3 °C. A temperatura de funcionamento do módulo óptico deve estar em conformidade com as Tabelas 3.13 e Tabelas 3.14 no SFF-8472 Draft 10Dot3 Dec. 2007.
- **Tensão de alimentação do módulo óptico:** apresentada por inteiro 16 dígitos, e a unidade será 100MV. Isso significa que o intervalo de valores é de 0 a 6,55 V, e a precisão da medição deve estar na faixa de ± 3%. Este parâmetro refere-se à tensão de alimentação do transmissor óptico.
- **Corrente de polarização do transmissor óptico:** apresenta 16 dígitos inteiros e a unidade de 2μA. Isso significa que o intervalo de valores é de 0 mA a 131 mA, e a precisão da medição deve estar na faixa de ± 10%.
- **Potência transmitida do transmissor óptico:** apresentada por um número inteiro de 16 dígitos e a unidade de 0.1 uW. Isso significa que o intervalo de valores é de 0 mW a 6.5535 mW (-40 dBm ~ + 8.2 dBm ou mais), e a precisão da medição deve estar na faixa de ± 3dB.
- **Potência recebida do transceptor óptico:** refere-se à potência óptica média recebida pela ONU, apresentada por um número inteiro de 16 dígitos e a unidade de 0.1 uW. Isso significa que o intervalo de valores é de 0 mW a 6.5535 mW (-40 dBm ~ + 8.2 dBm ou mais), e a precisão da medição deve estar na faixa de ±2 dB e varia de -30 dBm a 10 dBm.

Quando um parâmetro ou vários parâmetros do transceptor óptico da ONU são muito baixos ou muito altos (tomando o limite configurado como referência), a ONU enviará o Alarme ou o Aviso correspondente através do Event Notification (notificação de evento). Os tipos de alarme e aviso incluem TempHighAlarm, TempLowAlarm, VccHighAlarm, VccLowAlarm, TXBiasHighAlarm, TXBiasLowAlarm, TXPowerHighAlarm, TXPowerLowAlarm, RXPowerHighAlarm, RXPowerLowAlarm, TempHighWarning, TempLowWarning, VccHighWarning, VccLowWarning, TXBiasHighWarning, TXBiasLowWarning, TXPowerHighWarning, TXPowerLowWarning, RXPowerHighWarning, RXPowerLowWarning.

Visão geral da configuração da detecção dos parâmetros ópticos da ONU

Visão geral da configuração da detecção dos parâmetros ópticos da ONU

Configuração de task		Obrigatório / opcional	Detalhes de configuração
Configuração básica da detecção de parâmetros ópticos da ONU	Visualização dos parâmetros ópticos da ONU	Opcional	2.3
	Alarmes para os parâmetros ópticos da ONU	Opcional	2.4

Visualização dos parâmetros ópticos da ONU

Visualização dos parâmetros ópticos da ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de ONU	**onu** slot/port	Obrigatório
Visualização dos parâmetros ópticos interface PON	**show onu-opm-diagnosis**	Opcional

Exemplo de visualização dos parâmetros ópticos da ONU

» Exiba os parâmetros ópticos da onu-0/4/1:

OLT4840E(config)#onu 0/4/1

OLT4840E(onu-0/4/1)#show onu-opm-diagnosis

ONU: 0/4/1

Optical Transceiver Diagnosis :

Work Temperature : 38.25 C

Supply Voltage(Vcc) : 3.29 V

TX Bias Current : 16.99 mA

TX Power(Output) : 1.445 mW (3.00 dBm)

RX Power(Input) : 0.573 mW (-2.40 dBm)

Alarmes para os parâmetros ópticos da ONU

Configuração de alarmes dos parâmetros ópticos da ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Configuração do tempo de verificação dos alarmes de parâmetros ópticos	**onu-opm-alarm-interval** time	Opcional
Acesso ao modo de configuração de ONU	**onu** slot/pon/onu	Obrigatório
(Des)Habilitar alarmes de parâmetros ópticos	**onu-opm-alarm** enable/disable	Desabilitado por padrão
Configuração do alarme de corrente máxima de polarização	**onu-opm-threshold bias-high-alarm** current	Opcional
Configuração do alerta de corrente máxima de polarização	**onu-opm-threshold bias-high-warning** current	Opcional
Configuração do alarme de corrente mínima de polarização	**onu-opm-threshold** bias-low-alarm *current*	Opcional
Configuração do alerta de corrente mínima de polarização	**onu-opm-threshold bias-low-warning** current	Opcional

Operação	Comando	Obrigatório / opcional
Configuração do alarme de potência máxima de recebimento	**onu-opm-threshold rx-high-alarm** optical_power	Opcional
Configuração do alerta de potência máxima de recebimento	**onu-opm-threshold rx-high-warning** optical_power	Opcional
Configuração do alarme de potência mínima de recebimento	**onu-opm-threshold rx-low-alarm** optical_power	Opcional
Configuração do alerta de potência mínima de recebimento	**onu-opm-threshold rx-low-warning** optical_power	Opcional
Configuração do alarme de temperatura máxima	**onu-opm-threshold temp-high-alarm** temperature	Opcional
Configuração do alerta de temperatura máxima	**onu-opm-threshold temp-high-warning** temperature	Opcional
Configuração do alarme de temperatura mínima	**onu-opm-threshold temp-low-alarm** temperature	Opcional
Configuração do alerta de temperatura mínima	**onu-opm-threshold temp-low-warning** temperature	Opcional
Configuração do alarme de potência máxima de transmissão	**onu-opm-threshold tx-high-alarm** optical_power	Opcional
Configuração do alerta de potência máxima de transmissão	**onu-opm-threshold tx-high-warning** optical_power	Opcional
Configuração do alarme de potência mínima de transmissão	**onu-opm-threshold tx-low-alarm** optical_power	Opcional
Configuração do alerta de potência mínima de transmissão	**onu-opm-threshold tx-low-warning** optical_power	Opcional
Configuração do alarme de tensão máxima	**onu-opm-threshold voltage-high-alarm** voltage	Opcional
Configuração do alerta de tensão máxima	**onu-opm-threshold voltage-high-warning** voltage	Opcional
Configuração do alarme de tensão mínima	**onu-opm-threshold voltage-low-alarm** voltage	Opcional
Configuração do alerta de tensão mínima	**onu-opm-threshold voltage-low-warning** voltage	Opcional
Visualização dos parâmetros ópticos	**show onu-opm-threshold**	Opcional

Obs.: *ao configurar o parâmetro de alarme/alerta para a potência mínima de recebimento/transmissão, você deve configurar as opções de alerta antes de configurar as suas opções.*

Exemplo de alarmes de parâmetro óptico da ONU

» Requisitos de rede:

» **Explicação da rede:** defina o alarme de potência máxima de transmissão da ONU como sendo 1 dBm e o alerta de potência mínima recebida para -1 dBm.

Diagrama esquemático para a configuração de alarme do parâmetro óptico da ONU

» Passos de configuração:

Antes de ativar o alarme de parâmetro óptico, você deve configurar as opções de valores de limite relacionados.

OLT4840E (onu-0/4/1)#onu-opm-threshold tx-high-warning 1 rx-low-warning -1

OLT4840E (onu-0/4/1)#onu-opm-alarm enable

» Verifique o resultado:

Visualize o parâmetro óptico atual da ONU, todos os quais excederam o valor de limite configurado.

OLT4840E(onu-0/4/1)#show onu-opm-diagnosis

ONU: 0/4/1

» Optical Transceiver Diagnosis :

Work Temperature : 38.25 C

Supply Voltage(Vcc) : 3.29 V

TX Bias Current : 17.5 mA

TX Power(Output) : 1.449 mW (3.00 dBm)

RX Power(Input) : 0.549 mW (-2.60 dBm)

» Os alarmes serão exibidos a cada 10 segundos.

OLT4840E (onu-0/4/1)#

EVENT (onu opm alarm): on onu 0/4/1

TX Power High Warnning

RX Power Low Warnning

EVENT (onu opm alarm): on onu 0/4/1

TX Power High Warnning

RX Power Low Warnning

9.16. DBA

Visão geral do DBA

DBA (Alocação de largura de banda dinâmica): o OLT obtém as informações de trânsito de cada ONU de acordo com sua solicitação de largura de banda em tempo real, e aloca dinamicamente sua largura de banda de upstream através de um algoritmo específico para garantir que os quadros de dados não colidam um com o outro.

O sistema EPON controla a mensagem GATE e a mensagem REPORT através do MPCP, obtendo alocação dinâmica de largura de banda.

Visão geral da configuração de DBA

» Visão geral da configuração de DBA:

Configuração da atividade		Obrigatório/ opcional	Informação detalhada
Configurações básicas de DBA	Configuração da largura de banda de uplink	Opcional	1.3
	Configuração da largura de banda de downlink	Opcional	1.4

Obs.: *na configuração básica do DBA, a configuração de largura de banda de ligação de uplink significa configurar o valor de fir, cir e pir da largura de banda de upstream. A configuração de largura de banda de downlink significa configurar o valor de pir da largura de banda de downstream.*

Largura de banda de uplink

Configuração da largura de banda de uplink

» Configuração do modo sem autenticação:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**Configure terminal**	-
Acesse o modo de configuração da ONU	**Onu** slot/pon/onu	Obrigatório
Configuração da largura de banda de uplink	**Onu-bandwidth upstream**{fir|cir|pir } weight weight-id	Opcional
Visualização da largura de banda da uplink	**Show onu-bandwidth** upstream	Opcional

Obs.: *no modo de hardware com ajuste periódico dinâmico, o valor FIR deve ser 0 e o CIR total não pode ser superior a 955000. Os parâmetros devem estar em conformidade com: fir <= cir <= pir.*

Exemplo de configuração da largaura de banda de uplink

» Requisitos de rede:

Explicação da rede ----- A ONU regista no OLT, desabilita a transmissão, multicast e a supressão unicast desconhecida na porta OLT. Configure a largura de banda de uplink CIR da ONU para 100 e o PIR seja 1000.

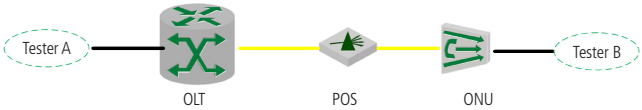


Diagrama de configuração para o modo sem autenticação

» Etapas de configuração:

» Configure a largura de banda de uplink de ONU 0/4/1:

OLT4840E(config)#onu 0/4/1

OLT4840E(onu-0/4/1)#onu-bandwidth upstream fir 0 cir 100 pir 1000 weight 10

Exiba a largura de banda de uplink de ONU 0/4/1:

OLT4840E(onu-0/4/1)#show onu-bandwidth upstream

ONU:0/4/1

upstream : fir= 0 cir=100 pir=1000 weight=10

» Verifique o resultado:

» O testador A envia pacotes unicast desconectados de velocidade de fio. O testador B pode receber pacotes com a taxa de 1000 ou mais, e a taxa real é de cerca de 5% com 1000. Comparada com a taxa real, a diferença é de cerca de 5%.

Largura de banda de downlink

Configuração da largura de banda de downlink

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Configuração da largura de banda de downlink	**onu-bandwidth downstream**{pir} burst burst-id	Opcional
Visualização da largura de banda da downlink	**show onu-bandwidth downstream**	Modo da ONU

Obs.: *no modo de hardware com ajuste periódico dinâmico, o PIR não pode ser superior a 1000000.*

Exemplo de configuração da largura de banda de downlink

» Requisitos de rede:

» Explicação da rede ----- A ONU registra o OLT e desabilita a supressão de unicast de transmissão, multicast e desconhecido na porta OLT. O valor PIR de downstream da ONU A é 4800.

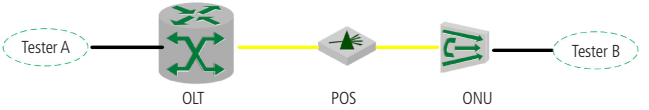


Diagrama de configuração da autenticação por MAC

» Etapas de configuração:
  » Configure a largura de banda de downlink de ONU 0/4/1:
    OLT4840E (config)#onu 0/4/1
    OLT4840E (onu-0/4/1)# onu-bandwidth downstream pir 4800 burst 130
  » Exiba a largura de banda de downlink de ONU 0/4/1:
    OLT4840E(onu-0/4/1)#show onu-bandwidth downstream
    downstream:
    onu-bandwidth: pir 4800 kbps burst 130
» Verifique o resultado:
» A porta do testador A transmite pacotes unicast conhecidos na velocidade do fio, e a porta do testador B recebe os pacotes com a taxa de 4800 ou mais.

9.17. ONU P2P

Visão geral de ONU P2P (ponto a ponto)

Você pode configurar as funções P2P da ONU para permitir que os usuários na mesma porta PON se comuniquem entre si.

Visão geral da configuração de ONU P2P

Visão geral da configuração de ONU P2P

Configuração de task		Obrigatório / opcional	Detalhes de configuração
Configuração básica para encaminhamento e controle da porta PON	ONU P2P	Opcional	1.3

ONU P2P

Configuração de ONU P2P

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da por PON	**interface pon** slot/port	Obrigatório
Habilite o ONU P2P	**onu-p2p**	Opcional

Operação	Comando	Obrigatório / opcional
Desabilite o ONU P2P	**no onu-p2p**	Opcional
Habilite a comunicação entre ONUs através de ONU P2P	**onu-p2p entry** rule-id **source-onu** onu-id **destination-onu** onu-id	Opcional
Desabilite a comunicação entre ONUs através de ONU P2P	**no onu-p2p entry** rule-id	Opcional
Visualização das configurações de ONU P2P	**show onu-p2p**	Opcional

Exemplo de configuração de ONU P2P

» Requisitos de rede:

Explicação da rede ----- Duas ONUs estão conectadas sob a mesma porta PON, ONU 1 conectada ao testador A e ONU 2 conectada ao testador B.

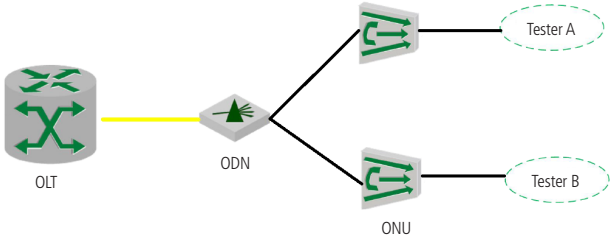


Diagrama de ONU P2P

» Passos de configuração:

» Habilite o ONU P2P para a porta PON 0/1

OLT4840E(config)#interface pon 0/1

OLT4840E(config-if-pon-0/1)# onu-p2p entry 1 source-onu 1 destination-onu 2

» Verifique o resultado:

  » Quando o ONU-P2P está habilitado, o testador A e B podem trocar pacotes.

  » Quando o ONU-P2P está desativado, o testador A e B não podem trocar pacotes.

9.18. Limite de MAC na ONU

Visão geral do limite de MAC

Você pode configurar o limite de MAC da ONU, de modo que o ONU possa limitar o número de MACs aprendidos.

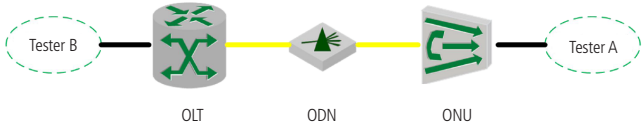
Configuração de limite de MAC na ONU

Operação	Comando	Obrigatório / opcional
Acesso o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração da ONU	**onu** slot/pon/onu	Obrigatório
Configuração global de limite de MAC em ONUs	**onu-mac-address-table max-mac-count** number	Opcional
Remover a configuração global de limite de MAC em ONUs	**no onu-mac-address-table max-mac-count** number	Opcional
Acesso o modo de configuração de portas da ONU	**interface ethernet** slot/port	Obrigatório
Configuração de limite de MAC na porta da ONU	**onu-mac-address-table max-mac-count** number	Opcional
Remover a configuração de limite de MAC na porta da ONUs	**no onu-mac-address-table max-mac-count** number	Opcional
Visualização das configurações de limite de MAC	**show onu-mac-address-table** max-mac-count	Opcional

Exemplo de configuração de limite de MAC em ONUs

» Requisitos de rede:

Explicação de rede ----- Conecte o testador a uma extremidade de OLT e ONU



Limite de aprendizagem do endereço MAC na ONU

» Passos de configuração:

» Defina o limite de aprendizagem do endereço MAC para 10 na ONU-0/1/1

OLT4840E(config)#onu 0/1/1

OLT4840E(onu-0/1/1)#onu-mac-address-table max-mac-count 10

» Verifique o resultado:

» O testador A envia pacotes de unicast Layer-2 com 20 endereços MAC de origem (aumento progressivo) começando em 00:00:00:00:01.

» Então, você pode visualizar as entradas de endereço MAC no OLT. Ele deve aprender apenas 10 endereços MAC começando com 00:00:00:00:01.

10. Configuração ARP

10.1. Visão geral do ARP

Função *ARP*

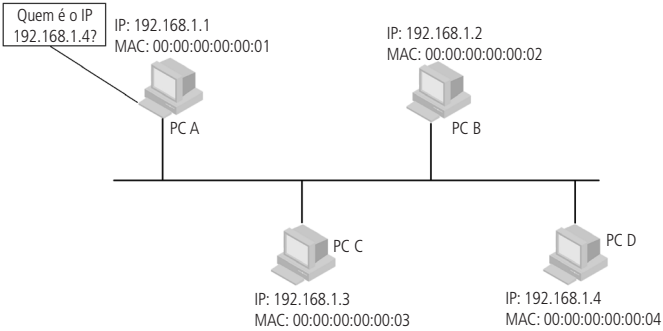
ARP, Address Resolution Protocol é um dos protocolos mais importantes na família TCP/IP. Um endereço IP é o endereço de um host na camada de rede. Para enviar um pacote de camada de rede para um host de destino, o dispositivo deve conhecer o endereço da camada de link de dados (como o endereço MAC) do host de destino. Para este fim, o endereço IP deve ser resolvido no endereço correspondente da camada do link de dados.

Os endereços de camada de link de dados que aparecem neste capítulo referem-se aos endereços MAC Ethernet de 48 bits.

Processo de funcionamento do ARP

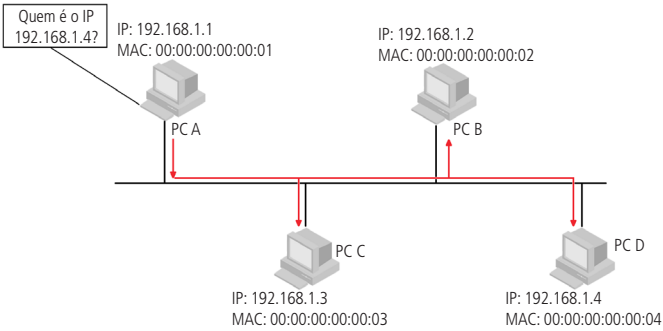
Tome a comunicação FTP, por exemplo, para descrever o processo operacional do ARP.

Conforme exibido a seguir, o host *A* espera acessar o host com o endereço IP *192.168.1.4*.



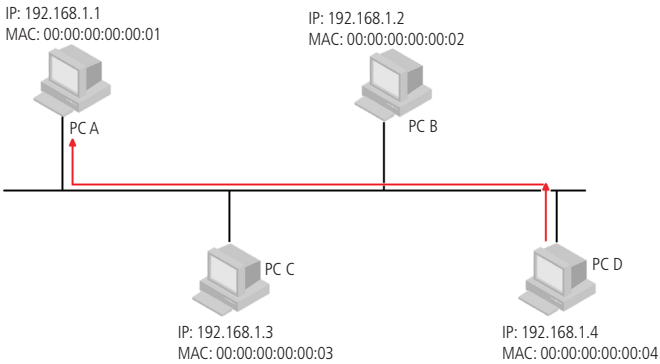
Suponha que esta seja uma rede Ethernet, e cada host não conhece outro host na rede de área local (LAN). Neste caso, o host deve conhecer o endereço MAC do host *192.168.1.4* antes de estabelecer a comunicação.

De acordo com o protocolo ARP, o host A enviará uma solicitação ARP para solicitar o endereço MAC de *192.168.1.4*. Este pedido é uma mensagem de transmissão, de modo que todos os hosts na rede da área local receberão essa solicitação, conforme exibido a seguir.



Encaminhamento de solicitação ARP

De acordo com o protocolo, apenas o host D pode responder o pedido ARP do host A, e esta resposta ARP é uma mensagem unicast.



Encaminhamento de uma resposta ARP

O Host A gravará o endereço IP e o endereço MAC do host D no cache ARP depois de receber a resposta do host D. Nesse caso, o host não precisa enviar solicitação ARP para solicitar o endereço MAC do host de destino, a menos que a tabela expire.

Tabela ARP

Após o equipamento conseguir o endereço MAC via ARP, ele o adicionará à sua tabela ARP, como endereço IP, endereço MAC, porta e assim por diante.

A tabela ARP é dividida em tabela ARP dinâmica e tabela ARP estática.

- A tabela ARP dinâmica é gerada e mantida através do pacote ARP, pode ser envelhecida, atualizada pelo novo pacote ARP e coberta pela tabela estática ARP. Se atingiu o tempo de validade, ele eliminará a tabela ARP quando a porta estiver desativada.
- A tabela ARP estática é basicamente configurada e mantida manualmente. Não pode ser envelhecida como a tabela ARP dinâmica.

A tabela ARP estática é dividida em tabela ARP estática curta e tabela ARP estática longa.

Ao configurar uma tabela ARP estática longa, você deve configurar o endereço IP e o endereço MAC, bem como a VLAN e a porta de saída deste ARP. Um pacote ARP estático longo pode ser usado para transmitir o pacote diretamente.

Ao configurar a tabela ARP estática curta, você precisa configurar o endereço IP e o endereço MAC. A tabela ARP estática curta não pode ser usada para transmitir o pacote diretamente. Quando você precisa usar a tabela ARP estática, você deve enviar o pacote de solicitação ARP primeiro, se o endereço IP de origem e o endereço MAC fonte do pacote e o de resposta forem iguais, basta completar esta tabela ARP, então você pode usá-lo para transmitir o pacote de dados IP.

Obs.: *ao configurar a tabela ARP estática longa manualmente, o endereço IP da tabela ARP deve estar no mesmo segmento de rede com o endereço IP da porta de saída ou a operação de adição não será bem-sucedida.*

10.2. Configuração ARP

Configuração da tabela ARP

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar a tabela ARP estática curta	**arp {ipaddress mac** mac **}**	Obrigatório
Configurar a tabela ARP estática longa	**arp {ipaddress mac** mac **vid port** port**}**	Obrigatório
Configurar o tempo de envelhecimento	**arp aging-time** aging-time	Opcional, por padrão é de *20min*
Alteração da tabela estática para tabela dinâmica	**arp bind dynamic {***ipaddress* **| all}**	Obrigatório
Remover a tabela ARP	**no arp { dynamic | static | all |** *ipaddress* **}**	Opcional
Visualização da tabela ARP	**show arp { dynamic | static | all}**	Opcional

ARP Peer

ARP Peer significa que dois OLTs aprendem o ARP um do outro apenas pela porta especificada.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-

Operação	Comando	Obrigatório/ opcional
Configurar a tabela ARP Peer	**arp peer {ipaddress** macport **}**	Obrigatório
Remover a tabela ARP Peer	**no arp peer**	Opcional

» Exemplo de configuração:
OLT4840E(config)#arp peer 192.168.1.1 00:56:3A:40:5A:01 0/1

O endereço MAC do Peer acima é 00:56:3A:40:5A:01. Além disso, a mensagem ARP corresponde a este endereço MAC que toma o efeito somente quando é proveniente de Ethernet 0/1. O IP 192.168.1.1 atua apenas como um rótulo.

Sobrescrever o ARP

O OLT lida com o conflito ARP através deste comando. Se a porta habilitar esta função, a tabela de conflito ARP será atualizada para esta porta. Ou o conflito ARP não será tratado.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** device/slot/port	-
Configuração da função de sobrescrever o ARP	**arp overwrite**	Obrigatório
Proibir a função de sobrescrever o ARP	**no arp overwrite**	Opcional

Encaminhamento de Gratuitous-ARP

Por padrão, o OLT não tomará a iniciativa de encaminhar a mensagem Gratuitous -ARP quando a porta estiver estado de linkup. Mas você pode configurar o OLT para encaminhar.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Encaminhar a mensagem ARP gratuita ao configurar a porta de linkup	**linkup gratuitous-arp**	Obrigatório
Limitação do encaminhamento da mensagem ARP gratuita quando a porta está no estado de linkup	**no linkup gratuitous-arp**	Opcional

Arp-Reply-Repeat

O OLT responde a cada mensagem de solicitação ARP com apenas uma mensagem de resposta por padrão. Você pode configurar como a porta responde a cada mensagem de solicitação ARP com múltiplas respostas de ARP, de modo a suportar um certo tipo de protocolo.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configure o intervalo e a frequência de ARP-Reply-Repeat	**arp-reply-repeat interval** interval **times** times	Opcional, a unidade é milissegundo e o parâmetro padrão refere-se a repetição de resposta a cada *20 milissegundos*
Acesse o modo de configuração de interface	**interface ethernet** device/slot/port	-
Configuração da função *ARP-Reply-Repeat*	**arp-reply-repeat**	Obrigatório, desabilitado por padrão
Desabilitar a função de ARP-Reply-Repeat	**no arp-reply-repeat**	Opcional

Detecção ARP

O princípio da detecção ARP é configurar o endereço IP remoto, ou seja, definir o estado da tabela ARP correspondente como estado PROBE e configurar o tempo de envelhecimento desta tabela ARP como intervalo de retransmissão. Se receber a resposta ARP remota, atualizará o tempo de envelhecimento desta tabela ARP como valor normal (20 minutos). Ou será retransmitido. Além disso, se atingir os tempos de retransmissão enquanto ainda não recebeu uma resposta, a tabela ARP será excluída.

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	-
Configuração do dispositivo IP remoto	**arp probe ip { ip }**	Obrigatório, você pode configurar até *4 IP.*
Remover o dispositivo IP remoto	**no arp probe ip { all | ip }**	Opcional
Configure o parâmetro de ARP-probe IP	**arp probe [poll-timer** value | **retransmit { count value | interval** value **}]**	Opcional, poll-timer: o intervalo de valores é de 60-300 segundos e o valor padrão é *180 segundos.* Contagem: tempos de retransmissão, o intervalo de valores é 2-5 e o valor padrão é *3 vezes*: intervalo de retransmissão, intervalo de valores de 1-3 segundos e o valor padrão é de *3 segundos.*

Operação	Comando	Obrigatório/ opcional
Visualização do parâmetro probe	**show arp probe**	Opcional

Obs.: *não é permitido configurar o cronômetro durante o procedimento de execução da ARP-probe.*

ARP-proxy

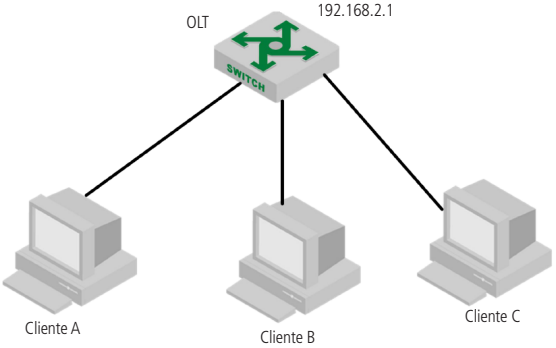
- **ARP-proxy:** a mensagem de solicitação do ARP é uma mensagem de transmissão, portanto não pode passar pela VLAN. Se o ARP estiver habilitado, as host da sub-VLAN na mesma interface super-VLAN podem ser capazes de executar a interação ARP, ou seja, os hosts podem se comunicar entre si.
- **ARP-proxy broadcast:** sub-VLAN pode ser capaz de executar ARP-proxy broadcast para outra sub-VLAN, por padrão, se a sub-VLAN permitir a função *ARP-proxy*. O comando *no ARP-proxy broadcast* pode ser usado para limitar a mensagem de solicitação ARP executando transmissão para outra sub-VLAN.
- **Ambiente de aplicação:** o ARP-proxy é adotado quando o host IP da sub-VLAN e a interface superVLAN IP estão no mesmo segmento de rede. Eles podem executar o encaminhamento de camada 3 através do gateway em vez de adotar o ARP-proxy se estiverem em um segmento diferente.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de VLAN	**vlan <vlanid>**	-
Habilitar o ARP-proxy	**arp-proxy**	Obrigatório
Desabilitar o ARP-proxy	**no arp-proxy**	Opcional
Habilitar o broadcast de ARP-proxy	**arp-proxy broadcast**	Opcional
Desabilitar broadcast de ARP-proxy	**no arp-proxy broadcast**	Opcional
Visualização das informações do proxy ARP configuradas no sistema atual	**show arp-proxy**	Opcional, pode ser executado em todos os modos

Operação	Comando	Obrigatório/ opcional
Visualização das informações do broadcast proxy ARP configuradas no sistema atual	**show arp-proxy broadcast**	Opcional, pode ser executado em todos os modos

» Exemplo de configuração:

Conforme exibido na figura a seguir: VLAN 2, 3, 4 são a sub-VLAN de SuperVLAN -interface1, e eles estão conectados a computerA, computerB, computerC, respectivamente, com o ARP-proxy ativado. Além disso, a VLAN 4 está no estado com o ARP-proxy broadcast desativado.



OLT4840E(config)#interface supervlan-interface 1

OLT4840E(config-if-superVLANInterface-1)#subvlan 2-4

OLT4840E(config-if-superVLANInterface-1)#ip address 192.168.2.1 255.255.255.0

OLT4840E(config-if-superVLANInterface-1)#exit

OLT4840E(config)#vlan 2-4

OLT4840E(config-if-vlan)#arp-proxy

Config arp-proxy enable successfully.

OLT4840E (config-if-vlan)#exit

OLT4840E (config)#vlan 4

OLT4840E (config-if-vlan)#no arp-proxy broadcast

Config arp-proxy broadcast disable successfully.

» **1:** cliente A encaminha o pacote de solicitação ARP, B \ C podem ser capaz de responder. Ping entre cliente A e cliente B é realizado com sucesso.

» **2:** cliente C encaminha o pacote de solicitação ARP, A \ C não podem responder. Ping entre cliente C e cliente A não realizado.

11. Espelhamento

O espelhamento significa copiar pacotes que correspondem à regra escolhida para a porta de destino de espelhamento. Geralmente, o destino está conectado ao dispositivo de detecção de dados. Os usuários podem analisar os pacotes espelhados, monitorar a rede e solucionar problemas de falhas. Ele é dividido em espelhamento de portas e espelhamento de fluxo.

11.1. Espelhamento de portas

Espelhamento de portas é usado para copiar os pacotes recebidos ou enviados em uma porta para a porta de destino de espelhamento. O OLT suporta espelhamento um-para-um e muitos-para-um, suportando várias fontes de espelhamento.

- **Espelhado:** pode ser uma porta ou um pacote que a CPU recebe ou envia.
- **Espelho:** para o OLT, a porta de destino do espelho pode ser apenas uma. Se a porta de destino de espelhamento estiver configurada, somente a última configuração entrará em vigor.

Configuração de espelhamento de porta

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da porta espelhada	**mirror source-interface {{ethernet | pon}** port-number**| cpu } {ingress | egress | both}**	Obrigatório. É possível configurar múltiplas portas como espelhadas
Configuração da porta espelho	**mirror destination-interface {ethernet | pon}** port-number	Obrigatório, apenas uma porta pode ser configurada como espelho
Remover o grupo de espelhamento	**no mirror {soure-interface {cpu | {ethernet | pon}** port-number **} | destination-interface ethernet** device/slot/port **| all }**	Opcional
Visualização do grupo de espelhamento	**show mirror**	Opcional

Exemplo de configuração de espelhamento de porta

1. Requisitos de rede:
   Pacotes espelhados da CPU, e 0/1, e 0/2 ~ e 0/4.

» Passos de configuração:

OLT4840E(config)#mirror source-interface cpu both

OLT4840E(config)#mirror source-interface ethernet 0/1 both

OLT4840E(config)#mirror source-interface ethernet 0/2 both

OLT4840E(config)#mirror destination-interface ethernet 0/4

» Validação de resultados:

OLT4840E(config)#show mirror

Information about mirror port(s)

The monitor port : e0/4

The mirrored egress ports : cpu,e0/1-e0/2.

The mirrored ingress ports : cpu,e0/1-e0/2.

The packet of CPU, e 0/1, e 0/2 can be mirrored to port e 0/4.

11.2. Espelhamento de fluxo

O espelhamento de fluxo significa copiar as regras de ACL que correspondem ao fluxo de serviço para a porta de destino para análise e monitoramento de pacotes. Antes de configurar o espelho de fluxo, você precisa definir as regras ACL que atendem aos requisitos. O dispositivo faz referência a essas regras ACL para a identificação do fluxo.

Configuração do espelhamento de fluxo

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do espelhamento de fluxo	**mirrored-to** {ip-group<1-199>|link-group<200-299>[**subitem**<0-127>]	Obrigatório
Remover o espelhamento de fluxo	**no mirrored-to** {ip-group<1-199>|link-group<200-299>[**subitem**<0-127>]	Opcional
Verificação da operação	**show mirror**	Opcional

Exemplo de configuração de espelhamento de fluxo

» Requisitos de rede:
Espelhe os pacotes cujo endereço IP de origem é 10.1.1.1 para e 0/7.

» Passos de configuração:
OLT4840E(config)#access-list 100 permit 10.1.1.1 0 any
OLT4840E(config)#mirror destination-interface ethernet 0/7
OLT4840E(config)#mirrored-to ip-group 100

» Validação de resultados:
A porta e 0/7 pode capturar pacotes com fonte IP 10.1.1.1

12. Gerenciamento de login SNMP

12.1. Visão geral de SNMP

O SNMP (*Simple Network Management Protocol*) é um importante protocolo de gerenciamento de rede em redes TCP/IP pela troca de pacotes. Ele oferece a possibilidade de gerenciamento centralizado de grandes redes e seu objetivo é garantir que as informações sejam transmitidas entre dois pontos. Esta ferramenta é útil para o administrador da rede recuperar informações de qualquer nó na rede, fazer modificações, encontrar falhas, realizar um diagnóstico de falhas, planejar a capacidade da rede e gerar de relatórios.

A estrutura SNMP é dividida em duas partes: NMS e Agent. NMS (Network Management Station) é uma estação de trabalho que executa programas de clientes, enquanto o Agente é um software executado em um dispositivo de rede que pode encaminhar os pacotes GetRequest, GetNextRequest e SetRequest. Ao receber a mensagem de solicitação NMS, o agente executa operações de leitura ou gravação e gera um pacote de resposta para retornar ao NMS. Por outro lado, quando o dispositivo encontrar um evento anormal, o agente enviará um pacote de trap para o NMS para relatar os eventos.

O sistema suporta SNMPv1, SNMPv2c e SNMPv3. O SNMPV1 fornece um mecanismo de autenticação simples, não suporta as comunicações de administrador para gerencia e a Trap v1 não possui mecanismo de confirmação. O modelo v2c é o modelo v1 aprimorado (em segurança), com estrutura de informações de gerenciamento, operação de protocolo, gerenciamento e capacidade de comunicação entre gerentes para aumentar a criação e exclusão da tabela, reduzindo o lado de armazenamento do agente. V3 implementa o mecanismo de autenticação do usuário e mecanismo de criptografia de pacotes, o que melhora a segurança do protocolo SNMP.

12.2. Configuração de parâmetros básicos

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
(Des)Habilite o SNMP	**snpm-server** [enable|disable]	Opcional, habilitado por padrão
Configuração do sysContact	**[no] snmp-server contact** syscontact	Opcional, com parâmetros padrão
Visualização da configuração do sysContact	**show snmp contact**	Opcional
Configuração do sysLocation	**[no] snmp-server location** syslocation	Opcional, com parâmetros padrão
Visualização da configuração do sysLocation	**show snmp location**	Opcional
Configuração do sysName	**[no] snmp-server name** sysname	Opcional, com parâmetros padrão
Visualização da configuração do sysName	**show snmp name**	Opcional
Configuração do tamanho máximo dos pacotes SNMP	**[no] snmp-server max-packet-length length**	Opcional
Visualização das informações do nó MIB	**show snmp mib** [modeule module-name]	Opcional

12.3. Configuração do nome de comunidade

O SNMP adota o esquema de autenticação de nomes de comunidade (definidos por uma string), os pacotes SNMP que não correspondem a eles serão descartados. Diferentes comunidades podem ter permissão de acesso somente leitura ou leitura-gravação. Quando o acesso é somente leitura ela só pode consultar as informações do sistema. No entanto, além de consultar as informações do sistema, uma comunidade com permissão de acesso de leitura e gravação pode executar a configuração do sistema. Por padrão, não existe um nome de comunidade.

» Configuração de nome de comunidade:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração para visualização do nome de comunidade criptografado ou não	**snmp-server community encrypt** { enable | disable }	Opcional, não criptografado por padrão
Visualização do nome da comunidade	**show snmp community**	Opcional
Remover o nome da comunidade	**no snmp-server community** community-index	Opcional

Obs.: *a função de criptografia do nome da comunidade é irreversível. Ou seja, depois que a criptografia é configurada, se a função de criptografia for desativada, a comunidade previamente criptografada não se tornará um texto simples e somente a comunidade recém-configurada será criptografada.*

12.4. Configuração de grupo

Esta configuração pode ser usada para configurar um grupo de controle de acesso. Por padrão, existem dois grupos snmpv3:

» **(1):** o grupo initial com o nível de segurança de auth.

» **(2):** o grupo initial com o nível de segurança de noauthpriv.

» Configuração de group:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de grupo	**snmp-server group** group-name **3 [auth | noauth | priv] read** read-view **write** write-view **notify** notify-view	Obrigatório
Configuração do contexto do grupo	**[no]snmp-server group group-name 3 context** context-name	Opcional
Visualização da configuração de grupo	**show snmp group** [group-name]	Opcional

12.5. Configuração de usuário

Ele é usado para configurar o usuário para o mecanismo local ou para o mecanismo remoto. Por padrão, os seguintes usuários existem:

» (1) initialmd5.

» (2) initialsha.

» (3) inicialnone.

Os três usuários acima são reservados para o sistema e não podem ser utilizados. Ao configurar um usuário, você precisa garantir que o mecanismo ao qual ele pertence seja identificável. Quando um mecanismo identificável é excluído, os usuários vinculados a ele também são excluídos.

» Configuração de usuário:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração para visualização da senha criptografado ou não	**snmp-server encrypt** { enable | disable }	Opcional, criptografado por padrão
Configuração de usuário	**snmp-server user** username groupname **[remote ipaddress [udp-port** port-number**]] [auth** { md5 | sha } **{ auth-password** authpassword **| auth-key** authkey **} [priv des priv-key { auth-key** privkey **| auth-password** privpassword **}]]**	Obrigatório
Remover usuário	**no snmp-server user** username **[remote** ipaddress **[udp-port** port-number **]]**	Opcional
Visualização do nome do usuário	**show snmp user [**username**]**	Opcional

Obs.: » *Para configurar um usuário remoto é necessário incluir os seguintes parâmetros remote [ipaddress] udp-port [port number]. Se você não incluir estes parâmetros, será configurado um usuário local.*

» ***Port number:*** *é o número da porta remota, se você não especificar, será utilizada a porta padrão* 162.

» *Existem três níveis de privilégio de usuário: noauthpriv (nenhuma autenticação e criptografia é necessária), esta é a configuração padrão; auth (autenticação é necessária, mas não criptografada); authpriv (requer autenticação e criptografia). O nível de segurança do usuário deve ser o mesmo que o grupo de segurança de grupo correspondente.*

12.6. Configuração de views

Views são usadas para configurar as visualizações disponíveis para acesso de controle e suas subárvores. O *iso*, *internet* e *sysview* existem por padrão. Não é possível eliminar e/ou modificar a *internet*.

» Configuração de views:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de views	**snmp-server view** view-nameoid-tree **{ included | excluded }**	Obrigatório
Remover a view	**no snmp-server view** view-name [oid-tree]	Opcional
Visualizar as configurações de views	**show snmp view** view-name	Opcional

12.7. Configuração de notificação SNMP

» Configuração de notificação SNMP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do IP da fonte de pacotes de informação	**[no]snmp-server trap-source { loopback-interface |vlan-interface | supervlan-interface }** if-id	Opcional
Habilitar a função de notificação	**[no]snmp-server enable [[informs | traps] [bridge | gbn | gbnsavecfg | interfaces | rmon | snmp]]**	Obrigatório
Visualizar as configurações de notificações	**show snmp notify**	Opcional
Configuração de notificação do host de destino	**[no]snmp-server host** ipaddress **[version {1 | 2c | 3 [auth | noauthpriv | priv] }** security-name **[udp-port** port-number**] [notify-type [bridge | gbn | gbnsavecfg | interfaces | rmon | snmp]]**	Obrigatório
Visualização de configuração do host de notificação	**show snmp host**	Opcional

12.8. Configuração de engine ID

Ele é usado para configurar o id da engine do snmp local e remoto. O ID local padrão é *134640000000000000000000*, este valor pode ser modificado, mas não pode ser excluído. O ID remoto pode ser adicionado e/ou removido (por padrão não está configurado). Uma vez que uma engine remota identificável é excluída, seus usuários correspondentes também serão excluídos. O número máximo de engine remotas configuráveis é 32. O comando de *no* é utilizado para restaurar o ID da engine local padrão ou excluir o ID da engine remoto.

» Configuração da Engine ID:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da engineid	**snmp-server engineid { local** engine-id **| remote** ipaddress **[udp-port** port-number**]** engine-id **}**	Opcional
Visualizar as configurações de engineid	**show snmp engineid { local | remote } [** id **]**	Opcional
Remover engineid	**no snmp-server engineid { local | remote** ipaddress port-number **}**	Opcional

12.9. Exemplo de configuração de SNMP

» Requisitos de rede:

Antes de acessar o OLT com o navegador mib, verifique se o terminal do navegador mib pode se comunicar com o OLT corretamente.

1. Configure a comunidade teste2 e, em seguida, faça com que o navegador mib acesse o OLT através do snmp v1 / v2;
2. Configure o nome do grupo como g3, o nome de usuário como u3, os níveis de segurança como auth, em seguida, faça com que o navegador mib acesse o OLT através do snmp v3;
3. Configure a notificação snmp. Notificar v2 e v3 respectivamente.

» Passos de configuração:

» Habilitar SNMP

OLT4840E(config)#snmp-server enable

» Configure a comunidade test2

OLT4840E(config)#snmp-server community test2 rw permit view iso

» Configure o nome do grupo como g3, o nome de usuário como u3, os níveis de segurança como auth

OLT4840E(config)#snmp-server group g3 3 auth notify iso read iso write iso

OLT4840E(config)#snmp-server user u3 g3 auth md5 auth-password password

OLT4840E(config)#show snmp group g3

groupname: g3

securitymodel: 3 auth

readview: iso

writeview: iso

notifyview: iso

context: default value(NULL)

OLT4840E(config)#show snmp user u3

User name: u3

Engine ID: 134640000000000000000000

Authentication Protocol: HMACMD5AuthProtocol

Group-name: g3

Validation: valid

» Configure a função de notificação

  » Habilite a função de notificação

  OLT4840E(config)#snmp-server enable traps

  #Configure o host de notificação

  OLT4840E(config)#snmp-server host 192.168.1.10 version 2 test2

  OLT4840E(config)#snmp-server host 192.168.1.10 version 3 auth u3

13. Configuração de ACL

Para filtrar o pacote de dados, você precisa configurar uma série de regras para identificar o objeto que precisa ser filtrado. Depois de reconhecer um objeto especial, ele pode configurar para permitir ou negar a passagem destes pacotes. A lista de controle de acesso (ACL) é usada para executar esta função.

A ACL classifica os pacotes de acordo com uma série de condições de correspondência, que podem ser o endereço de origem, endereço de destino, número da porta e assim por diante. O OLT detecta os pacotes com base nas condições especificadas na ACL para determinar se deseja encaminhar ou descartar os mesmos.

As regras de correspondência dos pacotes de dados podem ser introduzidas em outras situações em que é preciso distinguir o fluxo, como a classificação do fluxo na QoS.

De acordo com o objetivo da aplicação, a ACL pode ser dividida nas seguintes categorias:

- **ACL padrão (standard):** define regras baseadas apenas em endereços IP de origem.
- **ACL estendida (extended):** define regras baseadas em endereço IP de origem, endereço IP de destino, tipo de protocolo e atributos de protocolo de pacotes.
- **Layer 2 ACL:** informações de camada 2 como endereço MAC de origem, MAC de destino, prioridade de VLAN e tipo de protocolo.

13.1. Ordem de correspondência da ACL

Uma vez que a mesma ACL pode configurar vários sub-itens então pode existir um problema de ordem de correspondência. As ACLs suportam duas ordens de correspondência:

- **Config:** corresponde às regras ACL de acordo com a ordem de configuração.
- **Auto:** combina as regras da ACL de acordo com a regra de depth-first.
  - Depth-first significa que o sub-item com maior precedência terá correspondência primeiro.
- Ordem de correspondência da ACL:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da ordem de correspondência da ACL	**access-list** access-list **match-order {auto| config}**	Opcional, já está configurada por padrão

Obs.: *o modo* Config *é para usuários que conhecem bem a função* ACL, *é recomendável usar o modo* Auto, *pois ela classifica as regras na ordem correta automaticamente.*

Exemplo de configuração de ordem de correspondência da ACL

1. Se a ordem de correspondência for a ordem de config, configure dois sub-itens, o 0 deve ser para negar todos os endereços IPs de origem.

As configurações são as seguintes:

OLT4840E(config)#access-list 1 deny any // Configuração de 2 sub-itens da mesma ACL

Config ACL subitem successfully.

OLT4840E (config)#access-list 1 permit 1.1.1.1 0

Config ACL subitem successfully.

OLT4840E (config)#show access-list config 1 // Ordem de configuração por padrão

Standard IP Access List 1, match-order is config, 2 rule:

0	deny	any	
1	permit	1.1.1.1	0.0.0.0

2. Se a ordem de partida que você escolher for automática, a regra de correspondência ACL com maior precedência será o sub-item 0. As configurações são as seguintes:

OLT4840E (config)#access-list 1 match-order auto // Defina para a ordem automática

Config ACL match order successfully.

OLT4840E (config)#access-list 1 deny any

Config ACL subitem successfully.

OLT4840E (config)#access-list 1 permit 1.1.1.1 0

Config ACL subitem successfully.

OLT4840E(config)#show access-list config 1

Standard IP Access List 1, match-order is auto, 2 rule:

0	permit	1.1.1.1	0.0.0.0
1	deny	any	

13.2. ACL padrão (standard)

A ACL padrão apenas executa a análise e o processamento correspondentes nos pacotes de acordo com as regras especificadas no endereço IP de origem.

Se ela for identificada por números, sua sequência deve variar de 1 a 99. Podem ser criadas até 99 ACLs padrão; se for identificada por nomes, podem ser definidas até 1000 entradas. Além disso, o OLT pode definir até 128 sub-regras para cada ACL.

Se você deseja configurar uma regra com os parâmetros de intervalo de tempo, é necessário definir primeiro o intervalo de tempo correspondente. Para isso, consulte *13.5. Intervalo de tempo.*

» ACL identificada por números:

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	-
Defina uma ACL	**access-list** num **{ permit | deny } {** source-IPv4/v6 source-wildcard **| any | ipv6any } [time-range** name **]**	Obrigatório
Remover a ACL baseada em números	**no access-list [** num subitem |all **]**	*Opcional*, all - refere-se a todas as ACLs

» ACL identificada por nome:

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	-
Configure uma ACL padrão com base no nome e entre no modo de configuração de ACL	**access-list standard** name	Obrigatório
Configure uma regra de ACL	**{ permit | deny } {** source-IPv4/v6 source-wildcard **| any | ipv6any } [time-range** name **]**	Obrigatório
Remover uma ACL baseada em nome	**no access-list [**name **|** subitem **]** all	Opcional

» Descrições das regras padrão da ACL:

permit/deny	Escopo da regra de ACL	*permit* significa permitir o acesso, *deny* significa negar o acesso
{ source-IPv4/v6 source-wildcard **| any | ipv6any}**	Especifique o endereço de origem da regra ACL	*source-IPv4/v6 source-wildcard* é usado para determinar o intervalo de endereço IP de origem (IPv4 / v6) do pacote. Os endereços IPv4 são representados em notação decimal pontilhada; os endereços IPv6 são representados em hexadecimal; quando o *source-wildcard* é 0, indica o endereço do host; any | IPv6 faz referência a qualquer endereço de origem.
{ dest-IPv4/v6 dest-wildcard **| any | ipv6any }**	Especifique o endereço de destino da regra ACL	*dest-IPv4/ v6 dest-wildcard* é usado para determinar o intervalo de endereço IP de destino (IPv4 / v6). Os endereços IPv4 são representados em notação decimal pontilhada; os endereços IPv6 são representados em hexadecimal; quando o caractere *source-wildcard* é 0, ele indica o endereço do host; *any | ipv6any* faz referência para qualquer endereço de origem.
time-range name	Especifica o intervalo de tempo em que a regra produz efeitos	Consulte *13.5. Intervalo de tempo*

Exemplo de configuração

» Defina uma ACL padrão identificada com números para proibir os pacotes cujo endereço IP de origem é 10.0.0.1

OLT4840E#configure terminal

OLT4840E(config)#access-list 1 deny 10.0.0.1 0

Config ACL subitem successfully.

» Define uma ACL padrão identificada com nomes para proibir os pacotes cujo endereço IP de origem é 10.0.0.2

OLT4840E(config)#access-list standard stdacl

Create ACL item successfully.

OLT4840E(config-std-nacl-stdacl)#deny 10.0.0.2 0

Config ACL subitem successfully.

13.3. ACL estendida (extended)

Uma ACL estendida pode criar regras com base em informações do endereço IP de origem, endereço IP de destino, tipo de protocolo, as características do protocolo e assim por diante.

Se ela for identificada por números, a sequência varia de 100 a 199. Podem ser criadas até 100 ACLs estendidas. Se ela for identificada por nomes, podem ser definidas até 1000 entradas. Ao mesmo tempo, o OLT pode definir até 128 sub-regras para cada ACL.

Se você deseja configurar uma regra com os parâmetros do intervalo de tempo, é necessário definir primeiro o intervalo de tempo correspondente. Para isso, consulte *13.5. Intervalo de tempo*

» Identificação de ACL por números:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Defina uma ACL extendida	**access-list** num **{ permit | deny } [protocol] [established] {** source-IPv4/v6 source-wildcard **| any | ipv6any } [**source-port wildcard **] {** dest-IPv4/v6 dest-wildcard **| any | ipv6any } [**dest-port wildcard **]** **[**icmp-type icmp-code **] [**igmp-type**] [traffic-class** traffic-class**][precedence** precedence **] [tos** tos **] | [dscp** dscp **][fragments][time-range** name **]**	Obrigatório
Remover a ACL baseada em números	**no access-list [** num **|**all **]**	*all* - refere-se a todas as ACLs

» Descrição das regras de ACL extendidas:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configure uma ACL padrão com base no nome e entre no modo de configuração de ACL	**access-list standard** name	Obrigatório

Operação	Comando	Obrigatório/ opcional
Configure uma regra de ACL	**{ permit | deny } [** protocol **] [established] {** source-IPv4/v6 source-wildcard **| any | ipv6any } [**source-port wildcard **] {** dest-IPv4/ v6 dest-wildcard **| any | ipv6any } [**dest-port wildcard **] [**icmp-type icmp-code **] [**igmp-type**] [traffic-class** traffic-class**][precedence** precedence **] [tos** tos **] | [dscp** dscp **][fragments][time-range** name **]**	Obrigatório
Remover uma ACL baseada em nome	**no access-list [**name **|** subitem **]** all	Opcional, *all* - refere-se a todas as ACLs

Os parâmetros detalhados na ACL estendida são descritos na tabela a seguir.

» Descrição das regras ACL estendidas:

permitir/negar	Escopo da regra de ACL	*permit* significa permitir o acesso, deny significa negar o acesso
established	SYN flag no TCP	SYN = 1 siginifica ativo
{ *source-IPv4/v6 source-wildcard* **| any | ipv6any }**	Especifique o endereço de origem da regra ACL	*source-IPv4/v6sour-wildcard* é usado para determinar o intervalo de endereço IP de origem (IPv4 / v6) do pacote. Os endereços IPv4 são representados em notação decimal pontilhada; os endereços IPv6 são representados em hexadecimal; quando o *source-wildcard* é 0, indica o endereço do host; *any|ipv6any* se refere a qualquer endereço de origem.
{ dest-IPv4/v6 dest-wildcard**| any | ipv6any }**	Especifique o endereço de destino da regra da ACL	*dest-IPv4/v6 dest-wildcard* é usado para determinar o intervalo de endereço IP de destino (IPv4 / v6). Os endereços IPv4 são representados em notação decimal pontilhada; os endereços IPv6 são representados em hexadecimal; quando o *source-wildcard* é 0, indica o endereço do host; *any|ipv6any* refere-se a qualquer endereço de origem.

source-port/ dest-port wildcard	Números de porta de origem e destino TCP / UDP	*wildcard* - O número inverso determina o intervalo de números de porta
icmp-type icmp-code	Tipo de pacote de protocolo ICMP	É válido somente quando o protocolo é configurado como icmp / icmpv6
igmp-type	Tipo de pacote de protocolo ICMP	É válido somente quando o protocolo é configurado como IGMP
traffic-class	**traffic-class** in Ipv6	Disponível apenas para mensagens IPv6
precedence	Prioridade de precedência	A prioridade de IP varia de 0 a 7
tos	Prioridade de TOS	O valor varia de 0 a 15
dscp	Prioridade de DSCP	O valor varia de 0 a 63
fragments	Fragmentos de pacotes	A regra é válida apenas para pacotes não primários fragmentados

Exemplo de configuração de ACL extendida

» Define uma ACL estendida com base em números para negar pacotes FTP cujo endereço IP de origem seja 10.0.0.1.

OLT4840E(config)#access-list 100 deny tcp 10.0.0.1 0 ftp any

Config ACL subitem successfully.

» Define uma ACL estendida baseada em nome para negar pacotes FTP cujo endereço IP de origem seja 10.0.0.2.

OLT4840E(config)#access-list extended extacl

Create ACL item successfully.

OLT4840E(config-ext-nacl-extacl)#deny tcp 10.0.0.2 0 ftp any

Config ACL subitem successfully.

13.4. ACL Layer 2

As ACL Layer 2 (ACL de camada 2) podem ser configuradas com base nas informações da camada 2, como endereço MAC de origem, endereço MAC de destino, prioridade de VLAN e tipo de protocolo de camada 2.

Se for identificada por números, variando de 200 a 299. Você pode criar até 100 listas identificadas por números; se for identificada por nomes, podem ser definidas até 1000 entradas. Ao mesmo tempo, o OLT pode definir até 128 sub-regras para cada ACL.

Se você deseja configurar uma regra com os parâmetros do intervalo de tempo, é necessário definir primeiro o intervalo de tempo correspondente. Para a configuração do intervalo de tempo, consulte 12.5.

» ACL identificada por número:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Defina uma ACL extendida	**access-list** num **{ permit | deny } [** protocol **] [cos** vlan-pri **] ingress { { [inner-vid** vid **] [start-vlan-id end-vlan-id] [** source-mac-addr source-mac-wildcard **] [interface** interface-num **] } | any } egress { { [** dest-mac-addr dest-mac-wildcard **] [interface** interface-num **| cpu] } | any } [time-range** name **]**	Obrigatório
Remover a ACL baseada em números	**no access-list [** num **|**all **]**	Opcional, *all* - refere-se a todas as ACLs

» ACL identificada por nome:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configure uma ACL Layer 2 e acesse o modo de configuração de ACL	**access-list link** name	Obrigatório
Configure uma regra de ACL	**{ permit | deny } [** protocol **] [cos** vlan-pri **] ingress { { [inner-vid** vid **] [**start-vlan-id end-vlan-id **] [** source-mac-addr source-mac-wildcard **] [interface** interface-num **] } | any } egress { { [** dest-mac-addr dest-mac-wildcard **] [interface** interface-num **| cpu] } | any } [time-range** name **]**	Obrigatório
Remover uma ACL baseada em nome	no access-list [name | all}	Opcional, *all* refere-se a todas as ACL

» Descrição das regras de ACL Layer2:

permitir/negar	Escopo da regra de ACL	**permit** significar permitir o acesso, **deny** significa negar o acesso
protocol	Tipo de protocolo carregado pelo frame Ethernet	Em notação hexadecimal, alcance 0 para FFFF. Opcional para ARP, IP, RARP
cos	A prioridade da tag Vlan	Prioridade varia de 0 até 7
Ingress/ egress	Direção do pacote a ser aplicado a regra	-
inner-vid	O valor interno de vid de um pacote com duas tags	-
start-VLAN-ID *end-VLAN-ID*	Ele é usado para indicar a faixa de VLANs	Para o pacote com duas tags, é a faixa de vid da etiqueta externa; para o pacote com uma tag, e a faixa da própria tag.
source-mac-addr *source-mac-wildcard*	Opções de endereço fonte MAC	O source-mac-wildcard pode ser usado para indicar o intervalo fonte MAC
interface *interface-num*	O número da porta física	Dividido em porta de entrada e porta de saída
CPU	-	Indica que os dados serão encaminhados para a CPU
any	Qualquer endereço	Dividido em direção de entrada e saída

Exemplo de configuração para ACL Layer 2

» Defina uma ACL de camada 2 que é identificada por número e desabilite os pacotes ARP cujo endereço MAC de origem é 00:00:00:00:01.

OLT4840E(config)#access-list 200 deny arp ingress 00:00:00:00:00:01 0 egress any

Config ACL subitem successfully.

» Defina uma ACL de camada 2 que é identificada pelo nome e desative os pacotes ARP cujo endereço MAC de origem é 00:00:00:00:02.

OLT4840E(config)#access-list link lnkacl

Create ACL item successfully.

OLT4840E(config-link-nacl-lnkacl)#deny arp ingress 00:00:00:00:00:02 0 egress any

Config ACL subitem successfully.

13.5. Intervalo de tempo

A configuração do intervalo de tempo inclui o intervalo de tempo periódico e o intervalo de tempo absoluto. Configurar um intervalo de tempo periódico assume a forma de dias da semana. O intervalo de tempo absoluto é configurado a partir do horário de início até o final do intervalo de tempo.

» Configuração de intervalo de tempo:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Crie um intervalo de tempo e entre no modo de configuração do intervalo de tempo	**time-range** name	Obrigatório
Configure um intervalo de tempo absoluto	**absolute start** HH:MM:SS YYYY/MM/DD **[end** HH:MM:SS YYYY/MM/DD **]**	Obrigatório
Configuração de um intervalo de tempo periódico	**periodic** days-of-the-weekhh:mm:ss **to** [day-of-the-week] hh:mm:ss	
Remover os intervalos de tempo	**no time-range [all | name** name**]**	Opcional, *all* - significa que todos os intervalos serão removidos

Exemplo de configuração

» Configure o intervalo de tempo absoluto, que varia de 16:00 em 30 de março de 2015 às 16:00 em 31 de março de 2015.

OLT4840E(config)#time-range b

Config time range successfully.

OLT4840E(config-timerange-b)#absolute start 16:00:00 2015/03/30 end 16:00:00 2015/03/31

Config absolute range successfully .

OLT4840E(config-timerange-b)#show time-range name b

Current time is: 10:19:16 2015/03/30 Monday

time-range: b (Inactive)

absolute: start 16:00:00 2015/03/30 end 16:00:00 2015/03/31

» Configure o intervalo de tempo periódico, que varia de 8:00 a 18:00 e de segunda a sexta-feira.

OLT4840E(config)#time-range d

Config time range successfully.

OLT4840E(config-timerange-d)#periodic weekdays 8:00:00 to 18:00:00

Config periodic range successfully .

OLT4840E(config-timerange-d)#show time-range name d

Current time is: 10:23:33 2015/03/30 Monday

time-range:d (Inactive)

periodic: weekdays 08:00:00 to 18:00:00

13.6. Ativar a ACL

As ACLs precisam ser ativadas antes de entrarem em vigor e seguir as regras de: *a primeira ativação terá precedência.*

» Ativar a ACL:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
A regra para ativação da ACL	**access-group** [**ip-group** name | num] [**link-group** name | num] [**subitem** num]	Obrigatório
Desativar uma ACL específica	**no access-group [ip-group** name | num **][link-group** name **|** num **] [subitem** num **]**	
Desativar todas as ACLs	**no access-group all**	

Obs.: *quando o math-order for auto, seguir a ordem que foi estipulada pela OLT começando no* 0*, é possível visualizar através do comando show access-list config all.*

Exemplo de configuração para ativação de ACL

» Exemplo 1: configure uma ACL e depois a ative.

» Caso 1:

» Antes de ativar uma ACL:

OLT4840E(config)#access-list 1 deny any

Config ACL subitem successfully.

OLT4840E(config)#access-list 1 permit 1.1.1.1 0

Config ACL subitem successfully.

OLT4840E(config)#show access-list config 1

Standard IP Access List 1, match-order is config, 2 rule:

0 deny any

1 permit 1.1.1.1 0.0.0.0

» Configure para ativar uma ACL:

OLT4840E(config)#access-group ip-group 1 subitem 1

Activate ACL successfully .

OLT4840E(config)#access-group ip-group 1 subitem 0

Activate ACL successfully .

De acordo com o princípio de que a primeira ativação tem precedência, o dispositivo só permite que os pacotes com o endereço IP de origem 1.1.1.1 passem.

» Caso 2:

» Antes de ativar a ACL:

OLT4840E(config)#access-list 1 match-order auto

Config ACL match order successfully.

OLT4840E(config)#access-list 1 deny any

Config ACL subitem successfully.

OLT4840E(config)#access-list 1 permit 1.1.1.1 0

Config ACL subitem successfully.

OLT4840E(config)#show access-list config 1

Standard IP Access List 1, match-order is auto, 2 rule:

0 permit 1.1.1.1 0.0.0.0

1 deny any

» Configure para ativar a ACL:
OLT4840E(config)#access-group ip-group 1 subitem 0

Activate ACL successfully .

OLT4840E(config)#access-group ip-group 1 subitem 1

Activate ACL successfully

De acordo com o princípio de que a primeira ativação tem precedência, o dispositivo só permite que os pacotes com o endereço IP de origem 1.1.1.1 passem.

» Exemplo 2: configure várias ACLs e, em seguida, ative-as para alcançar o IP + MAC + ligação da porta.
OLT4840E(config)#access-list 1 permit 1.1.1.1 0

Config ACL subitem successfully.

OLT4840E(config)#access-list 200 permit ingress 00:00:00:00:00:01 0 interface ethernet 0/1 egress any

Config ACL subitem successfully.

OLT4840E(config)#access-group ip-group 1 link-group 200

Activate ACL successfully .

13.7. Visualização e depuração da ACL

Depois de concluir as configurações acima, você pode usar os seguintes comandos para visualizá-las.

» Visualização e depuração da ACL:

Operação	Comando	Obrigatório/ opcional
Contagem do número de ACL	**show access-list config statistic**	Opcional, executável em todos os modos
Visualização das ACLs	**show access-list config {all |** num | **name** | name}	
Contagem do número de ACLs ativas	**show access-list runtime statistic**	
Visualização de ACLs ativas	**show access-list runtime {all |** num | **name** | name}	

14. Configuração de QACL

QACL (QOS e ACL), refere-se à função de associar regras de trânsito às operações de tráfego usando ACL. Ou seja, as funções de QoS são realizadas por referência à lista de controle de acesso, incluindo filtragem de pacotes, taxa de acesso de compromisso, espelhamento de tráfego, estatística de tráfego, redirecionamento, reescrita ou inserção de VLAN, remarcação de precedência e cópia de tráfego para a CPU, trTCM e outras funções.

14.1. Conceitos relacionados à QACL

Tráfego

O tráfego refere-se a mensagem que passa pelo OLT.

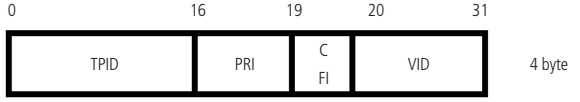
Classificação do tráfego

A classificação de tráfego refere-se à utilização de certas regras para identificar mensagens que atinjam determinadas características. A regra de classificação é regra de filtragem configurada pelo administrador de acordo com o requisito de gerenciamento, que pode ser simples, por exemplo: o tráfego de precedência diferente pode ser identificado de acordo com o campo ToS no cabeçalho da mensagem IP ou poderá ser mais complicado: como informações de camada 2, camada 3 e camada 4 incluindo endereço MAC, endereço IP, número da porta e outras informações relacionadas para classificar mensagens. Estas são regras de classificação de tráfego complexas. A classificação geral é limitada às informações de cabeçalho da mensagem do pacote e o conteúdo da mensagem.

Precedência

A precedência 802.1p está no cabeçalho da mensagem da Camada 2 e aplicável às ocasiões em que as mensagens da Camada 3 não precisam ser analisadas e o QoS precisa ser garantido na Camada 2.

Conforme descrito na seção de configuração de VLAN, cada host que suporta o protocolo 802.1Q adiciona um cabeçalho de tag 802.1Q de 4 bytes atrás do endereço de origem no cabeçalho do frame original ao enviar um pacote de dados. Conforme exibido na figura a seguir.



802.1Q tag

Na figura acima, o campo PRI é a precedência 802.1p, que consiste em 3 bits. O valor varia de 0 a 7. Estes três bits indicam a precedência do quadro, que consistem em oito prioridades, principalmente é usado para determinar a precedência para enviar pacotes de dados quando o switch está sobrecarregado.

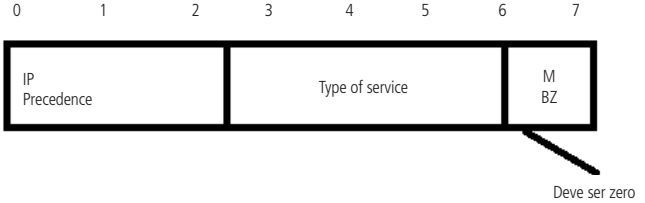
» Descrição de valores do 802.1Q:

Cos (decimal)	Cos (binário)	Implicação
0	000	Dispensável
1	001	Segundo plano
2	010	Melhor esforço
3	011	Esforço excelente
4	100	Carga controlada
5	101	Vídeo
6	110	Voz
7	111	Gerenciamento de rede

Prioridade de IP, ToS e DSCP

No cabeçalho do pacote IP de uma mensagem IPv4, o campo de tipo de serviço (TOS) tem 8 bits.

O campo Tipo de Serviço (TOS) inclui um campo de prioridade IP de 3 bits, um campo TOS de 4 bits e um bit não utilizado (deve ser zero). Quatro bits TOS representam respectivamente: latência mínima, rendimento máximo, máxima confiabilidade e custo mínimo. Entre os quatro bits, no máximo um bit pode ser configurado ao mesmo tempo. Se os 4 bits forem 0, significa serviço geral.



Precedência IP e precedência TOS

(IP de origem; Tipo de serviço; Deve ser Zero).

Existem oito prioridades para a preferência em IP.

» Descrição dos valores de precedência de IP:

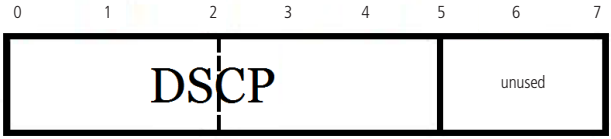
IP de origem (decimal)	IP de origem (binário)	Implicação
0	000	Rotina
1	001	Prioridade
2	010	Imediato
3	011	Flash
4	100	Sobrescrever a flash
5	101	Crítico
6	110	Internet
7	111	Rede

Origem do TOS possui 5 níveis.

» Descrição dos valores de TOS:

TOS (decimal)	TOS (binário)	Implicação
0	0000	Normal
1	0001	Mínimo custo
2	0010	Maior confiabilidade
4	0100	Throughput máximo
8	1000	Mínimo atraso

Logo depois, o RFC2474 redefine o domínio TOS do cabeçalho da mensagem IP, chamado domínio DS, onde a precedência DSCP é representada pelos primeiros 6 bits (0-5 bits) do domínio e o intervalo é de 0 a 63. Os primeiros 3 bits do DSCP são usados como seletores de classe, os bits 4 e 5 indicam a precedência de queda e o 6º bit é definido como 0 para indicar que o dispositivo é uma classe de serviço definida como o modelo DS. Os dois últimos bits são bits reservados.



Precedência DSCP

A rede Diffserv define quatro tipos de tráfego:

Classe de encaminhamento acelerado (EF), que é aplicável aos serviços de baixo atraso, baixa perda, baixo jitter e de largura de banda prioritária (como linhas virtuais alugadas), independentemente de outro tráfego compartilhar seu link.

A classe de encaminhamento garantido (AF) é dividida em quatro subcategorias (AF1/2/3/4). Cada classe AF é dividida em precedência de três largadas, que pode ser usada para classificar o negócio AF. As Classes AF têm nível QoS mais baixo que as classes EF.

O seletor de classe (CS) evolui a partir do campo IP TOS, possui um total de oito categorias.

O melhor esforço (BE) é uma categoria especial de CS, não há garantia. A classe AF pode ser rebaixada para a classe BE após a saturação, o tráfego de rede IP existente também é padronizado nesta categoria.

» Descrição de valor do DSCP:

DSCP (decimal)	DSCP (binário)	Palavra-chave
0	000000	be
46	101110	ef
10	001010	af1
18	010010	af2
26	011010	af3
34	100010	af4
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7

Obs.: *antes de configurar essas tarefas ACL, configure a licença ACL de acordo com seus requisitos.*

Consulte o Guia de Configuração da ACL.

14.2. Configuração de limite de velocidade de tráfego

O limite de velocidade baseado no tráfego pode monitorar a taxa de tráfego que entra no OLT. Se o tráfego exceder o limite configurado, são tomadas as medidas correspondentes, como deixar as mensagens que excedem o limite ou repor suas prioridades.

» Configuração de limite de velocidade de tráfego:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Acesse o modo de configuração de porta	**interface ethernet** device/slot/port	Opcional, o limite de velocidade do tráfego pode ser configurado sob o modo de global ou porta
Configuração de limite de velocidade de tráfego	**rate-limit { input | output } { [ip-group {** *num* **|** *name* **} [subitem** *subitem* **]] [link-group {** *num* **|** *name* **} [subitem** *subitem* **]] }** *target-rate*	Opcional, alguns dispositivos apenas suportam direção de entrada, alguns dispositivos suportam direção de entrada e saída

14.3. Configuração do trTCM

A função de trTCM é definida no RFC 2698, e principalmente com base em quatro tipos de parâmetros de fluxo: CIR, CBS, PIR, PBS.

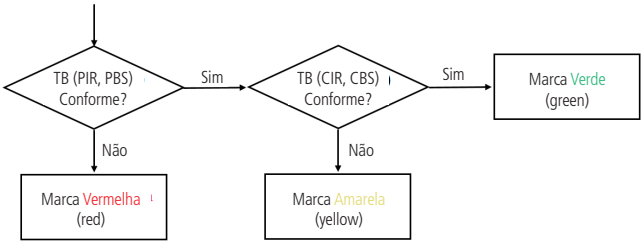
» Configuração do trTCM:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Configuração o modo de *color aware*	**two-rate-policer mode {color-aware | color-blind}**	Opcional
Diferentes mensagens DSCP são codificadas por cores	**two-rate-policer set-pre-color {***dscp-value* **{green | red | yellow}}**	Opcional

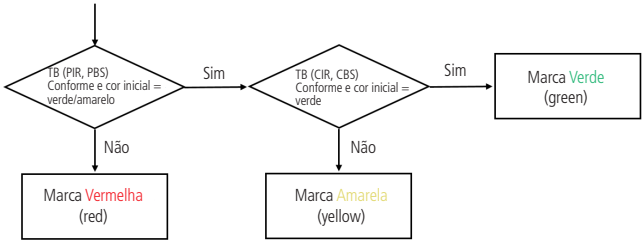
Operação	Comando	Obrigatório/ opcional
Configure uma política de aplicação de trTCM (ação de processamento para três mensagens de cores diferentes)	**rate-limit input{ [ip-group { num | name } [subitemsubitem]] [link-group { num | name } [subitemsubitem]] } two-rate-policer cir cir-value cbs cbs-value pir pir-value pbs pbs-value conform-action {copy-to-cpu | drop | set_dscp_value dscp_value |transmit } exceed-action {copy-to-cpu | drop | set_dscp_value dscp_value |transmit } violate-action{copy-to-cpu | drop | set_dscp_value dscp_value |transmit }**	Opcional

Obs.: *o modo* Color-aware *corresponde ao modo* Color-blind, *o padrão do sistema é o modo* Color-blind, *a diferença entre os dois é a seguinte:*

TrTCM em modo color-blind



TrTCM em modo Color-Aware



14.4. Configuração de redirecionamento de mensagem

O redirecionamento de mensagem significa que a mensagem encaminhada é redirecionada para uma porta de saída.

» Configurar o redirecionamento de mensagem:

Operação	Comando	Obrigatório/ Opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de redirecionamento de mensagem	**traffic-redirect { [ip-group {** num **|** name **} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]] } { [interface** interface-num **| cpu] }**	Opcional

14.5. Configuração de cópia de mensagem para a CPU

Depois que a mensagem de configuração é copiada para a função *CPU*, o OLT copia automaticamente uma mensagem específica para a CPU.

» Configuração da cópia da mensagem na CPU:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da cópia da mensagem na CPU	**traffic-copy-to-cpu { [ip-group {** num **|** name **} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]] }**	Opcional

14.6. Configuração de marcador de precedência

A função de marcador de precedência é uma estratégia de remarcar a prioridade para corresponder a mensagem ACL. A função de marcador de precedência pode observar a precedência de IP, a prioridade de ToS, DSCP e 802.1p da mensagem. Você também pode especificar a precedência local para essas mensagens que correspondem à ACL.

» Configuração do marcador de precedência:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do marcador de precedência	**traffic-priority { [ip-group {** num **|** name**} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]] } { [dscp** dscp-value **] [cos {** pre-value **| from-ipprec }] [local-precedence** pre-value **] }**	Opcional

Obs.: *se a precedência 802.1p e a precedência local forem especificadas, a opção usará a precedência 802.1p para colocar a mensagem na fila de saída da porta correspondente.*

14.7. Configuração das estatísticas de tráfego

A função de estatística do tráfego pode ser usada para coletar as correspondentes mensagens de regras ACL. A estatística é um valor acumulado que pode ser limpado por um comando. Se o usuário reconfigurar a estatística de tráfego, ela será desmarcada.

» Configuração das estatísticas de tráfego:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração das estatísticas de tráfego	**traffic-statistic { [ip-group {** num **|** name **} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]] }**	Opcional
Limpar as informações de estatísticas	**clear traffic-statistic { [all	[ip-group {** num **|** name **} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]]] }**	Opcional

14.8. Configuração para sobrescrever VLAN

A ID da VLAN configurada é reescrita pela VLAN-ID da regra ACL.

» Configuração para sobrescrever a VLAN da mensagem:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração para sobrescrever a VLAN da mensagem	**traffic-rewrite-vlan { [ip-group {** num **|** name**} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]] }** rewrite-VLAN -ID	Opcional

14.9. Configuração de inserção de VLAN

A regra ACL de correspondência de mensagens é inserida em uma VLAN externa. O VLAN-ID é o VID inserido. O valor da VLAN é a precedência da porta.

» Configurar a inserção de VLAN:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar a inserção de VLAN	**traffic-insert-vlan { [ip-group {** num **|** name**} [subitem** subitem **]] [link-group {** num **|** name **} [subitem** subitem **]] }** insert-VLAN -ID	Opcional

14.10. Visualização e manutenção de QACL

Operação	Comando	Obrigatório/ opcional
Visualização das configurações de QoS	**show qos-info all**	Opcional, pode ser executado em qualquer modo
Visualização de todas as estatísticas de QoS	**show qos-info statistic**	Opcional, pode ser executado em qualquer modo
Visualização dos parâmetros de cópia de mensagem para a CPU	**show qos-info traffic-copy-to-cpu**	Opcional, pode ser executado em qualquer modo
Visualização das configurações de espelhamento de tráfego	**show qos-info mirroed-to**	Opcional, pode ser executado em qualquer modo
Visualização das configurações do marcador de precedência	**show qos-info traffic-priority**	Opcional, pode ser executado em qualquer modo
Visualização dos parâmetros de redirecionamento	**show qos-info [traffic-redirect**	Opcional, pode ser executado em qualquer modo

Operação	Comando	Obrigatório/ opcional
Visualização da estatística de tráfego	**show qos-info traffic-statistic**	Opcional, pode ser executado em qualquer modo
Visualização das configurações de sobrescrever a VLAN	**show qos-info traffic-rewrite-vlan**	Opcional, pode ser executado em qualquer modo
Visualização das configurações de inserção de VLAN	**show qos-info traffic-insert-vlan**	Opcional, pode ser executado em qualquer modo
Visualização do trTCM	**show two-rate-policer** policer-id	Opcional, pode ser executado em qualquer modo
Visualização da configuração de taxa limite	**show qos-interface all**	Opcional, pode ser executado em qualquer modo
Visualização das informações de limite de taxa em todas as portas	**show qos-interface global rate-limit**	Opcional, pode ser executado em qualquer modo
Visualização das informações de limite de taxa em uma porta	**show qos-interface interface ethernet** port-id	Opcional, pode ser executado em qualquer modo
Estatísticas das regras de taxa limite	**show qos-interface statistic**	Opcional, pode ser executado em qualquer modo

» **show qos-info:** exibe as informações de configuração relacionadas à configuração de tráfego.

» **show qos-interface:** exibe as informações de configuração relacionadas ao limite de taxa.

14.11. Exemplo de configuração de QACL

» Requisitos e diagrama de rede:

A interconexão entre PCA e PCB é realizada através das portas Ethernet da OLT. A e B não pertencem ao mesmo segmento de rede. PCA se conecta no OLT através de Eth 0/1, e PCB se conecta no OLT através de Eth0/2.

PCB equipado com equipamento de detecção de dados. As necessidades específicas são as seguintes:

» Tráfego estatístico sem jornada de trabalho na Internet através do HTTP na porta E0/1.

» Redirecionar o tráfego através da porta E0/1 por HTTP para acessar a internet para E0/2.

O diagrama de rede é o seguinte:

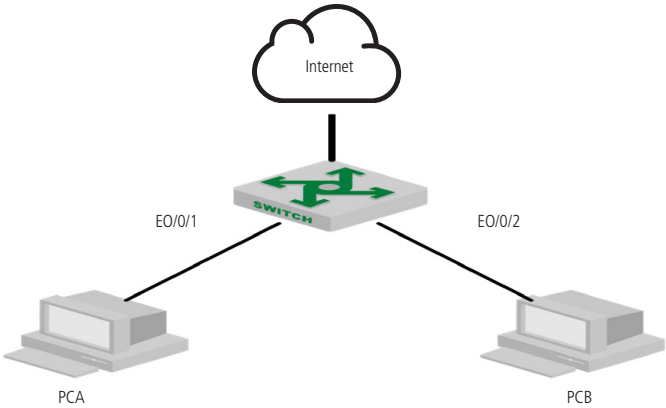


Diagrama de rede para configuração QACL

» Passos de configuração:

1. Configure o período de tempo

OLT4840E(config)#time-range a

OLT4840E(config-timerange-a)#periodic weekdays daily 08:30:00 to 18:00:00

OLT4840E(config)#time-range b

OLT4840E(config-timerange-b)#periodic weekdays 00:00:00 to 08:30:00

OLT4840E(config-timerange-b)#periodic weekend 00:00:00 to 23:59:00

2. Configure ACL, de acordo com o período de tempo diferente para acessar a Internet pela classificação de mensagens HTTP

   OLT4840E(config)#access-list 100 permit tcp any 192.168.0.1 0 80 time-range a

   OLT4840E(config)#access-list 100 permit tcp any 192.168.0.1 0 80 time-range b

3. Configurar o redirecionamento de tráfego e as estatísticas de trânsito

   OLT4840E(config)#traffic-statistic ip-group 100 subitem 0

   OLT4840E(config)#traffic-redirect ip-group 100 subitem 1 interface ethernet 0/2

15. Controle de Cos

15.1. Visão geral do controle do CoS

Quando a rede está congestionada, significa que muitas mensagens estão competindo por recursos ao mesmo tempo, problema que geralmente é resolvido por uma programação de fila. Os algoritmos comuns de agendamento de filas incluem SP, WRR, SP+WRR, WFQ e SP+WFQ.

O SP (*Strict-Priority Queuing*) foi projetado para aplicativos de negócios críticos. Uma característica importante do negócio crítico é priorizar os serviços para reduzir sua latência de resposta quando ocorre congestionamento. A fila de prioridade classifica todas as mensagens em oito classes (7, 6, 5, 4, 3, 2, 1, 0) e suas prioridades são reduzidas por cada uma delas.

Em sua programação, o SP envia estritamente uma fila de prioridade mais alta de acordo com a ordem definida. Quando a prioridade mais alta está vazia, o grupo da fila de prioridade mais baixa na fila é enviado. Desta forma, o negócio não crítico é colocado em fila de prioridade mais baixa, para garantir que o negócio-chave seja encaminhado, e apenas é transmitido na lacuna ociosa de manipulação de dados críticos.

A sua desvantagem é que mensagens de baixa prioridade podem não ser transmitidas por um longo período de tempo.

O agendamento da fila WRR divide cada porta em 8 filas de saída (7, 6, 5, 4, 3, 2, 1, 0 e suas prioridades são reduzidas em cada fila). Elas são agendadas e garantem que cada uma tenha um determinado tempo de serviço. O WRR pode ser configurado com um valor ponderado (w7, w6, w5, w4, w3, w2, w1, w0) para cada fila, representando o peso do recurso, como em uma porta de 100M, se o valor for configurado em 80, 70, 60, 50, 50, 40, 30, 20 (correspondentes a w7, w6, w5, w4, w3, w2, w1, w0, respectivamente).

Isso garante que a fila de prioridade mais baixa pode obter pelo menos 5 Mbit/s de largura de banda, evitando que mensagens em filas de baixa prioridade não fiquem tanto tempo sem transmitir como no SP.

Uma vantagem da fila WRR é que, embora várias filas sejam agendadas por polling, cada fila não recebe um intervalo fixo - se uma fila estiver vazia, ela muda imediatamente para o próximo cronograma da fila, portanto, a largura de banda pode ser totalmente utilizada.

Na programação da fila SP+WRR, se o valor de peso de uma fila for definido como 0, a fila executará o algoritmo de prioridade rígida (assim como no SP), caso contrário, é utilizado o valor de peso da fila WRR.

O WFQ utiliza o mesmo que o princípio WRR, a diferença é que o segundo usa pps e o WFQ usa bps para calcular o peso da fila. Em uma porta de 100M, configurada com o valor de agendamento da fila WFQ para 80, 70, 60, 50, 50, 40, 30, 20 (correspondendo a w7, w6, w5, w4, w3, w2, w1, w0, respectivamento), a fila de prioridade mais baixa é garantida para ter pelo menos uma largura de banda de 20 / (80+70+60+50+50+40+30+20) *% 100, onde a largura de banda é calculada usando bits/Bytes, por exemplo.

SP+WFQ também é calculado de acordo com o peso da fila Bps.

15.2. Configuração de controle de CoS

Configuração de controle de CoS

O agendamento de fila não possui alteração de função (habilitar / desativar), ele está habilitado por padrão e usa programação de SP (estrita prioridade).

Em SP+WRR ou SP+WFQ, uma fila com um peso de 0 usa SP e as outras filas são encaminhadas pelo peso WRR ou WFQ.

» Configuração de CoS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Utilizar a priorização por SP	**queue-scheduler strict-priority**	Opcional

Operação	Comando	Obrigatório/ opcional
Utilizar a priozação por WRR	**queue-scheduler wrr** w1 w2 w3 w4 w5 w6 w7 w8	Opcional
Utilizar a priorização por WFQ	**queue-scheduler wfq** w1 w2 w3 w4 w5 w6 w7 w8	Opcional
Utilizar a priorização por SP+WRR	**queue-scheduler sp+wrr** w1 w2 w3 w4 w5 w6 w7 w8	Opcional
Utilizar a priorização por SP+WFQ	**queue-scheduler sp+wfq** w1 w2 w3 w4 w5 w6 w7 w8	Opcional
Restaurar a priorização padrão	**no queue-scheduler**	Opcional
Visualização das informações	**show queue-scheduler**	Opcional

Obs.: *dispositivos suporta 8 filas.*

Configuração de 802.1p e mapeamento de fila de hardware

O sistema mapeia a prioridade 802.1p e da fila de hardware da mensagem. Para cada mensagem que entra no switch, o sistema mapeia a prioridade da fila de hardware de acordo com a prioridade 802.1p da mensagem. Por padrão, a relação de mapeamento entre 802.1p e prioridade de hardware é a seguinte:

802.1p	Fila de prioridade de hardware
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Ao alterar a relação de mapeamento entre prioridade 802.1p e filas de hardware, podemos alterar a relação de mapeamento entre prioridades 802.1p e as filas de saída.

Como a programação da fila de chip usa um algoritmo aleatório, se as duas prioridades 802.1p forem mapeadas para a mesma fila de prioridade de hardware, as mensagens de duas prioridades 802.1p não podem ser encaminhadas com o encaminhamento 1:1.

» Configuração de DSCP e mapeamento 802.1p:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da função de mapeamento DSCP	**[no] queue-scheduler dscp-map**	Opcional
Modificar o mapeamento dscp e 802.1p	**queue-scheduler dscp-map** dscp-v priority-v	Opcional
Visualização das informações de mapeamento DSCP	**show queue-scheduler dscp-map**	Opcional

15.3. Exemplo de configuração de COS

» Passos de configuração:

» Exiba o modo de priorização padrão:

OLT4840E(config)#show queue-scheduler

Queue scheduler status : enable

Queue scheduler mode : SP (Strict Priority)

» Exiba a relação de mapeamento de prioridade entre 802.1p e filas de hardware:

OLT4840E(config)#show queue-scheduler cos-map

Information about map of cos:

802.1P Priority Queue of class

---

0 0

1 1

2 2

3 3

4 4

5 5

6 6

7 7

Modifique a relação de mapeamento de prioridade entre 802.1p e filas de hard-

ware: pacotes com prioridade = 0 para fila 1, apenas para demonstração, o uso real é o valor padrão.

OLT4840E(config)#queue-scheduler cos-map 1 0

Config successfully.

OLT4840E(config)#show queue-scheduler cos-map

Information about map of cos:

802.1P Priority Queue of class

---

0 1

1 1

2 2

3 3

4 4

5 5

6 6

7 7

Utilize a priorização por WRR

OLT4840E(config)#queue-scheduler wrr 1 2 3 4 5 6 7 8

OLT4840E(config)#queue-scheduler wrr 1 2 3 4 5 6 7 8

Config queue scheduler successfully.

OLT4840E(config)#show queue-scheduler

Queue scheduler status : enable

Queue scheduler mode : WRR (Weighted Round Robin)

Queue0 weight is 1

Queue1 weight is 2

Queue2 weight is 3

Queue3 weight is 4

Queue4 weight is 5

Queue5 weight is 6

Queue6 weight is 7

Queue7 weight is 8

» Restaure as configurações de priorização padrão:
OLT4840E(config)#no queue-scheduler

Recover queue scheduler to default value(strict-priority) successfully.

OLT4840E(config)#show queue-scheduler

Queue scheduler status : enable

Queue scheduler mode : SP (Strict Priority)

16. Controle de encaminhamento

16.1. Controle de largura de banda

O controle de largura de é usada para limitar a taxa total de mensagens recebidas ou enviadas da porta.

Configuração de limite de largura de banda por porta

Na porta, configure o limite de largura de banda para a direção de entrada / saída da porta.

» Configure o limite de largura de banda para a porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Configuração de limite de largura de banda de saída da porta	**[no]bandwidth egress** rate	Opcional
Configuração de limite de largura de banda de entrada da porta	**[no]bandwidth ingress** rate	Opcional
Configuração de limite de largura de banda da porta baseada na fila de prioridade	**bandwidth queue** queue-id **{ maximum | minimum}** rate	Opcional
Cancelar o limite de largura de banda da porta baseada na fila de prioridade	**no bandwidth queue** queue-id **{ maximum | minimum** }	Opcional

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de controle de largura de banda baseado na CPU	**bandwidth cpu-queue** queue-id **{ maximum | minimum }** rate	Opcional
Cancelar o controle de largura de banda baseado na CPU	**no bandwidth cpu-queue** queue-id **{ maximum | minimum }**	Opcional

» Visualização e manutenção do limite de largura de banda:

Operação	Comando	Obrigatório/ opcional
Visualização do limite de largura de banda da porta	**show bandwidth-control interface [ethernet** port-number **]**	Opcional
Visualização do limite de largura de banda da porta baseada na fila de prioridade	**show bandwidth queue interface [ethernet** port-number **]**	Opcional
Visualização da largura de banda baseado na CPU	**show bandwidth cpu-queue**	Opcional

Exemplo de configuração de controle de largura de banda

» Requisitos de rede:

» Defina a velocidade de entrada da porta 1 a 1024 (1M).

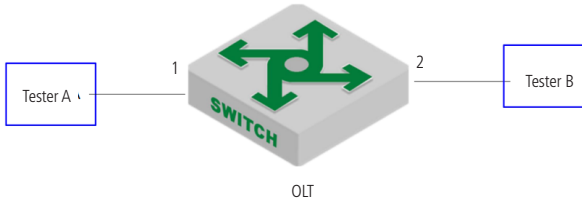


Diagrama esquemático de controle de largura de banda

» Passos de configuração:

» Configure o controle de largura de banda:

OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#bandwidth ingress 1024
OLT4840E(config-if-ethernet-0/1)#exit

» Exiba as informações de configuração:
OLT4840E(config)#show bandwidth-control interface ethernet 0/1
port Ingress bandwidth control Egress bandwidth control
e0/1 1024 kbps disable
Total entries: 1.

16.2. Função de storm-control

A função *Storm-Control* é implementada no modo de configuração da porta. Ou seja, o administrador pode definir diferentes políticas de storm control para diferentes portas.

» Configuração do Storm-control:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** device/slot/port	-
Configuração do tipo de mensagem de storm-control e o limiar de supressão	**Storm-control {broadcast |multicast |unicast}** target-rate	Opcional

Visualização e manutenção de storm-control

Depois de completar a configuração acima, você pode usar o seguinte comando para visualizar a configuração.

» Visualização e manutenção de Storm-control:

Operação	Comando	Obrigatório/ opcional
Visualização do tipo de mensagem de storm-control e e o limiar de supressão	**show interface ethernet** device/slot/port	Executável em todos os modos

Exemplo de configuração de storm-control

» Ative o storm-control na porta 1 e defina o valor de transmissão broadcast para 128 pps, o valor transmissão de multicast desconhecido para de 256 pps e o valor de transmissão unicast (um alto volume de unicast) desconhecido para de 512 pps.

OLT4840E(config)# interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#storm-control broadcast 128

OLT4840E(config-if-ethernet-0/1)#storm-control multicast 256

OLT4840E(config-if-ethernet-0/1)#storm-control unicast 512

» Exiba as informações de status do storm-control.

OLT4840E(config-if-ethernet-0/1)#show interface ethernet 0/1

Ethernet e0/5 is enabled, port link is down

Hardware address is 00:00:53:28:00:0a

SetSpeed is auto, ActualSpeed is unknown, Duplex mode is unknown

Current port type: 1000BASE-T

Priority is 0

Flow control is disabled

Broadcast storm control target rate is 128Kbps

Multicast storm control target rate is 256Kbps

Unicast storm control target rate is 512Kbps

PVID is 1

Port mode: hybrid

Untagged VLAN ID : 1

Input : 0 packets, 0 bytes

0 broadcasts, 0 multicasts, 0 unicasts

Output : 0 packets, 0 bytes

0 broadcasts, 0 multicasts, 0 unicasts

17. Proteção contra ataques

17.1. Função Antiataque DOS

O ataque DOS é um método de ataque simples e eficaz, muito prejudicial para muitas tecnologias de rede. Ele utiliza vários meios para consumir largura de banda da rede e recursos do sistema, ou atacar defeitos do sistema, de modo que o serviço é paralisado e não pode atender o usuário normalmente (consegue negar o acesso aos usuários). Configure o ataque anti-TTL.De acordo com o padrão, o campo TTL no cabeçalho IP deve ser maior que 0. Por padrão, se a mensagem de TTL = 0 for recebida, a opção descarta a mensagem como um ataque, mas permite que a mensagem de TTL = 0 seja descartada.

Antiataque TTL

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o antiataque TTL	**anti-dos ip ttl**	Opcional, por padrão *as mensagens com TTL = 0 são descartadas*
Desabilitar o antiataque TTL	**no anti-dos ip ttl**	Opcional, após a configuração, as mensagens normais serão processadas
Visualização das informações da configuração	**show anti-dos**	Opcional

Configuração de antiataque por fragmentos

Se o número de fragmentos de mensagem IP for grande, o OLT ocupará muitos recursos do sistema e poderá afetar outras mensagens. Portanto, um limite razoável para o comprimento da mensagem IP não permite muitos fragmentos. Se exceder o valor especificado, a mensagem será descartada como uma mensagem de ataque. Por padrão, uma mensagem IP possui 800 fragmentos.

» Configuração do antiataque por fragmento IP:

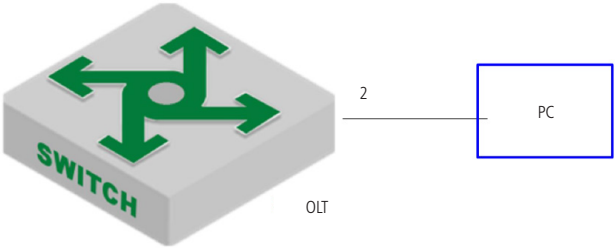
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Definir o número máximo de mensagens IP permitido	**[no]anti-dos ip fragment** maxnumbers	Opcional, não existe comando de restauração para o valor inicial de *800*
Visualização das informações de configuração	**show anti-dos**	Opcional

Exemplo de configuração

» Requisitos de rede:

O PC se conecta diretamente ao OLT. Verifique se o OLT manipula mais do que o número de fragmentos permitidos e o fragmento normal, respectivamente.

OLT: ip = 10.5.2.134; PC IP = 10.5.2.91



» Passos de configuração:

» Configure uma mensagem IP para ter até dois fragmentos:

OLT4840E(config)#anti-dos ip fragment 2

» OLT precisa de dois fragmentos da mensagem IP, você pode se comunicar corretamente.

OLT4840E (config)#ping -l 2800 10.5.2.91

PING 10.5.2.91: with 2800 bytes of data:

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

----10.5.2.91 PING Statistics----

5 packets transmitted, 5 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

» OLT precisa de três fragmentos da mensagem IP, você não pode se comunicar.

OLT4840E(config)#ping -l 3000 10.5.2.91

PING 10.5.2.91: with 3000 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

no answer from 10.5.2.91

» Remova a configuração de fragmentação IP (restaure o valor padrão de 800) e em seguida envie três partes de mensagens IP, a comunicação é normal.

OLT4840E(config)#no anti-dos ip fragment

OLT4840E(config)#ping -l 3000 10.5.2.91

PING 10.5.2.91: with 3000 bytes of data:

reply from 10.5.2.91: bytes=3000 time=10ms TTL=64

reply from 10.5.2.91: bytes=3000 time<10ms TTL=64

reply from 10.5.2.91: bytes=3000 time=10ms TTL=64

reply from 10.5.2.91: bytes=3000 time<10ms TTL=64

reply from 10.5.2.91: bytes=3000 time<10ms TTL=64

----10.5.2.91 PING Statistics----

5 packets transmitted, 5 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/4/10

17.2. Função de CPU-car

Um grande número de mensagens na CPU fará com que ela fique ocupada. Esta função é usada para limitar a taxa de recepção de mensagens pela CPU.

Configuração do CPU-car

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da taxa de CPU-car	**[no] cpu-car** value	Opcional, não existe comando de restauração para o valor inicial de *400pps*
Visualização das informações de configuração	**show anti-dos**	Opcional
Visualização das estatísticas de pacotes recebidos na porta	**show cpu-statistics [ethernet** port-number**]**	Opcional
Limpar as estatísticas de pacotes recebidos na porta	**clear cpu-statistics**	Opcional
Visualização das estatísticas de classificação de pacotes	**show cpu-classification [interface ethernet** port-number**]**	Opcional
Limpar as estatísticas de classificação de pacotes	**clear cpu-classification [interface ethernet** port-number**]**	Opcional
Visualização da utilização da cpu	**show cpu-utilization**	Opcional

Exemplo de configuração

» Requisitos de rede:

Limite a taxa de mensagem para menos de 50 pps no OLT.

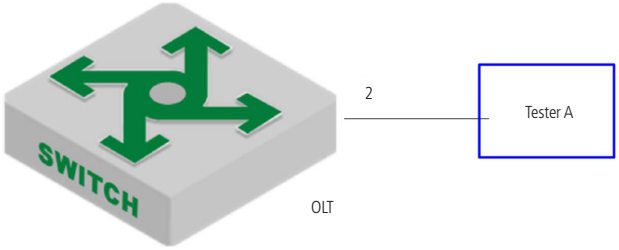


Diagrama de CPU-car

» Passos de configuração:

» Configure a velocidade do CPU-car para 50pps.

OLT4840E(config-if-ethernet-0/2)#port-car-rate 50

» Exiba as configurações:

OLT4840E(config)#show cpu-car

Send packet to cpu rate = 50 pps.

» Validação de resultados:

» Tester A envia mensagens de solicitação icmp para o OLT a uma taxa de 100 pps por 10 segundos, o número total de mensagens no OLT é 600, indicando que a função cpu-car funciona.

OLT4840E(config)#clear cpu-statistics

OLT4840E(config)#clear cpu-classification

OLT4840E(config)#clear interface

OLT4840E(config)#show cpu-statistics ethernet 0/2

Show packets sent to cpu statistic information

port 64Byte 128Byte 256Byte 512Byte 1024Byte 2048Byte

e0/2 600 0 0 0 0 0

OLT4840E(config)#show cpu-classification

Type	Count	Percent(%)
Total	600	100
BPDU	0	0
ERRP	0	0
ARP	0	0
MLD	0	0
IGMP	0	0
ICMP	600	100
OSPF	0	0
RIP	0	0
DHCP	0	0
SNMP	0	0
Telnet	0	0
PIM	0	0
BGP	0	0
SSH	0	0
Other	0	0

OLT4840E(config)#show statistics interface ethernet 0/2

Port number : e0/2

last 5 minutes input rate 5248 bits/sec, 10 packets/sec

last 5 minutes output rate 433832 bits/sec, 771 packets/sec

64 byte packets:1048

65-127 byte packets:0

128-255 byte packets:0

256-511 byte packets:0

512-1023 byte packets:0

1024-1518 byte packets:0

1048 packets input, 67072 bytes , 0 discarded packets

1048 unicasts, 0 multicasts, 0 broadcasts

0 input errors, 0 FCS error, 0 symbol error, 0 false carrier

0 runts, 0 giants

19 packets output, 1215 bytes, 0 discarded packets

0 unicasts, 9 multicasts, 10 broadcasts

0 output errors, 0 deferred, 0 collisions

0 late collisions

Total entries: 1.

17.3. Função de shutdown-control

Quando a rede está em loop ou recebe um ataque malicioso, muitas mensagens serão enviadas, elas desperdiçam largura de banda ou até geram um colapso na borda que afetará o uso normal de outros usuários. A função de shutdown-control é usada para evitar mensagens excessivas na rede. Ele monitora a largura de banda de cada porta no OLT. Quando o número de mensagens desconhecidas recebidas pela porta excede a segurança definida pelo administrador, a função de shutdown-control desliga automaticamente a porta para garantir que os outros links e dispositivos estejam protegidos do impacto na rede.

Habilite/desabilite o shutdown-control

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** port-num	-
Habilitar e configurar a taxa para shutdown	**shutdown-control {broadcast |multicast | unicast}** rate	Obrigatório
Função de shutdown	**no shutdown-control {**broadcast |multicast | unicast**}**	Opcional
Visualização das informações de configuração	**show shutdown-control interface** [ethernet port-numer]	Opcional

Configuração do modo de restauração

Se a porta está desligada e precisa restaurar seu padrão manualmente. Os administradores podem configurar a recuperação automática e definir o ciclo de recuperação, o padrão é *480s*.

» Configurar o modo de restauração:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do modo de restauração	**[no] shutdown-control-recover mode** {automatic | manual}	Opcional
Configuração do período de restauração automática	**[no] shutdown-control-recover automatic-open-time** value	Opcional, por padrão é definido em *480s*, apenas válido para restauração automática
Visualização das informações de configuração	**show shutdown-control interface [ethernet** port-number **]**	Opcional

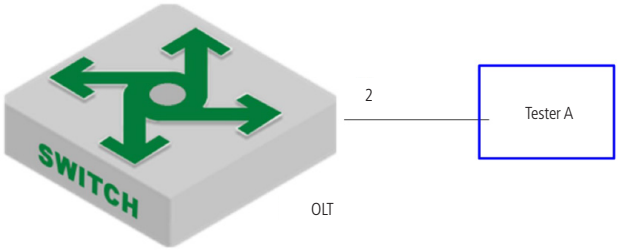
» Restauração manual de porta desligada:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	Obrigatório
Comando para desligar uma porta	**shutdown**	Obrigatório
Restauração da porta	**no shutdown**	Obrigatório

Exemplo de configuração

» Requisitos de rede:

A porta 2 que recebe taxa de unicast desconhecida é limitada para 1000pps, se for desligada, recupera automaticamente após 480s (valor padrão) é usado para o ciclo de recuperação.



Mapa de shutdown control

» Passos de configuração:
  » Ative a função de shutdown-control para unicast desconhecido e defina a taxa para 1000 pps.

  OLT4840E(config)#interface ethernet 0/2

  OLT4840E(config-if-ethernet-0/2)#shutdown-control unicast 1000

  OLT4840E(config-if-ethernet-0/2)#ex

  #Exiba as informações de configuração

  OLT4840E(config)#show shutdown-control interface ethernet 0/2

  port shutdown control recover mode : automatic

  Port recover time(second) : 480

  port shutdown control information :

  PortID Broadcast Broadcast Multicast Multicast Unicast Unicast RemainTime

  status value status value status value

  e0/2 disable - disable - enable 1000 -

  Total entries: 1

» Validação de resultados:

  OLT4840E(config)#logging monitor 0

  The tester sends an unknown message to the OLT 0/2 at a rate of 1100 pps.

  OLT4840E(config)#05:12:04: Switch: %DEVICE-3-LINKUPDOWN: e0/2 LinkDown.

  05:12:04: Switch: %OAM-5-SHUTDOWN-CTRL: port e0/2 was shutdown.

OLT4840E(config)#show shutdown-control interface ethernet 0/2

port shutdown control recover mode : automatic

Port recover time(second) : 480

port shutdown control information :

PortID Broadcast Broadcast Multicast Multicast Unicast Unicast RemainTime

status value status value status value

e0/2 disable - disable - enable 1000 07min48sec

Total entries: 1 .

OLT4840E(config)#show interface brief ethernet 0/2

Port Desc Link shutdn Speed Pri PVID Mode TagVlan UtVlan

e0/2 downERROR auto 0 1 hyb 1

Total entries: 1 .

OLT4840E(config)#05:20:06: Switch: %DEVICE-3-LINKUPDOWN: e0/2 LinkUp.

05:20:08: Switch: %OAM-5-PORTRECOVER: port e0/2 recover.

17.4. Antiataque DHCP

Normalmente, quando o cliente DHCP obtém o IP do servidor DHCP, a taxa de mensagem DHCP enviada pelo cliente DHCP é muito pequena. Geralmente, não causa probelmas ao servidor DHCP. No entanto, um invasor mal-intencionado pode enviar mensagens DHCP em altas taxas para o servidor, causando a sua queda, afetanado a alocação de IP para outros clientes.

A função Antiataque DHCP restringe a taxa de mensagem DHCP do cliente DHCP. O cliente com taxa excessiva será considerado como mal-intencionado, de modo a proteger o servidor DHCP para funcionar normalmente.

Habilitar/desabilitar o anti-DHCP

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o anti-DHCP	**[no] dhcp anti-attack**	Obrigatório, *desligado* por padrão

Operação	Comando	Obrigatório/ opcional
Visualização das informações de configuração	**show dhcp anti-attack [ethernet** port-number **]**	Opcional

Configuração de regras de processamento

Após o OLT detectar um ataque, ele pode tomar duas ações: 1) Descartar todas as mensagens do cliente (com base no endereço MAC de origem das mensagens) 2) Descartar apenas a mensagem DHCP do cliente (de acordo com o MAC de origem Endereço da mensagem), ou seja, o cliente não receberá IP.

Quando o OLT detecta um ataque, ele envia o endereço MAC da mensagem para o registro de ataque. Se a política está definida para descartar todos os pacotes, o usuário pode vincular manualmente o registro de ataque ao endereço MAC de blackhole.

» Configuração de regras de processamento:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração das regras de processamento	**dhcp anti-attack action [deny-all | deny-dhcp]**	Opcional, *Deny-DHCP* por padrão
Associar a tabela MAC de blackhole	**dhcp anti-attack bind blackhole [all | mac-address]**	Opcional, ele pode ser configurado somente quando *Deny-All* está especificado
Visualização das informações de configuração	**show dhcp anti-attack [ethernet** port-number **]**	Opcional

Configuração do limite de taxa

No antiataque DHCP, a taxa de mensagem DHCP enviada pelo mesmo usuário determina se existe um ataque. Se a taxa for igual ou superior a 16 pps, a mensagem será considerada como um ataque.

O administrador tem permissão para modificar o limite de taxa.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração dao limite de taxa	**[no] dhcp anti-attack threshold** value	Opcional, *16pps* por padrão
Visualização das informações de configuração	**show dhcp anti-attack [ethernet** port-number **]**	Opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Configuração do limite de taxa	**[no] dhcp anti-attack threshold** value	Opcional

Configuração da função de restauração

Quando o OLT detecta um ataque, ele envia o endereço MAC fonte da mensagem para a tabela de ataque. A tabela de ataque possui um tempo de validade. Quando o tempo de validade expira, o item da tabela é excluído. O tempo de validade padrão é de *10 minutos*. Se você não deseja excluir um item da tabela, você pode configurar o tempo como *0*.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Visualização das informações de configuração	**show dhcp anti-attack [ethernet** port-number **]**	Opcional, também visualiza a tabela de ataque
Configuração do tempo de restauração	**dhcp anti-attack recover-time** value	Opcional, por padrão é valor é de *10 m*, 0 significa que não haverá o envelhecimento
Configuração da restauração manual	**interface ethernet** port-number	-

Configuração de porta confiável

Por padrão, todas as portas são consideradas não confiáveis após o antiataque DHCP global estar habilitado e você precisa monitorar se o ataque DHCP existe ou não. Se a porta não possuir um ataque DHCP, você pode modificá-la para uma porta de confiança. Então, você não precisa monitorar se há ataque ou não.

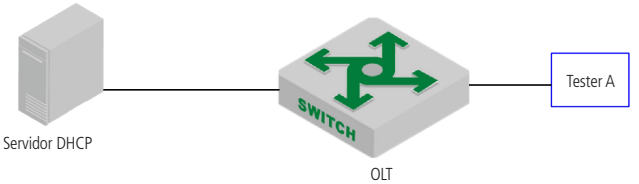
» Configuração de porta confiável:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de porta para porta confiável	**[no]dhcp anti-attack trust**	Opcional, todas as portas não são confiáveis por padrão
Visualização das informações de configuração	**show dhcp anti-attack interface ethernet** port-number	Opcional

Exemplo de configuração

» Requisito de rede:

Habilitada a função Anti-DHCP na OLT. Tester A emula o PC para enviar a mensagem DHCP. Para demonstrar o efeito, configure o limite de taxa de ataque Anti-DHCP para 1pps e ative a função de recuperação automática.



Antiataque DHCP

» Exemplo de configuração:

» Configure ataque anti-DHCP:

OLT4840E(config)#dhcp anti-attack

OLT4840E(config)#dhcp anti-attack action deny-dhcp

OLT4840E(config)#dhcp anti-attack threshold 1

OLT4840E(config)#dhcp anti-attack recover-time 3

» Exiba as informações de log:
OLT4840E(config)#logging monitor 0

OLT4840E(config)#debug dhcp

» Validação de resultados:

» O Tester A solicita dhcp a uma taxa de 2pps. A informação do log será a seguinte:
OLT4840E(config)#

05:26:56: Switch: %DHCP-4-DHCP: 19616:33: Deny user 00:00:00:01:11:23,dhcpRate 2pps

05:26:58: Switch: %DHCP-4-DHCP: 19618:33: Deny user 00:00:00:01:11:23,dhcpRate 2pps

» Envie o registro do ataque
OLT4840E(config)#show dhcp anti-attack

Dhcp anti-attack: enabled

Dhcp rate limit:1pps

User recovery time:3 minutes

Reject type:DenyDHCP

DeniedSrcMAC Port Vlan DenyType RemainAgingTime(m)

00:00:00:01:11:23 e0/1 2 DenyDHCP 3

Total entry: 1.

» Após 3 minutos o registro perde a validade
OLT4840E(config)#show dhcp anti-attack

Dhcp anti-attack: enabled

Dhcp rate limit:1pps

User recovery time:3 minutes

Reject type:DenyDHCP

DeniedSrcMAC Port Vlan DenyType RemainAgingTime(m)

Total entry: 0.

17.5. ARP-Spoofing e Flood Attack

Visão geral de ARP-Spoofing

Se dois hosts precisam se comunicar, eles devem conhecer o endereço MAC um do outro. O protocolo ARP torna esse procedimento transparente para os usuários. No entanto, não há instruções de certificação no protocolo ARP, que se torna vulnerável à ataques como consequência.

Todos os dispositivos na LAN podem receber o pedido ARP do host A, então, se o host C for um invasor, ele finge ser o host B para enviar a resposta do ARP para o host A *meu endereço é 00:00:00:00:03*, O host A irá acreditar nessa resposta e depois adicioná-la a tabela ARP. No entanto, o IP desta tabela é 192.168.1.4 enquanto o MAC correspondente é 00:00:00:00:03. Portanto, o host C pode interceptar e capturar a mensagem que deve ser enviada para o host B. Devido ao host A estar tratando com uma falsa tabela ARP, isso também é chamado de ataques de falsificação de ARP.

Depois de ativar esta função, todos os ARP que passarão pelo OLT serão redirecionados para a CPU para uma verificação. Os pacotes ARP serão verificados um por um se eles correspondem a tabela ARP estática, a tabela de ligação estática ip-source-guard e a tabela DHCP-snooping. Se passar pela inspeção de acompanhamento este pacote ARP pode ser transmitido. Se não passar pela inspeção o pacote será tratado de acordo com a estratégia configurada: descartar ou Flood (enviar para todas as portas), a função de ataque Anti-ARP-Spoofing vem desativada por padrão.

Visão geral de ataque por ARP-Flooding

O ataque de flooding do ARP aproveita esta falha do mecanismo ARP, enviando aleatoriamente muitos pacotes ARP para atacar o equipamento na rede local (LAN).

O objetivo principal do invasor da ARP é impactar a CPU do equipamento da rede e em seguida, esgotar os recursos da CPU do equipamento do core. O OLT deve julgá-lo antes do tempo e proibir a transmissão do pacote de inundação de modo a defender ataques deste tipo.

A função *ARP Anti-Flooding* pode identificar cada fluxo de ARP e em seguida, avaliar se é um ataque de flooding ARP de acordo com o valor de taxa ARP configurado. O OLT tomará como ataque de flooding se o tráfego ARP de um determinado host exceder o valor de taxa ARP configurada, ele colocará este host na lista negra para proibir a transmissão de seus pacotes.

Para facilitar o gerenciamento e a manutenção dos administradores de rede, ele pode ser capaz de executar auto-protect e salvar mensagens de aviso relevantes. Quanto aos usuários que foram proibidos, o administrador pode configurá-los como: recuperação manual ou recuperação automática.

O processo no OLT é o seguinte:

1. Habilite a função *Anti-Flood* do ARP, informe o pacote ARP para a CPU, identifique o fluxo diferente de acordo com o endereço MAC de origem do pacote ARP;
2. Configure a taxa ARP. O OLT tomará como ataque ARP se a taxa exceder o valor de limite configurado;
3. Se você selecionar o comando de Deny-All (negar todos), quando um tráfego de ARP exceder o valor de limite configurado, o OLT colocará este endereço MAC na lista de endereços de blackhole e proibirá a transmissão de todos pacotes com esse endereço de origem;
4. Se você selecionar o comando Deny-ARP (negar ARP), quando um tráfego exceder o valor limite configurado, o OLT proíbira apenas os pacotes ARP com esse endereço de origem;
5. Quanto à recuperação das mensagens que estão proibidas de serem encaminhadas, o administrador pode configurar o tempo de recuperação como recuperação automática ou recuperação manual.

Configuração de Anti-Spoofing

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o Anti-Spoofing ARP	**arp anti-spoofing**	Obrigatório
Desabilitar o Anti-Spoofing ARP	**no arp anti-spoofing**	Opcional

Operação	Comando	Obrigatório/ opcional
Configuração da abordagem de mensagem desconhecida: descartar o Flood	**arp anti-spoofing unknown {diacard | flood}**	O pacote ARP desconhecido refere-se ao IP desses pacotes ARP que não correspondem a nenhum item das opções da tabela estática do ARP, da tabela IP-soure-guard e da tabela DHCP-Snooping. Em outras palavras, este IP não existe em nenhuma tabela.

Configuração de proteção de host

A configuração de proteção de host significa que ao vincular IP+porta, esse IP só poderá gerar Flood para outras interfaces através dessa porta. Se o pacote ARP deste IP acessar de outras portas, ele será descartado.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o Anti-Spoofing ARP	**arp anti-spoofing**	Obrigatório
Configuração do modo de processo de descarte da mensagem ARP desconhecida	**arp anti-spoofing unknown flood**	Obrigatório
Configuração da proteção de host	**host-guard bind ip** *ipaddress* **interface ethernet** *device/slot/port*	Obrigatório
Remover porteção de host	**no host-guard bind { ip** *ipaddress*| **interface ethernet** *device/slot/port* **}**	

Configuração de inspeção de consistência de MAC

Quando existe um determinado pacote de ataque ARP, o MAC no pacote de dados Ethernet é diferente do MAC de origem no pacote ARP. Depois de ativar a inspeção de consistência de origem-MAC, o OLT irá verificar se o endereço MAC de origem do pacote Ethernet é o mesmo no pacote ARP. Se não forem iguais, o OLT descartará o pacote.

Esta função está desativada por padrão.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o Anti-Spoofing ARP	**arp anti-spoofing**	Obrigatório
Habilitar a inspeção de consistência	**arp anti-spoofing valid-check**	Obrigatório
Desabilitar a inspeção de consistência	**no arp anti-spoofing valid-check**	Opcional

Configuração do Anti-Gateway-Spoofing

O equipamento não pode atuar como gateway, mas pode ser capaz de configurar uma lista de de gateway corretos (IP+MAC). Se algum dispositivo na LAN tentar simular ser o gateway através de mensagens ARP, o OLT descartará estes pacotes depois de comparar com a lista configurada e identificar que o MAC é de um invasor.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o Anti-Spoofing ARP	**arp anti-spoofing**	Obrigatório
Habilitar o Anti-Spoofing	**arp anti-spoofing deny-disguiser** ipadress mac	Obrigatório
Desabilitar o Anti-Gateway-Spoofing	**no arp anti-spoofing deny-disguiser**	Opcional

Configuração de porta confiável

A porta confiável não executará uma verificação de ataque e spoof quando receber a mensagem ARP.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** device/slot/port	-
Configuração de porta confiável	**arp anti trust**	Opcional,*não confiável* por padrão
Restaurar padrão não confiável	**no arp anti trust**	Opcional

Configuração de antiataque Flood

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o *Anti-Flood*	**arp anti-flood**	Obrigatório
Desabilitar o *Anti-Flood*	**no arp anti-flood**	Opcional
Configuração do limite de segurança	**arp anti-flood threshold** threshold	Opcional, por padrão o limite é de *16pps*
Configuração do processamento de ataque do dispositivo	**arp anti-flood action {deny-arp|deny-all}**	Opcional, por padrão ele utilizará o *Deny_ARP*

Operação	Comando	Obrigatório/ opcional
Configuração do tempo de restauração de usuário banido	**arp anti-flood recover-time** time	Opcional. Intervalo de tempo configurável é <0-1440> minutos. Se você definir o valor como sendo 0, significa que deve ser restaurado manualmente. Por padrão, o tempo de recuperação é de 10 *minutos*.
Voltar a encaminhar pacotes de um usuário banido	**arp anti-flood recover {**H:H:H:H:H:H **| all}**	Opcional
Víncule o blackhole dinâmico com o blackhole estático	**arp anti-flood bind blackhole {**H:H:H:H:H:H **| all}**	Opcional, somente quando o modo de processamento é *Deny-All*
Acesse o modo de configuração de portas	**interface ethernet** device/slot/port	-
Configuração do limite para a porta	**arp anti-flood threshold** threshold	Opcional, funciona apenas se o limite da porta for menor que o limite global

Visualização e manutenção

Operação	Comando	Obrigatório/ opcional
Visualização das configurações de Anti-Spoofing ARP	**show arp anti-spoofing**	Opcional
Visualização das configurações de Anti-Flood e lista de dispositivos mal intencionados	**show arp anti-flood**	Opcional
Visualização do status da interface	**show arp anti interface**	Opcional

Exemplo de configuração de Anti-Spoofing ARP

» Requisitos de rede:

Conforme exibido na figura, a porta Eth 0/1 porta se conecta ao servidor DHCP, porta Eth 0/2 e a porta Eth 0/3 se conectam ao Cliente A e B, respectivamente. Além disso, essas três portas estão voltadas para a VLAN 1.

Habilite DHCP-Snooping, configure a porta Eth 0/1 como a porta de confiança do DHCP-Snooping para habilitar o Anti-ARP-Spoofing.

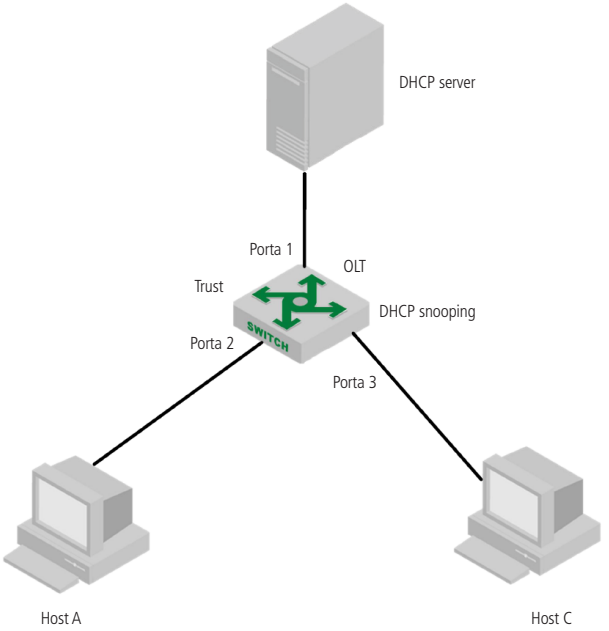


Diagrama de rede

» Etapas de configuração:
  » Habilitar DHCP-Snooping:
  OLT4840E(config)#dhcp-snooping
  » Defina a porta Ethernet 0/1 como a porta de confiança do DHCP-Snooping
  OLT4840E(config-if-ethernet-0/1)#dhcp-snooping trust
  Config DHCP-Snooping mode of port successfully.
  » Tabela de vínculo de IP-soure-guard
  OLT4840E(config)#ip-source-guard bind ip 192.168.5.10 mac 40:16:9f:f2:75:a8 in terface ethernet 0/3 vlan 1
  Add ip-source-guard bind entry successfully.

» Ativar função *Anti-ARP-Spoofing*

OLT4840E(config)#arp anti-spoofing

OLT4840E(config)#arp anti-spoofing unknown discard

OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#arp anti trust

Cliente A DHCP obtém IP para formar a tabela de clientes DHCP-Snooping.

O cliente A encaminha a mensagem ARP para DHCP-Server, DHCP-Server pode receber esta mensagem.

Cliente B configurado como static ip = 192.168.5.10, MAC = 40:16:9f:f2:75:a8. Cliente B encaminha a mensagem ARP para o DHCP-Server, que pode receber esta mensagem de ARP.

Se o cliente B habilitar o Anti-ARP-Spoofing, fonte IP da mensagem ARP = Cliente A, o equipamento descartará a mensagem se considerar que esta é uma mensagem falsa.

Esta instância estima se esta mensagem ARP é falsa ou não de acordo com a tabela de clientes do DHCP-Snooping, tabela de bind ip-soure-guard ou tabela ARP estática.

18. Single Spanning Tree

18.1. Introdução ao STP

O single spanning tree inclui o spanning tree (STP) e rápido spanning tree (RSTP).

Aplicação prática de STP

STP é uma parte do protocolo de bridging IEEE802.1D, sua principal função é evitar o loop de topologia de camada 2.

Unidade de dados do protocolo Bridge

Para executar o STP, o usuário precisa compartilhar informações entre OLTs. A informação compartilhada é a unidade de dados do protocolo bridge, que é enviada sob a forma de informações de multicast e apenas outros dispositivos de camada 2 podem ouvi-la. O OLT aprende a topologia de rede usando o BPDU: as conexões entre os dispositivos e e se existem certos loops na rede.

Se loops forem encontrados, o OLT desativa uma ou algumas das portas para garantir que estes loops na rede sejam eliminados. Ou seja, em uma rede, apenas um caminho está disponível de um dispositivo para qualquer outro. Se houver alguma alteração na rede, como uma queda de link, novos links adicionados, novo OLT adicionado ou falha em um OLT, o OLT na rede compartilha essas informações, o que faz com que o algoritmo STP produza uma nova topologia.

Conceitos básicos de STP

Bridge root

Depois que o algoritmo STP é executado, o primeiro passo é eleger o root OLT. O OLT de root está no topo da topologia da spanning tree. O OLT com o ID mais baixo é selecionado como o root. O ID consiste em duas partes:

» A prioridade do OLT. Por padrão, é *32.768*.

» O endereço MAC do OLT.

O administrador pode especificar um OLT como root anterando o seu ID. Quando a topologia de rede muda, quando há uma falha no root ou um novo OLT é adicionado à rede, o processo de eleição de OLT root é reiniciado.

Porta de root

Você também precisa selecionar a porta mais próxima do OLT root em todos os OLT que não são root para se comunicarem com ele.

Bridge designada

Em cada LAN individual existe um OLT chamado de bridge designada, que pertence à bridge de menor custo de caminho para a root LAN. Um OLT root é uma bridge elegida para todas as LANs às quais está conectado.

Porta designada

Depois de eleger o OLT de root e a porta root, você precisa escolher uma porta para alcançar o OLT root em cada link, que é a porta designada. Especificar uma porta requer as seguintes condições:

» Em dois OLTs de um link, serão selecionadas as portas no OLT que têm o menor custo do trajeto acumulado para o OLT root. Se o custo acumulado dos dois OLTs for o mesmo, será selecionado o OLT com o ID mais baixo.

» Se vários links no mesmo OLT estiverem conectados ao OLT root, a porta OLT com a prioridade mais baixa é selecionada como a porta designada. Se as prioridades forem iguais, será selecionada a porta com o número mais baixo como a porta designada.

18.2. Introdução ao RSTP

Rapid Spanning Tree Protocol é uma versão otimizada do protocolo STP. *Rápido* significa que, quando uma porta é selecionada como uma porta root e uma porta designada, o atraso para a entrada no estado de reencaminhamento é encurtado em certas condições, o que reduzirá o tempo necessário para que a rede atinja a estabilidade.

- **A condição para a transição rápida da porta root é:** a porta root antiga no dispositivo parou de encaminhar e a porta a de upstream começou a encaminhar dados.
- **A condição para a transição rápida de porta específica é:** a porta é uma porta de borda ou está conectada a um link ponto a ponto. Para o primeiro caso, a porta pode entrar diretamente no estado de encaminhamento. Já no segundo, o dispositivo pode entrar no estado de encaminhamento imediatamente após ter recebido handshake do dispositivo em downstream.

O RSTP pode convergir rapidamente. No entanto, existem as seguintes desvantagens com relação ao STP: todas as bridges em uma LAN compartilham um spanning tree e não podem bloquear links redundantes de acordo com a VLAN, todas as mensagens da VLAN são encaminhadas ao longo de uma spanning tree.

18.3. Configuração de spanning tree

O comando de configuração de STP / RSTP são os mesmos.

Habilitar o spanning tree

Após a inicialização global, todas as portas participarão no cálculo da topologia do spanning tree. Se o administrador deseja excluir algumas portas do cálculo do STP, é possível usar o comando *no spanning-tree* no modo de configuração para desativá-la.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o spanning tree globalmente	**no spanning tree**	Obrigatório, o comando é válido para STP / RSTP / MSTP
Desligar o spanning tree globalmente	**no spanning tree**	Opcional

Operação	Comando	Obrigatório/ opcional
Selecionar o modo do spanning tree	**spanning-tree mode** { stp | rstp | mstp }	Opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Spanning tree na porta	**spanning-tree**	Opcional
Desativar o spanning tree na porta	**no spanning-tree**	Opcional

Obs.: *depois que o spanning tree está habilitado globalmente, o sistema funciona no modo* RSTP *por padrão.*

Configurar a prioridade de bridge no OLT

A prioridade da bridge do OLT determina se ele pode ser selecionado como o root do STP. Ao configurar uma prioridade menor de bridge, você pode especificar que um OLT se torne o root da spanning tree.

Por padrão, a prioridade da bridge do OLT é *32768*.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar a prioridade do STP	**spanning-tree** bridge priority	Opcional

Configuração do parâmetro de tempo

O OLT tem três parâmetros de tempo: Forward Delay, Hello Time e Max Age. O usuário pode configurar esses três parâmetros no cálculo OLT para STP / RSTP.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o intervalo de mensagem de Hello	**spanning-tree hello-time** seconds	Opcional
Configurar o Forward Delay do sistema	**spanning-tree forward-delay** seconds	Opcional
Configurar o aging time do sistema	**spanning-tree max-age** seconds	Opcional

Obs.: » *Um valor de Hello Time excessivamente longo faz com que a bridge considere uma falha de link e comece a recalcular o spanning tree devido a uma falsa perda de pacote. Um valor excessivamente curto de Hello Time faz com que a bridge envie informações de configuração com frequência, aumentando a carga da CPU. Hello Time está no intervalo de 1 a 10 segundos. Recomenda-se usar o valor padrão de* 2 segundos, *devendo ser inferior ou igual ao foward delay-2.*

» *Se o foward delay for muito pequeno, um caminho redundante temporário pode ser introduzido; se for muito grande, a rede pode não retomar a comunicação por um longo período de tempo. Seu valor deve estar no intervalo de 4 a 30 segundos. Recomenda-se usar o padrão de* 15 segundos. *Ele deve ser maior ou igual ao Hello time + 2.*

» *Max Age define o intervalo de tempo máximo para a mensagem STP. Se expirar, a mensagem é descartada. Se esse valor for muito pequeno, o cálculo do spanning tree pode ser mais frequente, o congestionamento da rede pode ser confundido com a falha do link de rede; se esse valor for muito grande, pode não ser propício para detectar a falha do link em tempo hábil. O valor Max Age varia de 6 a 40 segundos e depende do diâmetro da rede. Recomenda-se o valor padrão de* 20 segundos. *O Max Age deve ser maior ou igual a 2 * (Hello Time + 1) e menor ou igual a 2 * (Forward Delay-1).*

Configuração do custo de caminho da porta

Ao configurar o custo do caminho de uma porta, esta pode se tornar uma porta root ou uma porta designada facilmente.

Este custo depende da taxa de link da porta, quanto maior a taxa, menor ele será. O STP pode detectar automaticamente a taxa de link da porta e traduzi-la para o custo do caminho correspondente, seu valor varia de 1 a 65.535. Recomenda-se usar o valor padrão e alterar o custo de uma porta fará com que o spanning tree seja recalculado.

Quando a velocidade da porta é de 10M, o valor padrão é *20,00,000*. O valor padrão é *200,000* para *100M* e *20,000* é o valor padrão para *1000M*. Quando a taxa de porta não está disponível, o custo do caminho é *200.000* por padrão.

» Configuração do custo de caminho da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	Opcional
Modificar o custo de caminho da porta	spanning-tree cost path-cost	Opcional

Se várias portas são agregadas em um grupo de agregação, o custo do caminho padrão do grupo é p [1 - (n-1/10)], onde p é o custo do caminho da porta e n é o número das portas do grupo de agregação.

Você pode definir manualmente o custo do caminho do grupo de agregação.

» Configuração do custo de caminho do grupo de agregação:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Definir o custo do caminho do grupo de agregação	**channel-group** id **spanning-tree cost** path-cost	Opcional

Configuração de prioridade de porta

Ao configurar a prioridade de uma porta, você pode melhorar a sua possibilidade se tornar uma porta root.

Quanto menor for o valor de prioridade (de 0 a 240, devendo ser um múltiplo inteiro de 16, por padrão, é 128), maior ela será. Alterar este valor em uma porta Ethernet fará com que o spanning tree seja recalculado.

» Configuração de prioridade de porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	Opcional

Operação	Comando	Obrigatório/ opcional
Configurar a prioridade STP da porta	**spanning-tree port-priority** priority	Opcional

Configuração da função de Mcheck

O OLT que opera no modo *RSTP* pode se conectar a uma chave STP para garantir a compatibilidade. No entanto, depois que o vizinho muda o modo de trabalho para RSTP, as duas portas conectadas entre si continuam funcionando no modo *STP* por padrão. A função *Mcheck* é usada para forçar a porta a enviar mensagem RSTP e confirmar se a porta adjacente pode funcionar neste modo. Se sim, o OLT muda automaticamente para o modo *RSTP*.

Obs.: *a função* Mcheck *requer que a porta envie BPDU. Portanto, é útil apenas na porta especificada.*

» Configuração da função de Mcheck:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	Opcional
Executar a função *Mcheck*	**spanning-tree mcheck**	Opcional

Configuração do link ponto a ponto

No RSTP, uma porta entra rapidamente em um estado de encaminhamento, para isso, é necessário que a porta seja um link ponto a ponto e não um link de mídia compartilhada. O usuário pode especificar manualmente o tipo de link de uma porta ou determiná-lo automaticamente com base no modo *Duplex* da porta.

Se a porta está no modo *Automático* e estiver no modo *Full duplex,* é avaliada como um link ponto a ponto. Se estiver em half duplex, é um link não ponto a ponto.

Quando o OLT está no modo *True* forçado, a porta é um link ponto a ponto.

Quando o OLT está no modo *False* forçado, a porta é um link não ponto a ponto.

Configuração de porta para porta de borda

Uma porta de borda significa uma porta conectada com um dispositivo terminal, como um host, e essas portas podem entrar no estado de encaminhamento em pouco tempo. A porta de borda é válida apenas para RSTP.

» Configuração de porta para porta de borda:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração de porta para porta de borda	**spanning-tree portfast**	Obrigatório
Configuração de porta para deixar de ser porta de borda	**no spanning-tree portfast**	Opcional

Definir a porta para enviar a taxa máxima de BPDU

A taxa máxima de BPDU enviada por porta é o número máximo de mensagens BPDU enviadas em cada Hello time.

Por padrão, a taxa de BPDU enviada pela porta envia 3 por Hello time.

» Definir a porta para enviar a Taxa Máxima de BPDU:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Definir a porta para enviar a Taxa Máxima de BPDU	**spanning-tree transit-limit** transit-limit	Opcional

Configuração da função de proteção de root da porta

A bridge de root pode receber a mensagem de configuração de prioridade mais alta devido a uma configuração incorreta ou um ataque malicioso na rede. Assim, ela pode perder o status de bridge de root e causar mudanças na topologia de rede.

Suponha que o tráfego original seja encaminhado através de um link de alta velocidade, essa mudança irregular fará com que o tráfego que passa pelo link de alta velocidade seja enviado para um link de baixa velocidade, o que resulta em congestionamento da rede. A proteção dos roots pode impedir que isso aconteça.

Para uma porta com proteção de root ativada, a função de porta só pode ser de porta designada. Uma vez que uma configuração de prioridade mias alta foi recebida na porta, existem duas opções para configurar o seu status:

» **Bloquear porta:** o estado da porta será configurado para descartar as mensagens de configuração da BPDU e não encaminhar mensagens de dados.

» **Descartar pacotes:** o estado da porta é de encaminhamento, apenas a configuração BPDU é descartada e os pacotes comuns são transmitidos normalmente.

» Configuração da função de proteção de root da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da proteção de root para o processamento de mensagem	**spanning-tree root-guard action {block-port | drop-packets}**	Obrigatório
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a proteção de root para a porta	**spanning-tree root-guard**	Obrigatório
Desabilitar a proteção de root para a porta	**no spanning-tree root-guard**	Opcional

Configuração da função de loop-guard

Função *Loop-guard*: evita que uma porta bloqueada devido a um link anormal (não comunicação bidirecional) não receba informações de configuração BPDU, que mudariam seu estado para encaminhamento.

Quando a porta está configurada com esta opção, a porta permanece bloqueada mesmo que a configuração da BPDU não seja recebida.

» Configuração da função de loop-guard da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função de loop-guard	**spanning-tree loop-guard**	Não pode ser compartilhado com o root-guard
Desabilitar a função de loop-guard	**no spanning-tree loop-guard**	Opcional

Configuração da função de BPDU-Guard

Para um dispositivo de camada de acesso, uma porta de acesso geralmente está diretamente conectada a um terminal de usuário (como um PC) ou um servidor de arquivos. Nesse caso, esta porta é configurada como uma porta de borda para implementar uma transição rápida. Quando ela recebe mensagens BPDU, o sistema irá configurá-la automaticamente como portas não-borda e recalcular os spanning tree para gerar as mudanças na topologia da rede. Essas portas normalmente não devem receber uma mensagem BPDU. Se alguém forjar uma BPDU para atacar maliciosamente o dispositivo, a rede ficará instável.

O dispositivo fornece a função de proteção BPDU para evitar tais ataques: após a ativação da função de proteção BPDU em um dispositivo, se uma porta configurada com um atributo de porta de borda receber uma mensagem BPDU, o dispositivo desligará a porta e solicitará ao usuário a informação Syslog. A porta deve ser restaurada manualmente.

» Configuração da função de BPDU-Guard:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**Configure terminal**	-
Habilitar o BPDU-Guard globalmente	**Spanning-tree bpdu-guard**	No modo *Global*, esta função é habilitada em todas as portas

Operação	Comando	Obrigatório/ opcional
Desabilitar o BPDU-Guard globalmente	**No spanning-tree bpdu-guard**	Opcional
Acesse o modo de configuração de porta	**Interface ethernet** interface-num	-
Habilitar o BPDU-Guard globalmente	**Spanning-tree bpdu-guard**	Esta função terá efeito apenas em uma porta
Desabilitar o BPDU-Guard globalmente	**No spanning-tree bpdu-guard**	Opcional

Obs.: *a função de proteção BPDU da porta só faz efeito na porta configurada com o atributo de porta de borda. Se esta porta receber uma mensagem BPDU de outra porta e tornar-se uma porta comum novamente e a função de proteção BPDU estiver habilitada, ela só executará as ações se for reiniciada como uma porta de borda.*

Configuração da função de filtro BPDU

Depois que o filtro BPDU é definido na porta de borda, o dispositivo descartará a mensagem BPDU recebida e a porta não enviará mais essa mensagem.

» Configuração da função *BPDU-Filter* para a porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o BPDU-Filter globalmente	**spanning-tree bpdu-filter**	No modo *Global*, esta função é habilitada em todas as portas
Desabilitar o BPDU-Filter globalmente	**no spanning-tree bpdu-filter**	Opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar o BPDU-Filter na interface	**spanning-tree bpdu-filter**	Esta função terá efeito apenas em uma porta

Operação	Comando	Obrigatório/ opcional
Desabilitar o BPDU-Filter globalmente	**no spanning-tree bpdu-filter**	Opcional

Função *BPDU-Car*

Se um grande número de mensagens de BPDU estão na CPU, ela poderá apresentar problemas. A função *BPDU-Car* limita a taxa de mensagem bppu na CPU, para evitar estas situações.

» Configuração do BPDU-Car:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o BPDU-Car	**[no]port-car**	Opcional, está *habilitado* por padrão
Configuração de taxa de BPDU na CPU	**port-car-rae** value	Opcional, por padrão *(número de portas * 30) pps*
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Habilitar/desabilitar o BPDU-Car	**[no]port-car**	Opcional, está *habilitado* por padrão
Configuração de taxa de BPDU na CPU	**port-car-rae** value	Opcional, por padrão *30pps*
Visualização das informações de configuração	**show port-car**	Opcional

Função *Discard-BPDU*

A função *Discard-BPDU* é usada para descartar a mensagem STP. Se o dispositivo não quiser receber mensagens BPDU de outras redes, esta função deve ser ativada.

A função *Discard-BPDU* está desativada por padrão. A configuração global e a configuração da porta são mutuamente exclusivas: globalmente, todas as portas estão habilitadas. Se você só precisa ativar certas portas designadas, não é necessário configurá-las globalmente.

» Configuração do Discard-BPDU global:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o BPDU	**[no]discard-bpdu**	Opcional, está *desabilitado* por padrão
Visualização das informações de configuração	**show discard-bpdu**	Opcional

» Configurção do Discard-BPDU na porta:

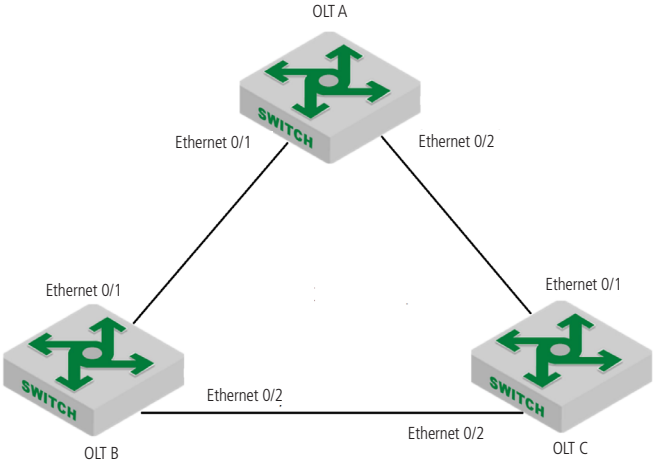
Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Habilitar/desabilitar o BPDU	**[no]discard-bpdu**	Opcional, está *desabilitado* por padrão
Visualização das informações de configuração	**show discard-bpdu**	Opcional

Visualização e manutenção

Depois de completar a configuração acima, você pode usar o seguinte comando para visualizar a configuração.

Operação	Comando	Obrigatório/ opcional
Exibir o status da porta de extensão, ou seja, os parâmetros de configuração da spanning tree. Endereço MAC do root OLT e assim por diante.	**show spanning-tree interface [brief [ethernet** interface-list **]**	Opcional, executável em todos os modos

Exemplo de configuração de RSTP



» Requisitos de rede:

Como exibido acima, o OLT-A atua como a bridge de root. OLT-B atua como a bridge designada. Os links que ligam OLT-B e OLT-C são links de backup. OLT-B, OLT-A ou OLT-C falham, o link de backup funciona.

» Procedimento de configuração:

» Configuração do OLT A:

» Configure a porta ethernet0/1 e a porta ethernet0/2 como trunk:

OLT4840E(config)#interface range ethernet 0/1 ethernet 0/2

OLT4840E(config-if-range)#switchport mode trunk

» Configure a prioridade da bridge OLT4840E para 0. Certifique-se de que o OLT-A seja a bridge root.

OLT4840E(config)#spanning-tree priority 0

» Inicie o RSTP globalmente

OLT4840E(config)#spanning-tree

OLT4840E(config)#spanning-tree mode rstp

» Configuração da OLT B:

» Configure a porta ethernet0/1 e a porta ethernet0/2 como trunk:

S-switch-B(config)#interface range ethernet 0/1 ethernet 0/2

S-switch-B(config-if-range)#switchport mode trunk

S-switch-B(config-if-range)#exit

» Configure a prioridade da bridge do OLT-B para 4096, certifique-se de que OLT-B seja a bridge designada e o custo do caminho da configuração Ethernet 0/1 e Ethernet 0/2 deve ser 10.

S-switch-B(config)#spanning-tree priority 4096

S-switch-B(config)#interface range ethernet 0/1 ethernet 0/2

S-switch-B(config-if-range)#spanning-tree cost 10

S-switch-B(config-if-range)#exit

» Inicie o RSTP globalmente.

S-switch-B(config)#spanning-tree

S-switch-B(config)#spanning-tree mode rstp

» Configuração da OLT C:

» Configure a porta ethernet0/1 e a porta ethernet0/2 como trunk

S-switch-C(config)#interface range ethernet 0/1 ethernet 0/2

S-switch-C(config-if-range)#switchport mode trunk

S-switch-C(config-if-range)#exit

» Configurar o custo do caminho da Ethernet 0/1 e Ethernet 0/2 para 10. Certifique-se de que o link que liga OLT-B e OLT-C seja o principal.

S-switch-C(config)#interface range ethernet 0/1 ethernet 0/2

S-switch-C(config-if-range)#spanning-tree cost 10

S-switch-C(config-if-range)#exit

» Inicie o RSTP globalmente.

S-switch-C(config)#spanning-tree

S-switch-C(config)#spanning-tree mode rstp

S-switch-C(config)# spanning-tree priority 32768

» Verifique as configurações:

» Execute o comando de exibição no OLT4840E e veja o resultado da eleição e o status da porta do RSTP. Os resultados são os seguintes:

OLT4840E(config)#show spanning-tree interface ethernet 0/1 ethernet 0/2
The bridge is executing the IEEE Rapid Spanning Tree protocol
The bridge has priority 0, MAC address: 000a.5a13.b13d
Configured Hello Time 2 second(s), Max Age 20 second(s),
Forward Delay 15 second(s)
Root Bridge has priority 0, MAC address 000a.5a13.b13d
Path cost to root bridge is 0
Stp top change 3 times

Port e0/1 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a DesignatedPort
Port path cost 200000
Port priority 128
root guard enabled and port is not in root-inconsistent state
Designated bridge has priority 0, MAC address 000a.5a13.b13d
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
Times: Hello Time 2 second(s), Max Age 20 second(s)
Forward Delay 15 second(s), Message Age 0
sent BPDU: 54
TCN: 0, RST: 54, Config BPDU: 0
received BPDU: 10
TCN: 0, RST: 10, Config BPDU: 0

Port e0/2 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled

The port is a DesignatedPort

Port path cost 200000

Port priority 128

root guard enabled and port is not in root-inconsistent state

Designated bridge has priority 0, MAC address 000a.5a13.b13d

The Port is a non-edge port

Connected to a point-to-point LAN segment

Maximum transmission limit is 3 BPDUs per hello time

Times: Hello Time 2 second(s), Max Age 20 second(s)

Forward Delay 15 second(s), Message Age 0

sent BPDU: 16

TCN: 0, RST: 17, Config BPDU: 0

received BPDU: 3

TCN: 0, RST: 3, Config BPDU: 0

OLT A é eleito como a bridge de root, porque o OLT A tem a maior prioridade em toda a rede. Ethernet 0/1 e Ethernet 0/2 de OLT A são portas designadas. Elas estão no estado de encaminhamento.

» Execute o comando de exibição no OLT B e visualize o resultado da eleição e o status da porta do RSTP. A seguinte informação é exibida:

OLT4840E (config)#show spanning-tree interface ethernet 0/1 ethernet 0/2

The bridge is executing the IEEE Rapid Spanning Tree protocol

The bridge has priority 4096, MAC address: 0000.0077.8899

Configured Hello Time 2 second(s), Max Age 20 second(s),

Forward Delay 15 second(s)

Root Bridge has priority 0, MAC address 000a.5a13.b13d

Path cost to root bridge is 10

Stp top change 3 times

Port e0/1 of bridge is Forwarding

Spanning tree protocol is enabled

remote loop detect is disabled
The port is a RootPort
Port path cost 10
Port priority 128
root guard disabled and port is not in root-inconsistent state
Designated bridge has priority 0, MAC address 000a.5a13.b13d
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
Times: Hello Time 2 second(s), Max Age 20 second(s)
Forward Delay 15 second(s), Message Age 0
sent BPDU: 21
TCN: 0, RST: 12, Config BPDU: 9
received BPDU: 204
TCN: 0, RST: 202, Config BPDU: 2

Port e0/2 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a DesignatedPort
Port path cost 10
Port priority 128
root guard disabled and port is not in root-inconsistent state
Designated bridge has priority 4096, MAC address 0000.0077.8899
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
Times: Hello Time 2 second(s), Max Age 20 second(s)
Forward Delay 15 second(s), Message Age 1
sent BPDU: 191

TCN: 0, RST: 178, Config BPDU: 3

received BPDU: 13

TCN: 0, RST: 5, Config BPDU: 8

A prioridade do OLT B é menor que a de OLT A. Ethernet 0/1 do OLT B é a porta root e esta no estado de encaminhamento. Ao mesmo tempo que o OLT B tem uma prioridade maior do que o OLT C, a Ethernet 0/2 do OLT B é designada com porta backup e está no modo de descarte.

» Execute o comando de exibição no OLT C e visualize o resultado da eleição e o status da porta do RSTP. A seguinte informação é exibida:

OLT4840E (config)#show spanning-tree interface ethernet 0/1 ethernet 0/2

The bridge is executing the IEEE Rapid Spanning Tree protocol

The bridge has priority 32768, MAC address: 000a.5a13.f48e

Configured Hello Time 2 second(s), Max Age 20 second(s),

Forward Delay 15 second(s)

Root Bridge has priority 0, MAC address 000a.5a13.b13d

Path cost to root bridge is 20

Stp top change 3 times

Port e0/1 of bridge is Forwarding

Spanning tree protocol is enabled

remote loop detect is disabled

The port is a RootPort

Port path cost 10

Port priority 128

root guard disabled and port is not in root-inconsistent state

Designated bridge has priority 0, MAC address 000a.5a13.b13d

The Port is a non-edge port

Connected to a point-to-point LAN segment

Maximum transmission limit is 3 BPDUs per hello time

Times: Hello Time 2 second(s), Max Age 20 second(s)

Forward Delay 15 second(s), Message Age 0
sent BPDU: 3
TCN: 0, RST: 3, Config BPDU: 0
received BPDU: 396
TCN: 0, RST: 396, Config BPDU: 0

Port e0/2 of bridge is Discarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a AlternatePort
Port path cost 10
Port priority 128
root guard disabled and port is not in root-inconsistent state
Designated bridge has priority 4096, MAC address 0000.0077.8899
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
Times: Hello Time 2 second(s), Max Age 20 second(s)
Forward Delay 15 second(s), Message Age 1
sent BPDU: 8
TCN: 0, RST: 8, Config BPDU: 0
received BPDU: 417
TCN: 0, RST: 418, Config BPDU: 0

A prioridade do OLT C é menor que a de OLT A e OLT B. O custo da rota de Ethernet 0/1 para a bridge de root é menor que o de Ethernet 0/2. Então Ethernet 0/1 é calculado como a porta root e no estado de encaminhamento. Ethernet0 / 2 é calculado como a porta alternativa e no estado de descarte.

19. Configuração de Multiple Spanning Tree

19.1. Visão geral de MSTP

O Spanning Tree Protocol não pode migrar o estado das portas rapidamente. Mesmo no link ponto a ponto ou na borda, ele deve ter um atraso de duas vezes o forward delay, para que a porta possa ser transferida para o estado de encaminhamento.

O RSTP (*Rapid Spanning Tree Protocol*) pode convergir a rede mais rapidamente, porém existem algumas deficiências similares ao STP: todas as bridges da LAN compartilham um spanning tree e não podem bloquear links redundantes de acordo com a VLAN, todas as mensagens de VLAN são encaminhadas ao longo deste spanning tree.

O protocolo Multiple Spanning Tree Protocol (MSTP) processa a rede com loop em uma rede de árvore acíclica para evitar a proliferação e o loop infinito de pacotes nela. Também fornece vários encaminhamentos redundantes de dados. O balanceamento de carga dos dados da VLAN é alcançado durante o seu encaminhamento.

O MSTP é compatível com STP e RSTP, podendo compensar defeitos desta duas tecnologias, convergindo rapidamente e distribuindo o tráfego de diferentes VLAN ao longo de seu próprio caminho. Assim, ele pode fornecer um melhor mecanismo de compartilhamento de carga para o link redundante.

Unidade de dados do protocolo de bridge

O MSTP usa o BPDU para calcular o spanning tree assim como STP / RSTP. O BPDU do MSTP carrega informações de configuração do MSTP no OLT.

Conceitos básicos de MSTP

» Região MST

Elas são compostas por vários OLTs na rede e seus segmentos entre eles. Esses OLTs são compatíveis com MSTP e possuem o mesmo nome de domínio, a mesma configuração de VLAN para spanning-tree, a mesma versão MSTP e conexão de ligação física.

Uma rede pode ter múltiplas regiões MST. O usuário pode usar o MSTP para dividir vários OLTs na mesma região.

» CIST

O spanning tree comum e interno é composto de todos os OLTs e LANs conectados. Esses OLTs podem pertencer a diferentes áreas de MSTP, ou podem executar um protocolo STP/ RSTP tradicional. O OLT que executa dois protocolos em uma rede de multi-spanning tree é considerado apenas na sua própria área.

Depois que a topologia da rede está estável, todo o CIST seleciona uma bridge de root CIST. Em cada área, a bridge de root na área CIST é eleita como o caminho mais curto da intra-área para o root CIST.

» CST

CST é uma sigla para common spanning tree. Se cada área de multiple spanning tree tratada como um único OLT, o CST é o spanning tree que conecta todos esses *OLTs individuais*.

» IST

IST é uma sigla para internet spanning tree, que se refere à parte do CIST em uma área de multiple spanning tree, e também pode ser entendido que o IST e o CST formam o CIST.

» MSTI

O MSTI é uma sigla para multiple spanning tree instances. O protocolo MSTI permite que diferentes VLANs sejam divididas em diferentes spanning trees, portanto uma pluralidade de instâncias de spanning trees é estabelecida. Normalmente, uma instância de spanning tree com o número 0 é o CIST, que pode ser estendido para toda a rede. A instância do spanning tree que começa a partir de 1 está no interior de uma determinada área. Cada instância do spanning tree pode receber múltiplas VLANs. Inicialmente, todas as VLANs são atribuídas no CIST.

Em uma área de multi-spanning tree, todos os MSTIs são independentes uns dos outros. Eles podem selecionar diferentes OLTs como seus próprios roots.

» Bridge de root CIST

A bridge root CIST é a bridge com a maior ID de prioridade em toda a rede.

» Custo de rota externa CIST

O custo do caminho do root externo CIST é o custo do caminho entre a bridge e o root CIST. Este custo é igual para todas as bridges na mesma região MST.

» Root CIST regional

O root CIST regional é a bridge de menor custo no caminho de root externo. Na verdade, é a bridge root do IST, ou a bridge virtual da região MST. Se o root CIST estiver em uma região MST, ele também é a bridge root da região CIST na região MST.

» Custo interno da rota de root CIST

O custo interno da rota de root CIST é o custo do caminho do root da região

MST na bridge de root regional CIST, que é válido apenas nesta região.

» Bridge CIST designada

A bridge designada pela CIST é a mesma que a bridge designada pelo STP.

» Root MSTI regional

O root MSTI regional é a bridge de root MSTI em cada região do MST. Ela pode não ser a mesma para diferentes MSTI.

» Custo interno da rota de root MSTI

O custo interno da rota de root MSTI é o custo do caminho do root da região MST no root regional do MSTI, que é válido apenas na região.

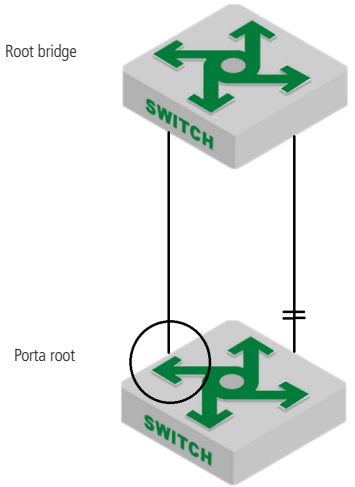
» Bridge MSTI designada

A bridge designada pela MSTI é a mesma que a bridge designada pelo STP.

Papel da porta

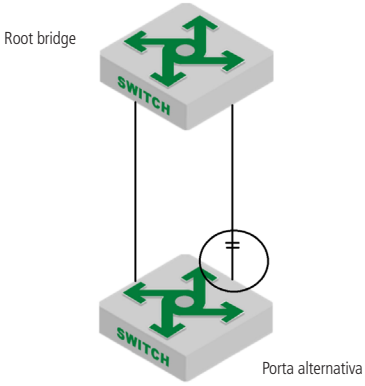
O protocolo MSTP tem atribuição de função de porta semelhante ao RSTP.

Porta root



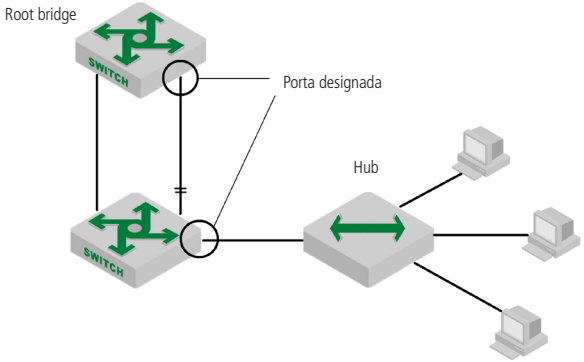
A porta root representa o caminho do OLT atual para a bridge de root da rede, que possui o menor custo de caminho do root.

Porta alternativa (alternative)



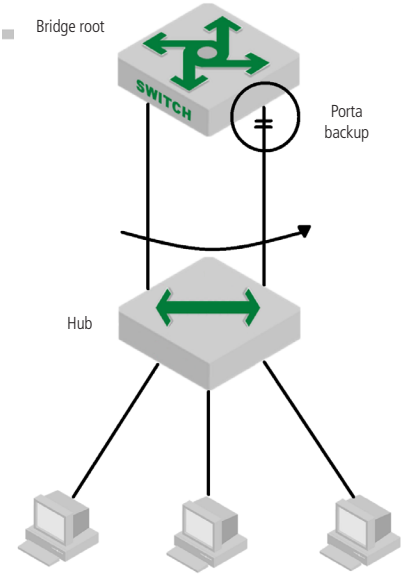
A porta alternativa atua como o backup do OLT atual para a bridge root da rede. Quando a porta root falhar, a porta alternativa se torna imediatamente como a nova porta root.

Porta designada (designated)



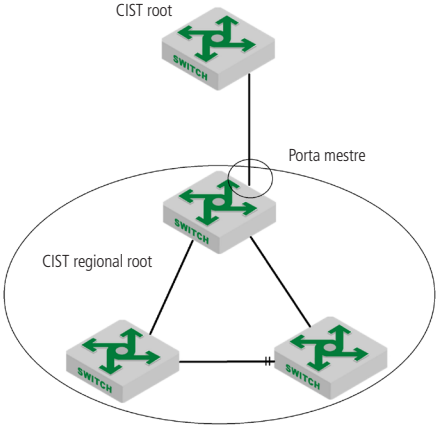
A porta designada pode ser conectada com um OLT em downstream ou uma rede de área local (LAN), que pode atuar como o caminho da LAN para a bridge root da rede.

Porta de backup



Quando as duas portas do OLT estão diretamente conectadas ou se conectam à mesma LAN, a porta com menor prioridade torna-se a porta de backup (a maior se torna a porta designada). Se houver uma falha, a porta de backup se torna a porta designada para começar a funcionar.

Porta mestre (master)



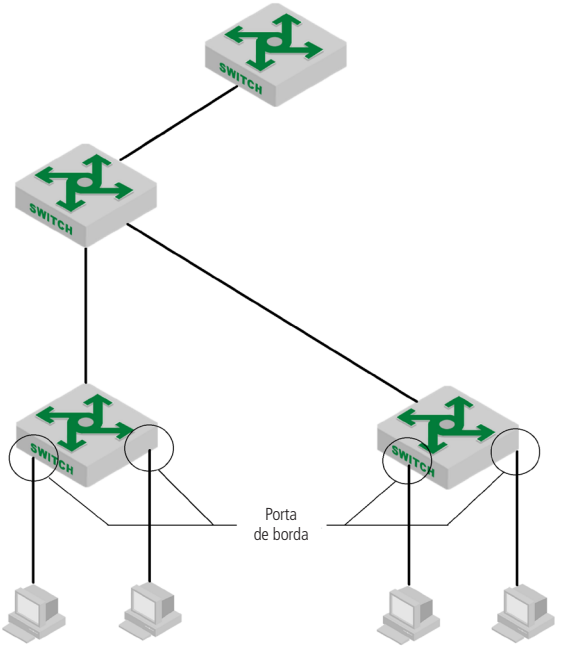
A porta mestre atua como o caminho mais curto que liga a bridge de root CIST em várias regiões do spanning tree. A porta mestre é a porta root da bridge de root no CIST.

Porta de limite (boundary)

O conceito de porta de limite é ligeiramente diferente entre o CIST e cada MSTI. No CIST, uma porta de limite representa uma porta que se conecta a outra região do multi-spanning tree. No MSTI, esta função indica que a instância do spanning tree não está mais estendida nesta porta.

Porta de borda (edge)

Nos protocolos RSTP e MSTP, a porta de borda indica que a porta se conecta diretamente ao host da rede. Essas portas não precisam esperar para entrar no estado de encaminhamento e não causam um loop na rede.



No caso inicial, o protocolo MSTP (incluindo RSTP) considera todas as portas como portas de borda, garantindo assim o estabelecimento rápido de topologia de rede. Se uma delas recebe uma BPDU de outro OLT, a porta retorna ao estado normal. Se receber uma DPBDU de STP 802.1D, a porta espera um tempo de duas vezes o forward delay para entrar no estado de encaminhamento.

19.2. Configuração do MSTP

Iniciar o MSTP

Depois que a árvore global é gerada automaticamente, todas as portas participam do cálculo da topologia do spanning tree. Se o administrador deseja excluir determinadas portas deste cálculo, deve-se usar o comando *no spanning-tree* para desativar a função no modo de configuração de porta.

» Iniciar o MSTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Selecionar o modo do spanning tree	**spanning-tree mode mstp**	Obrigatório
Iniciar o spanning tree globalmente	**spanning-tree**	Obrigatório
Desativar o spaning tree globalmente	**no spanning-tree**	Opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar o spanning tree na porta	**spanning-tree**	Opcional
Desativar o spanning tree na porta	**no spanning-tree**	Opcional

Configuração dos parâmetros de tempo do MSTP

O controle de tempo do MSTP inclui o forward delay, hello time, maximum age, and max hops. O usuário pode configurar esses quatro parâmetros para calcular o spanning tree para MSTP no OLT.

» Configuração dos parâmetros de tempo do MSTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do forward delay da bridge	**spanning-tree mst forward-time** forward-time	Opcional
Configuração do hello time na bridge	**spanning-tree mst hello-time** hello-time	Opcional
Configuração do max age na bridge	**spanning-tree mst max-age** max-age	Opcional
Configuração do max hops na bridge	**spanning-tree mst max-hops** max-hops	Opcional

Obs.: » *Um valor de Hello Time excessivamente longo faz com que a bridge considere uma falha de ligação e comece a recalcular a extensão por causa da perda de pacotes; um valor muito curto faz com que a bridge envie informações de configuração com frequência, aumentando a carga da rede e da CPU. Ele está no intervalo de 1 a 10 segundos. Recomenda-se usar o valor padrão de* 2 segundos. *O hello time deve ser menor ou igual ao forward delay-2.*

» *Se o forward delay for muito pequeno, um caminho redundante temporário pode ser introduzido. Se for muito grande, a rede pode não retomar a comunicação por um longo período de tempo. Seu valor está no intervalo de 4 a 30 segundos. Recomenda-se usar o valor padrão* 15 segundos. *O tempo de forward delay deve ser maior ou igual ao Hello Time + 2.*

» *Max Age define o intervalo de tempo máximo para o envelhecimento da mensagem do protocolo MSTP. Se o timer expirar, o pacote será descartado. Se o valor for muito pequeno, o cálculo da spanning tree pode ser frequente. É possível interpretar mal o congestionamento da rede como uma falha no link. Se o valor for muito grande, não é propício para a detecção de falha do link. O Max Age está na faixa de 6 a 40 segundos. O valor do tempo Max Age depende do diâmetro da rede da rede comutada. Recomenda-se o valor padrão de* 20 segundos. *O Max Agedeve ser maior ou igual a 2 * (Hello time + 1) e menor que ou igual a 2 * (Forward delay-1).*

Configuração do identificador de configuração do MSTP

O identificador de configuração do MSTP inclui o nome da configuração, o nível de revisão e o mapeamento entre a instância e a VLAN. O MSTP trata a bridge com o mesmo identificador de configuração e interligação lógica como uma bridge virtual.

» Configure o identificador de configuração do MSTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da configuração do nome do MSTP	**spanning-tree mst name** name	Opcional
Configuração do nível de revisão do MSTP	**spanning-tree mst revision** revision-level	Opcional
Configuração do mapeamento entre a instância do MSTP e a VLAN	**spanning-tree mst instance** instance-num **vlan** vlan	Opcional
Remover o mapeamento entre a instância do MSTP e a VLAN	**no spanning-tree mst instance** instance-num **vlan** vlan	Opcional

Configuração da prioridade de bridge MSTP

No MSTP, a prioridade da bridge é baseada nos parâmetros de cada spanning tree. A prioridade da bridge, juntamente com a prioridade da porta e o custo do caminho da porta determinam a topologia de cada instância do spanning tree e formam a base para o balanceamento de carga do link.

O valor da prioridade da bridge determina se o OLT pode ser selecionado como a bridge root da spanning tree. Ao configurar uma prioridade de bridge menor, o usuário pode especificar que um OLT se torne a bridge root da spanning tree.

Por padrão, a prioridade de bridge do OLT é *32768*.

» Configurar a prioridade da bridge MSTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configure a prioridade da bridge na instância do MSTP	**spanning-tree mst instance** instance-num **priority** priority	Opcional

Configurar o estado da porta de limite de uma porta

A porta de limite refere-se à porta que se conecta ao host. Essas portas podem entrar no estado de encaminhamento dentro de um curto período de tempo após o link, mas mudarão automaticamente para a porta não-de-borda uma vez que receberem a mensagem do spanning tree.

» Configurar o estado da porta de fronteira de uma porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração de porta como uma porta de fronteira	**spanning-tree mst portfast**	Opcional
Configuração de porta como uma porta não de fronteira	**no spanning-tree mst portfast**	Opcional

Configuração de tipo de conexão da porta

Existem dois tipos de link: um é o link de mídia compartilhada (conectado pelo hub etc.) e o outro é o link ponto a ponto. O tipo de link é usado principalmente na proposta de transição rápida do estado da porta - mecanismo de consentimento. Somente a porta de link ponto a ponto pode permitir a rápida transição do estado da porta.

No MSTP, a porta entra rapidamente no estado de encaminhamento, o que exige que ela seja um link ponto a ponto e não um link de mídia compartilhada. O usuário pode especificar manualmente o tipo de link ou determiná-lo automaticamente (a porta de full duplex é automaticamente considerada como link ponto a ponto, a porta half-duplex determina automaticamente o link não ponto a ponto).

» Configuração do tipo de conexão da porta MSTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração do tipo de conexão da porta	**spanning-tree mst link-type point-to-point {auto | forcetrue| forcefalse}**	Opcional

Configuração do custo de rota da porta

O custo de rota da porta é dividido em custos internos e externos. O primeiro é baseado nos parâmetros de configuração de cada instância MSTP. Ele é usado para determinar a topologia de diferentes instâncias em cada região MSTP. O último é um parâmetro independente que determina a topologia do CST composto de regiões.

Ao configurar o custo do caminho de uma porta, o usuário pode facilitar que uma porta se torne uma porta root ou uma porta designada.

O custo do caminho de uma porta depende da sua taxa do link. Quanto maior, menor será a configuração do parâmetro. O protocolo MSTP detecta automaticamente a taxa de link da porta atual e a converte no custo do caminho correspondente.

Configurar o custo do caminho de uma porta Ethernet fará com que o spanning tree seja recalculado. Ele varia de 1 a 65.535 e recomenda-se usar o valor padrão. Deixe o protocolo MSTP calcular o custo do caminho da porta atual.

O custo do caminho da porta padrão é baseado na velocidade da porta: *200.000* quando a velocidade da porta é de *10M*; *200.000* quando a porta é *100M*; *200.000* quando a taxa de porta não está disponível.

» Configuração do custo de rota da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração do custo de rota interna da porta	**spanning-tree mst instance** instance-num **cost** cost	Opcional
Configuração do custo de rota externa da porta	**spanning-tree mst external cost** cost	Opcional

Configuração de prioridade de porta

Em MSTP, a prioridade da porta é baseada nos parâmetros de cada spanning tree. Ao configurar a prioridade de uma porta, o usuário po facilitar que uma porta seja uma porta root.

Quanto menor for o valor da prioridade configurado, maior ela será. Alterar esta informação fará com que o spanning tree seja recalculado. A prioridade do spanning tree de uma porta varia de 0 a 240 e deve ser um múltiplo inteiro de 16. Por padrão, a prioridade do spanning tree de porta é *128*.

» Configuração de prioridade de porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração de prioridade porta	**spanning-tree mst instance** instance-num **port-priority** priority	Opcional

Configuração de proteção de root da porta

Devido a um erro de configuração ou um ataque malicioso na rede, a bridge de root pode receber uma mensagem de configuração de uma prioridade mais alta, perdendo seu status de bridge de root e causando alterações incorretas da topologia de rede. Suponha que o tráfego original seja encaminhado através do link de alta velocidade. Essa mudança ilegal levará ao tráfego a ser alterado para um link de baixa velocidade e, consequentemente, ao congestionamento da rede. A proteção de root pode impedir que isso aconteça.

Para uma porta com proteção de root ativada, o papel de porta só pode ser de porta designada. Uma vez recebida uma informação de configuração de alta prioridade pela porta, o status dessas portas será definido para descartar e não ser encaminhado (O link conectado a esta porta está desconectado). Se a informação de configuração não é recebida dentro de um período de tempo, a porta retorna o estado original.

No MSTP, esta função funciona em todas as instâncias.

» Configuração de proteção de root da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a proteção de root da porta	**spanning-tree mst root-guard**	Opcional
Desabilitar a proteção de root da porta	**no spanning-tree mst root-guard**	

Configuração da função *Digest Snooping*

Quando a porta do OLT se conecta com um OLT da Cisco usando um spanning tree privado, devido aos protocolos privados, mesmo que as regiões do MST estejam configuradas iguais, eles não podem se comunicar entre si. O recurso de digest snooping evita que isso aconteça. Depois que a função de Digest snooping é ativada em uma porta, ao receber estas BPDU do fornecedor OLT, ele as considera como mensagens da mesma região MST e registra a configuração BPDU. Quando as mensagens BPDU são enviadas para os OLTs desses fornecedores, o OLT adiciona a configuração de digest snooping. Desta forma, o OLT implementa o funcionamento entre esses OLTs na região do MST.

» Configuração da função *Digest Snooping*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função *Digest Snooping*	**spanning-tree mst config-digest-snooping**	Opcional
Desabilitar spanning-tree mst config-digest-snooping	**no spanning-tree mst config-digest-snooping**	

Configuração da função *loop-guard*

A função *loop-guard*: impede uma porta bloqueada adote um estado de encaminhamento depois de não receber as informações de configuração da BPDU. Quando a porta é configurada com esta opção, ela permanece bloqueada mesmo que a BPDU de configuração não seja recebida.

» Configuração da função de loop-guard:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função *loop-guard*	**spanning-tree mst loop-guard**	Opcional

Operação	Comando	Obrigatório/ opcional
Desabilitar a função *loop-guard*	**no spanning-tree mst loop-guard**	-

Configuração da função de BPDU-Guard

Para um dispositivo de camada de acesso, a porta de acesso geralmente se conecta diretamente ao terminal de usuário ou ao servidor de arquivos. Nesse caso, elas são definidas como portas de borda para permitir a sua transição rápida. Quando recebem a mensagem BPDU, o sistema automaticamente as define como portas não-de-borda e recalcula o spanning tree, fazendo as alterações de topologia de rede. Essas portas normalmente não devem receber uma mensagem BPDU. Se alguém forjar um BPDU para atacar o dispositivo, a rede ficará instável.

O dispositivo fornece a função de proteção BPDU para evitar esses ataques: depois que a função de proteção BPDU é ativada em um dispositivo, se uma porta configurada com atributos da porta de borda receber uma mensagem BPDU, o dispositivo desligará a porta e solicitará ao usuário a informação Syslog.

» Configuração da função de BPDU-Guard:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar a função *BPDU-Guard globalmente*	**[no] spanning-tree mst bpdu-guard**	Opcional, no modo *Global*, será habilitado em todas as portas
Desabilitar a função *BPDU-Guard globalmente*	**no spanning-tree mst bpdu-guard**	Opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função *BPDU-Guard*	**spanning-tree mst bpdu-guard**	Obrigatório, será habilitado em uma única porta
Desabilitar a função *BPDU-Guard*	**no spanning-tree mst bpdu-guard**	Opcional

Obs.: *a função de proteção da BPDU só tem efeito em portas configuradas com o atributo de porta de borda. Neste caso, ao receber a mensagem BPDU de outra porta, ela se torna a porta não-borda. A porta só pode produzir efeitos quando é reiniciada como uma porta de borda.*

Configuração da função de BPDU-Filter

Se o BPDU estiver configurado na porta de borda, o dispositivo descartará a mensagem BPDU recebida e a porta não o enviará.

» Configuração da função de BPDU-Filter:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar a função *BPDU-Filter*	**[no] spanning-tree mst bpdu-filter**	No modo *Global*, será habilitado em todas as portas
Desabilitar a função *BPDU-Filter*	**no spanning-tree mst bpdu-filter**	Opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função BPDU-Filter	**[no] spanning-tree mst bpdu-filter**	Opcional, será habilitado em uma única porta
Desabilitar a função *BPDU-Filter*	**no spanning-tree mst bpdu-filter**	Opcional

Configuração da função *Mcheck*

O OLT que funciona no modo *MSTP* pode ser conectado a uma OLT no modo *STP*. No entanto, depois que o vizinho mudar seu modo de funcionamento para MSTP, as duas portas conectadas ainda funcionarão no modo *STP* por padrão. A função *Mcheck* é usada para forçar uma porta para enviar pacotes *MSTP* e determinar se a porta adjacente pode funcionar neste modo. Se sim, o OLT funcionará no modo *MSTP* automaticamente.

» Configuração da função *Mcheck*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração da função *Mcheck*	**spanning-tree mst mcheck**	Opcional

Obs.: *a função* Mcheck *requer que a porta envie a mensagem BPDU somente na porta especificada.*

Habilitar/desabilitar a instância MSTP

Para controlar o MSTP de forma flexível, o usuário pode habilitar o recurso DISABLE (desabilitar) INSTANCE (instância). O efeito deste recurso é semelhante ao da execução de *no spanning-tree* no modo *STP*. A porta mapeada para o VLAN da instância é encaminhada para todas as conexões.

» Habilitar/desabilitar da instância MSTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Ignorar a publicação de uma instância do MSTP	**spanning-tree mst disable instance** instance-number	Opcional
Restauração da publicação de uma instância do MSTP	**no spanning-tree mst disable instance** instance-number	Opcional

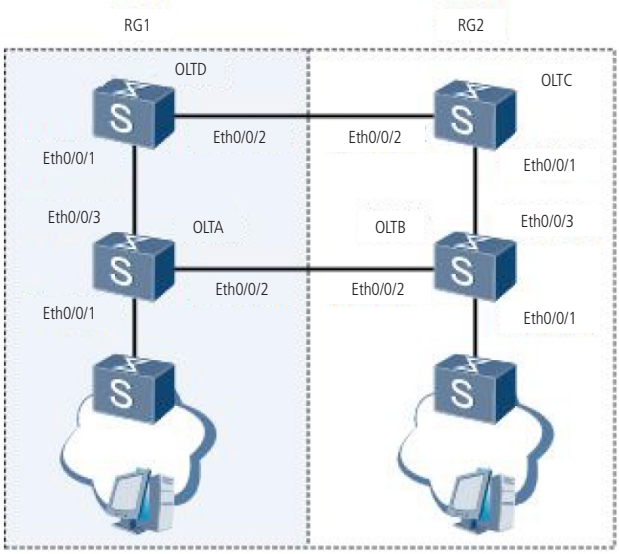
Visualização e manutenção do MSTP

Depois de completar a configuração acima, você pode usar o seguinte comando para visualizar a configuração.

» Visualização e manutenção do MSTP:

Operação	Comando	Obrigatório/ opcional
Visualização do identificador da configuração MSTP	**show spanning-tree mst config-id**	Opcional, executável em todos os modos
Visualização de todas as informações de portas MSTI	**show spanning-tree mst instance brief** id	
Visualização de todas as informações da porta MSTI	**show spanning-tree mst instance** id **interface ethernet** interface-list	
Visualização dos exemplos ignorados	**show spanning-tree mst disabled-instance**	

Exemplo de configuração de MSTP



» Requisitos de rede:

Na rede exibida na figura acima, OLT A e OLT C são configurados em um domínio com o nome RG1 e o MSTI 1 é criado. Configure OLT B e OLT D para outro domínio. O nome de domínio é RG2 e MSTI1 e MSTI2 são criados.

Configure OLT C como o root CIST. No domínio RG1, OLT C é o root do domínio CIST e OLTC é o root do domínio do MSTI1. Aplique a função de proteção root às portas Ethernet 0/1 e Ethernet 0/2 na OLTC. No domínio RG2, OLT D é o root regional CIST, OLT B é o root regional do MSTI1 e OLT D é o root regional do MSTI2.

O switch L2 conectado a OLT A e OLT B não suporta MSTP. Defina Ethernet 0/1 como a interface de borda para OLT A e OLT B.

» Passos de configuração:

» Configure OLT C:

» Crie VLAN de 1 a 20 e configure as portas Ethernet 0/1 e Ethernet 0/2 como portas trunk e adicione-as à VLAN 1 a 20.

OLT4840E (config)#interface range ethernet 0/1 ethernet 0/2

OLT4840E (config-if-range)#switchport mode trunk

OLT4840E (config-if-range)#exit

OLT4840E (config)#vlan 1-20

OLT4840E (config-if-vlan)#switchport ethernet 0/1 ethernet 0/2

OLT4840E (config-if-vlan)#exit

» Configure a região MST do OLT4840E.

OLT4840E (config)#spanning-tree mst name RG1

OLT4840E (config)#spanning-tree mst instance 1 vlan 1-10

» Defina a prioridade do OLT-C no MSTI 0 a 0, garantindo que o OLT-C seja o root comum do CIST.

OLT4840E(config)#spanning-tree mst instance 0 priority 0

» Defina a prioridade do OLT-C no MSTI 1 a 0, garantindo que OLT-C seja o root comum do MSTI1.

OLT4840E(config)#spanning-tree mst instance 1 priority 0

» Ative a proteção root na porta Ethernet0 / 1 e Ethernet0 / 2.

OLT4840E(config)#interface range ethernet 0/1 ethernet 0/2

OLT4840E(config-if-range)#spanning-tree mst root-guard

OLT4840E(config-if-range)#exit

- » Habilite o MSTP.

  OLT4840E(config)#spanning-tree mode mstp

  OLT4840E(config)#spanning-tree

- » Configure o OLT-A:
  - » Crie VLAN de 1 a 20 e configure as portas Ethernet 0/2 e Ethernet 0/3 como portas trunk e adicione-as à VLAN 1 a 20.

    OLT4840E (config)#interface range ethernet 0/2 ethernet 0/3

    OLT4840E (config-if-range)#switchport mode trunk

    OLT4840E (config-if-range)#exit

    OLT4840E (config)#vlan 1-20

    OLT4840E (config-if-vlan)#switchport ethernet 0/2 ethernet 0/3

    OLT4840E (config-if-vlan)#exit

  - » Configure a região MST do OLT4840E.

    OLT4840E (config)#spanning-tree mst name RG1

    OLT4840E (config)#spanning-tree mst instance 1 vlan 1-10

  - » Configure Ethernet 0/1 como uma interface de borda.

    OLT4840E(config)#interface ethernet 0/1

    OLT4840E(config-if-ethernet-0/1)#spanning-tree mst portfast

    OLT4840E(config-if-ethernet-0/1)#exit

  - » Habilitar o MSTP

    OLT4840E(config)#spanning-tree mode mstp

    OLT4840E(config)#spanning-tree

- » Configure a OLT-D
  - » Crie VLAN de 1 a 20 e configure as portas Ethernet 0/1 e Ethernet 0/2 como portas trunk e adicione-as à VLAN 1 a 20.

    OLT4840E (config)#interface range ethernet 0/1 ethernet 0/2

    OLT4840E (config-if-range)#switchport mode trunk

    OLT4840E (config-if-range)#exit

    OLT4840E (config)#vlan 1-20

    OLT4840E (config-if-vlan)#switchport ethernet 0/1 ethernet 0/2

    OLT4840E (config-if-vlan)#exit

- » Configure a região do OLT-D.

  OLT4840E(config)#spanning-tree mst name RG2

  OLT4840E(config)#spanning-tree mst instance 1 vlan 1-10

  OLT4840E(config)#spanning-tree mst instance 2 vlan 11-20

- » Defina a prioridade do OLT-D no MSTI0 para 4096. Certifique-se de que o OLT-D seja o root da região CIST do RG2.

  OLT4840E(config)#spanning-tree mst instance 0 priority 4096

- » Defina a prioridade do OLT-D no MSTI 2 para 0. Certifique-se de que o OLT-D seja o root da região MSTI 2.

  OLT4840E(config)#spanning-tree mst instance 2 priority 0

- » Habilite o MSTP

  OLT4840E(config)#spanning-tree mode mstp

  OLT4840E(config)#spanning-tree

» Configure a OLT-B

- » Crie VLAN de 1 a 20 e configure as portas Ethernet 0/2 e Ethernet 0/3 como portas trunk e adicione-as à VLAN 1 a 20.

  OLT4840E (config)#interface range ethernet 0/2 ethernet 0/3

  OLT4840E (config-if-range)#switchport mode trunk

  OLT4840E (config-if-range)#exit

  OLT4840E (config)#vlan 1-20

  OLT4840E (config-if-vlan)#switchport ethernet 0/2 ethernet 0/3

  OLT4840E (config-if-vlan)#exit

- » Configure a região MST do OLTP.

  OLT4840E(config)#spanning-tree mst name RG2

  OLT4840E(config)#spanning-tree mst instance 1 vlan 1-10

  OLT4840E(config)#spanning-tree mst instance 2 vlan 11-20

- » Defina a prioridade do OLT-B no MSTI 1 a 0, assegure-se de que OLT-B seja o root do domínio MSTI.

  OLT4840E(config)#spanning-tree mst instance 1 priority 0

- » Configure Ethernet 0/1 como uma interface de borda.

  OLT4840E(config)#spanning-tree mode mstp

  OLT4840E(config)#spanning-tree

» Verificação da configuração:

» Execute o comando de exibição no OLT-C para ver o resultado da eleição e o status da porta de multiple spanning tree. Os resultados são os seguintes:

OLT4840E(config)#show spanning-tree mst instance 0 interface ethernet 0/1 ethernet 0/2

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 0-000a.5a13.f48e

Cist root is 0-000a.5a13.f48e,root port is

Region root is 0-000a.5a13.f48e,root port is

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20

External root path cost is 0,internal root path cost is 0

Port e0/1 of instance 0 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard enable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/1

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 20

Received BPDUs:TCN 0,RST 18,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 137,Config BPDU 0

Port e0/2 of instance 0 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard enable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/2

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 20

Received BPDUs:TCN 0,RST 85,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 86,Config BPDU 0

OLT4840E(config)#show spanning-tree mst instance 1 interface ethernet 0/1 ethernet 0/2

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 0-000a.5a13.f48e

Cist root is 0-000a.5a13.f48e,root port is

Region root is 0-000a.5a13.f48e,root port is

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20

External root path cost is 0,internal root path cost is 0

Port e0/1 of instance 1 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard enable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/1

Port is a(n) non-edge port,link type is point-to-point

Port time:RemainingHops 20

Received BPDUs:TCN 0,RST 18,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 182,Config BPDU 0

Port e0/2 of instance 1 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard enable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/2

Port is a(n) non-edge port,link type is point-to-point

Port time:RemainingHops 20

Received BPDUs:TCN 0,RST 130,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 131,Config BPDU 0

Como OLT-C tem a prioridade intra-CIST mais alta, OLT-C é selecionado como o root comum do CIST, e também é a o root regional do RG1. A porta Ethernet 0/1 e a porta Ethernet 0/2 de OLT-C são portas designadas no CIST. Eles estão no estado de encaminhamento.

OLT-C tem a prioridade mais alta no MSTI1 no domínio RG1, então OLT-C é selecionado como o root do domínio do MSTI1. Ethernet 0/1 e Ethernet 0/2 são calculados como as portas designadas no MSTI1. Eles estão no estado de encaminhamento.

» Execute o comando de exibição no dispositivo OLT-A para ver o resultado da eleição e o status da porta de multiple spanning tree. Os resultados são os seguintes:

OLT4840E(config)#show spanning-tree mst instance 0 interface ethernet 0/1 ethernet 0/2

ethernet 0/3

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 32768-000a.5a13.b13d

Cist root is 0-000a.5a13.f48e,root port is e0/3

Region root is 0-000a.5a13.f48e,root port is e0/3

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 18

External root path cost is 0,internal root path cost is 200000

Port e0/1 of instance 0 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 32768-000a.5a13.b13d,designated port is e0/1

Port is a(n) edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 19

Received BPDUs:TCN 0,RST 0,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 249,Config BPDU 0

Port e0/2 of instance 0 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 32768-000a.5a13.b13d,designated port is e0/2

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 19

Received BPDUs:TCN 0,RST 30,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 279,Config BPDU 0

Port e0/3 of instance 0 is forwarding

Port role is RootPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/1

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 19

Received BPDUs:TCN 0,RST 313,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 18,Config BPDU 0

OLT4840E(config)#show spanning-tree mst instance 1 interface ethernet 0/1

ethernet 0/2
ethernet 0/3
Current spanning tree protocol is MSTP
Spanning tree protocol is enable
Bridge id is 32768-000a.5a13.b13d
Cist root is 0-000a.5a13.f48e,root port is e0/3
Region root is 0-000a.5a13.f48e,root port is e0/3
Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 19
External root path cost is 0,internal root path cost is 200000

Port e0/1 of instance 1 is forwarding
Port role is DesignatedPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 32768-000a.5a13.b13d,designated port is e0/1
Port is a(n) edge port,link type is point-to-point
Port time:RemainingHops 19
Received BPDUs:TCN 0,RST 0,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 273,Config BPDU 0

Port e0/2 of instance 1 is forwarding
Port role is DesignatedPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 32768-000a.5a13.b13d,designated port is e0/2
Port is a(n) non-edge port,link type is point-to-point
Port time:RemainingHops 19
Received BPDUs:TCN 0,RST 30,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 303,Config BPDU 0

Port e0/3 of instance 1 is forwarding

Port role is RootPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/1

Port is a(n) non-edge port,link type is point-to-point

Port time:RemainingHops 19

Received BPDUs:TCN 0,RST 337,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 18,Config BPDU 0

Ethernet 0/3 do OLT-A é a porta root em CIST e MSTI1. Ethernet 0/2 é a porta designada em CIST e MSTI1. Eles estão no estado de encaminhamento. O Ethernet 0/1 é a porta de borda e no estado de encaminhamento.

» Execute o comando de exibição no OLT-D para ver o resultado da eleição e o status da porta de multiple spanning tree. Os resultados são os seguintes:
OLT4840E(config)#show spanning-tree mst instance 0 interface ethernet 0/1 ethernet 0/2

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 4096-0000.0077.8899

Cist root is 0-000a.5a13.f48e,root port is e0/2

Region root is 4096-0000.0077.8899,root port is e0/2

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20

External root path cost is 200000,internal root path cost is 0

Port e0/1 of instance 0 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 4096-0000.0077.8899,designated port is e0/1

Port is a(n) non-edge port, link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 20

Received BPDUs:TCN 0,RST 663,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 58,Config BPDU 0

Port e0/2 of instance 0 is forwarding

Port role is RootPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 0-000a.5a13.f48e,designated port is e0/2

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 20

Received BPDUs:TCN 0,RST 652,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 655,Config BPDU 0

OLT4840E(config)#show spanning-tree mst instance 1 interface ethernet 0/1 ethernet 0/2

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 32768-0000.0077.8899

Cist root is 0-000a.5a13.f48e,root port is e0/2

Region root is 0-0000.0a0a.0001,root port is e0/1

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20

External root path cost is 200000,internal root path cost is 200000

Port e0/1 of instance 1 is forwarding

Port role is RootPort, priority is 128

Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 0-0000.0a0a.0001,designated port is e0/3
Port is a(n) non-edge port,link type is point-to-point
Port time:RemainingHops 19
Received BPDUs:TCN 0,RST 973,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 370,Config BPDU 0

Port e0/2 of instance 1 is forwarding
Port role is MasterPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 32768-0000.0077.8899,designated port is e0/2
Port is a(n) non-edge port,link type is point-to-point
Port time:RemainingHops 19
Received BPDUs:TCN 0,RST 962,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 655,Config BPDU 0

OLT4840E(config)#show spanning-tree mst instance 2 interface ethernet 0/1 ethernet 0/2
Current spanning tree protocol is MSTP
Spanning tree protocol is enable
Bridge id is 0-0000.0077.8899
Cist root is 0-000a.5a13.f48e,root port is e0/2
Region root is 0-0000.0077.8899,root port is
Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20
External root path cost is 200000,internal root path cost is 0

Port e0/1 of instance 2 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 0-0000.0077.8899,designated port is e0/1

Port is a(n) non-edge port,link type is point-to-point

Port time:RemainingHops 20

Received BPDUs:TCN 0,RST 1003,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 401,Config BPDU 0

Port e0/2 of instance 2 is forwarding

Port role is MasterPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 0-0000.0077.8899,designated port is e0/2

Port is a(n) non-edge port,link type is point-to-point

Port time:RemainingHops 20

Received BPDUs:TCN 0,RST 992,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 655,Config BPDU 0

O OLT-D tem uma prioridade mais baixa no CIST do que o OLT-C e Ethernet 0/2 do OLT-D é calculado como a porta root no CIST. Ao mesmo tempo, porque o OLT-C e o OLT-D não pertencem ao mesmo domínio, Ethernet 0/2 do OLT-D é calculado como a porta mestre no MSTI1 e no MSTI2. O OLT-D tem precedência sobre o OLT-B no CIST e Ethernet 0/1 do OLT-D é calculado como a porta designada no CIST.

No MSTI1, o OLT-D tem uma prioridade menor do que o OLT-B. O OLT-B é eleito como ao root regional MSTI1. Portanto, Ethernet 0/1 do OLT-D é calculado como a porta root.

No MSTI2, o OLT-D tem precedência sobre o OLT-B. O OLT-D é eleito como o root regional MSTI2. Portanto, Ethernet 0/ do OLT-D é calculado como a porta designada.

» Execute o comando de exibição no OLT-B para ver o resultado da eleição e o status da porta de multiple spanning tree. Os resultados são os seguintes:

OLT4840E(config)#show spanning-tree mst instance 0 interface ethernet 0/1 ethernet 0/2

ethernet 0/3

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 32768-0000.0a0a.0001

Cist root is 0-000a.5a13.f48e,root port is e0/3

Region root is 4096-0000.0077.8899,root port is e0/3

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 19

External root path cost is 200000,internal root path cost is 200000

Port e0/1 of instance 0 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 32768-0000.0a0a.0001,designated port is e0/1

Port is a(n) edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 19

Received BPDUs:TCN 0,RST 0,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 24,Config BPDU 0

Port e0/2 of instance 0 is discarding

Port role is AlternatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 32768-000a.5a13.b13d,designated port is e0/2

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 20

Received BPDUs:TCN 0,RST 770,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 7,Config BPDU 0

Port e0/3 of instance 0 is forwarding

Port role is RootPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state

Designated bridge is 4096-0000.0077.8899,designated port is e0/1

Port is a(n) non-edge port,link type is point-to-point

Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 19

Received BPDUs:TCN 0,RST 783,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 773,Config BPDU 0

OLT4840E(config)#show spanning-tree mst instance 1 interface ethernet 0/1 ethernet 0/2

ethernet 0/3

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Bridge id is 0-0000.0a0a.0001

Cist root is 0-000a.5a13.f48e,root port is e0/3

Region root is 0-0000.0a0a.0001,root port is

Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 19

External root path cost is 200000,internal root path cost is 0

Port e0/1 of instance 1 is forwarding

Port role is DesignatedPort, priority is 128

Port external path cost is 200000,internal path cost is 200000

Root guard disable and port is not in root-inconsistent state
Designated bridge is 0-0000.0a0a.0001,designated port is e0/1
Port is a(n) edge port,link type is point-to-point
Port time:RemainingHops 20
Received BPDUs:TCN 0,RST 0,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 96,Config BPDU 0

Port e0/2 of instance 1 is discarding
Port role is AlternatedPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 0-0000.0a0a.0001,designated port is e0/2
Port is a(n) non-edge port,link type is point-to-point
Port time:RemainingHops 20
Received BPDUs:TCN 0,RST 842,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 7,Config BPDU 0

Port e0/3 of instance 1 is forwarding
Port role is DesignatedPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 0-0000.0a0a.0001,designated port is e0/3
Port is a(n) non-edge port,link type is point-to-point
Port time:RemainingHops 20
Received BPDUs:TCN 0,RST 855,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 846,Config BPDU 0

OLT4840E(config)#show spanning-tree mst instance 2 interface ethernet 0/1 ethernet 0/2
ethernet 0/3

Current spanning tree protocol is MSTP
Spanning tree protocol is enable
Bridge id is 32768-0000.0a0a.0001
Cist root is 0-000a.5a13.f48e,root port is e0/3
Region root is 0-0000.0077.8899,root port is e0/3
Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 19
External root path cost is 200000,internal root path cost is 200000
Port e0/1 is not a member of instance 2

Port e0/2 of instance 2 is discarding
Port role is AlternatedPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 32768-0000.0a0a.0001,designated port is e0/2
Port is a(n) non-edge port,link type is point-to-point
Port time:RemainingHops 19
Received BPDUs:TCN 0,RST 858,Config BPDU 0
Transmitted BPDUs:TCN 0,RST 7,Config BPDU 0

Port e0/3 of instance 2 is forwarding
Port role is RootPort, priority is 128
Port external path cost is 200000,internal path cost is 200000
Root guard disable and port is not in root-inconsistent state
Designated bridge is 0-0000.0077.8899,designated port is e0/1
Port is a(n) non-edge port,link type is point-to-point

Port time:RemainingHops 19

Received BPDUs:TCN 0,RST 871,Config BPDU 0

Transmitted BPDUs:TCN 0,RST 861,Config BPDU 0

O OLT-D tem uma prioridade mais alta no CIST do que o OLT-B. Ethernet 0/2 do OLT-B é calculado como uma porta alternativa. Como o OLT-B não está no mesmo domínio que OLT-A, a porta do OLT-B é calculada como portas alternativas no MSTI1 e no MSTI2.

No MSTI1, a prioridade do OLT-D é menor que a do OLT-B. O OLT-B é eleito como a raiz do MSTI1. Portanto, Ethernet 0/3 do OLT-B é calculado como a porta designada.

No MSTI2, a prioridade do OLT-D é maior que a do OLT-B. O OLT-D é eleito como a raiz do MST2. Portanto, Ethernet 0/3 do OLT-B é calculado como a porta raiz.

A porta Ethernet 0/1 do OLT-B é uma porta de bordo e contido apenas no MSTI0 e no MSTI1. Não está incluído no MSTI2. Portanto, está no estado de encaminhamento no MSTI0 e no MSTI1 e não é exibido no MSTI2.

20. GSTP

20.1. Introdução ao GSTP

O OLT está conectado ao cliente. Se houver um loop na rede do cliente, ele afetará toda a rede do operador. GSTP serve para resolver este problema. Depois que o GSTP é ativado em uma porta, o OLT envia periodicamente uma mensagem de detecção. Se a rede do cliente tiver um loop, o OLT receberá a mensagem de detecção. Nesse caso, o OLT considera que a rede do cliente possui loop e a porta conectada à porta do cliente, de acordo com a estratégia de tratamento, é descartada ou desligada.

Algumas pessoas podem perguntar: o spanning tree também pode funcionar como uma detecção de loop remoto, por que precisaríamos de GSTP? Isso ocorre porque se a rede do cliente também possui equipamentos para abrir o spanning tree, uma mudança na topologia da rede do cliente facilmente afeta a rede. Se a rede geral é conectada a porta do cliente que não pode abrir o spanning tree, como uma alternativa existe o GSTP.

20.2. Configuração do GSTP

Habilitação da configuração

» Habilitar em todas as portas:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar em todas as portas	**[no] spanning-tree remote-loop-detect interface**	Obrigatório
Visualização das informações de configuração	**show spanning-tree remote-loop-detect interface**	Opcional

» Habilitar apenas para a porta designada:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Habilitar para a porta designada	**[no] spanning-tree remote-loop-detect interface ethernet** port-id	Obrigatório
Acesse o modo de configuração de porta	**interface ethernet** port-id	Obrigatório
Habilitar para a porta	**[no]spanning-tree remote-loop-detect**	Obrigatório
Visualização das informações de configuração	**show spanning-tree remote-loop-detect interface [ethernet** port-id**]**	Opcional

Obs.: *existem duas maneiras de configurar para uma porta designada: 1. Digite a porta especificada e ative o GSTP. 2. Digite a porta especificada quando a porta estiver ativada globalmente. Ambos possuem o mesmo efeito, apenas uma das ações é necessária.*

Configuração da regra de processamento

Quando o GSTP detecta a existência de loop, existem duas ações possíveis: uma é descartar os pacotes da porta, a outra é o desligamento da porta, e depois periodicamente restaurar a porta; o uso padrão é a porta descartar seus pacotes.

» Configuração da regra de processamento:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da regra de processamento	**spanning-tree remote-loop-detect action { shutdown | discarding }**	Obrigatório

Configuração do tempo de recuperação

Quando GSTP detecta que existe um loop e o comando shutdown é usado, a porta desligada recupera periodicamente. O período de recuperação padrão é de 20 segundos e pode ser modificado conforme necessário. Se estiver configurado como 60s, isso significa que ele não será restaurado automaticamente.

» Configuração do tempo de recuperação:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Configuração da regra de processo de desligamento	**spanning-tree remote-loop-detect action shutdown**	Obrigatório
Configuração do tempo de recuperação	**spanning-tree remote-loop-detect recover-time** value	Opcional
Visualização das informações de configuração	**show spanning-tree remote-loop-detect interface**	Opcional

Configuração do período de detecção

Após a ativação da função *GSTP*, as mensagens de detecção GSTP são periodicamente enviadas a partir da porta correspondente. Se o OLT receber uma mensagem GSTP de si mesmo, ele considera que existe um loop e o processa de acordo com a política de processamento. O tempo de detecção é 5s por padrão, o usuário pode modificar o tempo de transmissão.

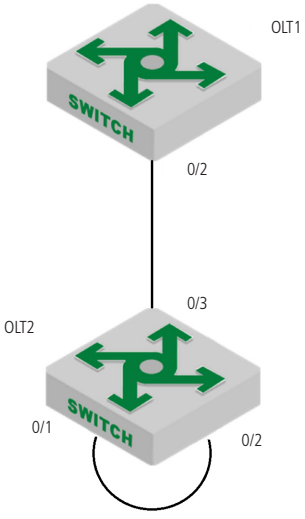
» Configuração do período de detecção:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	Obrigatório
Configuração do período de detecção	**spanning-tree remote-loop-detect interval-time** value	Opcional
Visualização das informações de configuração	**show spanning-tree remote-loop-detect interface**	Opcional

Exemplo de configuração de GSTP

» Requisitos de rede:

Conforme exibido na figura, a porta 2 do OLT1 possui o GSTP ativado e o OLT1 está conectado ao OLT2. Quando há um loop no OLT2, o OLT1 detecta que há um loop na porta 2, está descarta os pacotes por padrão.



GSTP

» Procedimento de configuração:

» Configuração do OLT1: habilite a função *GSTP* da porta 2.

SW1(config)# spanning-tree remote-loop-detect interface ethernet 0/9

SW1(config)#interface range ethernet 0/2

SW1(config-if- 0/2)#no spanning-tree

» OLT2 conecta a porta 1 e a porta 2 para formar um loop, o GSTP do OLT1 é exibido como exibido a seguir:

OLT1(config)#show spanning-tree remote-loop-detect interface ethernet 0/2

Loopback-detection action is Discarding

The interval time is 5 second(s)

The recovery time is 20 second(s)

Port Information:

port loopback status

e0/2 Enable Discarding

» Depois que a política de processamento GSTP for alterada para desligamento, o GSTP é exibido da seguinte forma:

OLT1(config)#spanning-tree remote-loop-detect action shutdown

OLT1(config)#show spanning-tree remote-loop-detect interface ethernet 0/2

Loopback-detection action is Shutdown

The interval time is 5 second(s)

The recovery time is 20 second(s)

Port Information:

port loopback status

e0/2 Enable Shutdown

21. Configuração de PVST

21.1. Introdução ao PVST

Per-VLAN Spanning Tree é o protocolo privado de spanning tree da Cisco. A VLAN está mapeada para a instância que é apenas uma instância correspondente a uma VLAN, pertencente a uma relação de mapeamento.

PVST + é uma melhoria da Cisco baseada no PVST para resolver o problema de trabalhar com outros OLTs de outros fornecedores, permitindo que as informações do spanning tree padrão IEEE passem para o PVST.

PVST + executa o spanning tree padrão na VLAN 1, e o protocolo PVST é executado em outras VLANs. Como o número de instâncias é limitado, a VLAN 1 e outras VLANs não configuradas são uniformemente mapeadas para a instância 0 e outras VLANs que precisam ser configuradas são mapeadas para outras instâncias. Assim, execute o protocolo padrão do spanning tree no caso 0 e outros exemplos executem o protocolo PVST.

21.2. Configuração do PVST

Configuração do modo *PVST*

Depois de habilitar o spanning tree globalmente e configurar o modo *PVST*, por padrão, todas as portas participam do cálculo da topologia PVST. Rapid-PVST pode tornar a transição do estado da porta rápida.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Iniciar o spanning tree	**spanning-tree**	Obrigatório
Configuração do modo *PVST*	**spanning-tree mode pvst**	Obrigatório, por padrão é RSTP
Configuração do modo *PVST fast*	**spanning-tree mode rapid-pvst**	Opcional

Configuração dos parâmetros de tempo do PVST

Os parâmetros de tempo PVST incluem: forward delay, hello time, max age e cálculo do spanning tree para PVST.

» Configuração do hello time:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Configuração do hello time	**spanning-tree pvst hello-time** hello-time	Opcional, por padrão é de *2s*

Um valor de Hello Time excessivamente longo faz com que a bridge considere uma falha de link e recalcule o spanning tree, porque o link perde a mensagem. Um valor de Hello Time excessivamente curto faz com que a bridge envie informações de configuração com frequência, o que aumenta a carga da rede e da CPU. O Hello Time está no intervalo de 1 a 10 segundos. Recomenda-se usar o valor padrão de 2 segundos. O horário da hora deve ser inferior ou igual ao forward time-2.

» Configuração do foward time:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do forward time	**spanning-tree pvst forward-time** forward-time	Opcional, por padrão é de *15s*

» Configuração do max time:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do max-age	**spanning-tree pvst max-age** max-age	Opcional, por padrão é de *20s*

» **Max-age:** define a idade máxima para a mensagem do protocolo PVST. Se ela expirar, a mensagem será descartada. Se esse valor for muito pequeno, o cálculo do spanning tree será mais frequente, o congestionamento da rede pode ser confundido com a falha do link de rede; se esse valor for muito grande, ele não é propício para a detecção da falha de ligação em tempo. O max age está na faixa de 6 a 40 segundos. O valor do tempo Max Age depende do diâmetro da rede comutada. Recomenda-se o valor padrão de *20 segundos*. O Max Age deve ser maior ou igual a *2 * (Hello Time + 1)* e menor que ou igual a *2 * (Foward time -1)*.

Configuração de VLAN e mapeamento de instância

Uma VLAN é mapeada para uma instância PVST, e uma instância corresponde a uma VLAN.

» Configuração de VLAN e mapeamento de instância:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da VLAN e mapeamento de instânci	**spanning-tree pvst ins-id** instance-id **vlan** vlan-id	Obrigatório

Configuração de prioridade de instância PVST

No PVST, a prioridade de uma bridge é baseada nos parâmetros de cada MSTI. A prioridade da bridge, juntamente com a prioridade da porta e o custo do caminho da porta, determina a topologia de cada MSTI e constitui a base para o equilíbrio da carga do link.

O valor da prioridade da bridge do OLT determina se o OLT pode ser selecionado como a bridge root do spanning tree. Ao configurar uma prioridade de bridge menor, o usuário pode especificar que um OLT se torna a bridge root do spanning tree.

» Configuração de prioridade de instância PVST:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração de prioridade de instância PVST	**spanning-tree pvst instance** instance-id **priority** priority	Opcional, por padrão o valor é *32768*

Configuração do custo da rota da porta

Ao configurar o custo do caminho de uma porta, você pode transformar mais facilmente a porta em uma porta root ou uma porta designada.

O custo do caminho de uma porta depende da taxa de ligação da porta. Quanto maior for a taxa de link, menor será a configuração do parâmetro. O protocolo PVST detecta automaticamente a taxa de ligação da porta atual e o traduz no custo do caminho correspondente.

Configurar o custo do caminho de uma porta Ethernet fará com que o spanning tree seja recalculado. O custo de um caminho de porta varia de 1 a 65.535. Recomenda-se usar o valor padrão, de modo a deixar o protocolo PVST calcular o custo do caminho da porta atual. Por padrão, o custo do caminho é determinado com base na taxa atual da porta.

O custo do caminho da porta padrão é baseado na velocidade da porta. O padrão é 200.000 quando a velocidade da porta é de 10M; 200.000 quando a porta é 100M; 20.000 quando a porta é 1000M. Quando a taxa de porta não está disponível, o custo do caminho é de 200.000 por padrão.

» Configuração do custo da rota da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configure a prioridade da instância PVST	**spanning-tree pvst instance** instance-id **path-cost** cost-num	Opcional

Configuração de prioridade de porta

No PVST, a prioridade da porta é baseada nos parâmetros de cada MSTI. Ao configurar a prioridade de uma porta, você pode facilmente configurar uma porta para uma porta root.

Quanto menor for o valor da prioridade, maior será a prioridade. Alterar a prioridade de uma porta Ethernet fará com que o spanning tree seja recalculado.

» Configuração da prioridade da porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Configuração da prioridade da porta	**spanning-tree pvst instance** instance-id **priority** priority	Opcional, por padrão o valor é de *128*

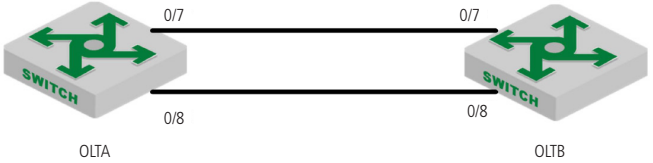
Visualização e manutenção do PVST

» Visualização e manutenção do PVST:

Operação	Comando	Obrigatório/ opcional
Visualização da informação de configuração do PVST	**show spanning-tree pvst instance brief l** instance-list	Opcional
Visualização da informação de depuração do PVST	**debug pvst**	Opcional

21.3. Exemplo de configuração do PVST

» Requisitos de rede:



Conforme exibido na figura acima, configure o PVST exigindo que os dados da VLAN 2 passem pelo link da porta 0/7 e os dados da VLAN 3 para passar pelo link da porta 0/8. O OLT está na configuração padrão e o endereço MAC do OLTA é 00:0a:5a:00:04:00, o endereço MAC do OLTB é 00:0a:5a:00:04:1e.

» Passos de configuração e validação de resultado:

1. 0/7 e 0/8 dos OLTA e OLT B são adicionados à VLAN 2 e à VLAN 3, e estão configurados no modo *Trunk*.

   OLT4840E(config)#vlan 2-3

   OLT4840E(config-if-vlan)#switchport ethernet 0/7 ethernet 0/8

OLT4840E(config-if-vlan)#exit

OLT4840E(config)#interface range ethernet 0/7 ethernet 0/8

OLT4840E(config-if-range)#switchport mode trunk

OLT4840E(config)#vlan 2-3

OLT4840E(config-if-vlan)#switchport ethernet 0/7 ethernet 0/8

OLT4840E(config-if-vlan)#exit

OLT4840E(config)#interface range ethernet 0/7 to ethernet 0/8

OLT4840E(config-if-range)#switchport mode trunk

OLT4840E(config-if-range)#

2. Habilite o spanning tree, configure o modo do spanning tree como PVST, mapear VLAN 2 para PVST instância 2 e map VLAN 3 para PVST instância 3

OLT4840E(config)#spanning-tree

OLT4840E(config)#spanning-tree mode pvst

OLT4840E(config)#spanning-tree pvst ins-id 2 vlan 2

OLT4840E(config)#spanning-tree pvst ins-id 3 vlan 3

OLT4840E(config)#spanning-tree

OLT4840E(config)#spanning-tree mode pvst

OLT4840E(config)#spanning-tree pvst ins-id 2 vlan 2

OLT4840E(config)#spanning-tree pvst ins-id 3 vlan 3

3. Ao consultar as instâncias PVST separadamente, OLTB é selecionado como a bridge root da instância 2 e da instância 3, 0/8 é a porta selecionada e o estado bloqueado na instância 2 e na instância 3, porque o MAC do OLTB é menor.

OLT4840E(config)#show spanning-tree pvst instance brief 2

Current spanning tree protocol is pvst

PVST Instance 2 vlans mapped: 2

Bridge ID 32768-000a.5a00.041e

Root ID 32768-000a.5a00.041e

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15

Root time HelloTime 2,MaxAge 20,ForwardDelay 15

Root path cost: 0

PortID Config Role Sts PathCost Prio.Nbr Type

---

e0/7 YES Design FWD 200000 128.7 P2P

e0/8 YES Design FWD 200000 128.8 P2P

OLT4840E(config)#show spanning-tree pvst instance brief 3

Current spanning tree protocol is pvst

PVST Instance 3 vlans mapped: 3

Bridge ID 32768-000a.5a00.041e

Root ID 32768-000a.5a00.041e

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15

Root time HelloTime 2,MaxAge 20,ForwardDelay 15

Root path cost: 0

PortID Config Role Sts PathCost Prio.Nbr Type

---

e0/7 YES Design FWD 200000 128.7 P2P

e0/8 YES Design FWD 200000 128.8 P2P

OLT4840E(config)#show spanning-tree pvst instance brief 2

Current spanning tree protocol is pvst

PVST Instance 2 vlans mapped: 2

Bridge ID 32768-000a.5a00.0400

Root ID 32768-000a.5a00.041e

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15

Root time HelloTime 2,MaxAge 20,ForwardDelay 15

Root path cost: 200000

PortID Config Role Sts PathCost Prio.Nbr Type

---

e0/7 YES Root FWD 200000 128.7 P2P

e0/8 YES Alte DIS 200000 128.8 P2P

OLT4840E(config)#show spanning-tree pvst instance brief 3

Current spanning tree protocol is pvst

PVST Instance 3 vlans mapped: 3

Bridge ID 32768-000a.5a00.0400

Root ID 32768-000a.5a00.041e

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15

Root time HelloTime 2,MaxAge 20,ForwardDelay 15

Root path cost: 200000

PortID Config Role Sts PathCost Prio.Nbr Type

---

e0/7 YES Root FWD 200000 128.7 P2P

e0/8 YES Alte DIS 200000 128.8 P2P

4. Neste momento, os dados de VLAN 2 e VLAN 3 passam pelo link correspondente a porta 0/7 e não estão em conformidade com a expectativa. Agora, modificando o valor COST da porta 0/8 do OLTA, o custo para a porta root é menor do que a da porta 0/7:

OLT4840E(config)#interface ethernet 0/8

OLT4840E(config-if-ethernet-0/8)#spanning-tree pvst instance 3 path-cost 20000

5. Veja a informação da instância PVST. Você pode ver que a porta 0/8 da OLTA é reeleita como a porta root e tem o status de encaminhamento. Neste momento, pacotes de VLAN 3 são encaminhados através do link onde 0/8 está localizado.

OLT4840E(config-if-ethernet-0/8)#show spanning-tree pvst instance brief 3

Current spanning tree protocol is pvst

PVST Instance 3 vlans mapped: 3

Bridge ID 32768-000a.5a00.0400

Root ID 32768-000a.5a00.041e

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15

Root time HelloTime 2,MaxAge 20,ForwardDelay 15

Root path cost: 20000

PortID Config Role Sts PathCost Prio.Nbr Type

---

e0/7 YES Alte DIS 200000 128.7 P2P

e0/8 YES Root FWD 20000 128.8 P2P

22. Configuração de ERRP

22.1. Introdução a função de ERRP

Ethernet Redundant Ring Protocol (ERRP) é um protocolo especificamente projetado para um anel Ethernet. Ele evita broadcast storms (um volume alto de broacast) causados por loops de dados; quando um link no anel é desconectado, o caminho de comunicação entre os nós na rede pode ser restaurado rapidamente. Em comparação com o STP, o ERRP possui mais rapidez na convergência topológica e no tempo de convergência independentemente do número de nós na rede.

Para evitar conflitos entre ERRP e STP no cálculo do congestionamento da porta / status de liberação, estas funções são mutuamente exclusivos na porta. Ou seja, o protocolo STP não pode ser ativado nas portas conectadas ao anel ERRP.

Introdução do conceito

Região ERRP

A região ERRP é identificada por um ID (número inteiro). Um conjunto de grupos OLT configurados com o mesmo ID de domínio, VLAN de controle e conectados entre si formam um domínio ERRP. Este domínio tem os seguintes elementos constituintes:

- loop ERRP.
- VLAN de controle pelo ERRP.
- Nó mestre.
- Nó de transporte.
- Nó de borda e nó de borda assistente.

Loop ERRP

O anel ERRP também é identificado por um ID inteiro, e corresponde fisicamente a uma topologia Ethernet conectada em anel. Um domínio ERRP consiste em um ou mútiplos anéis conectados entre si, um deles é o *anel mestre* e os outros são *sub-anéis*. Eles são distinguidos pelo nível especificado no momento da sua configuração, o nível mestre é 0 e o seguinte é 1.

O anel ERRP possui dois estados:

- **Health state:** todos os links estão normais e o anel está conectado.

» **Fault state:** um link está com defeito. Um ou muitos links físicos da rede estão desativados.

Papel do nó

O nó do anel ERRP é dividido em *nó mestre* e *nó de trânsito*, especificado pelo usuário. O primeiro é o nó de decisão e controle para proteção. Deve haver apenas um *nó mestre*, todos os outro são chamados de nós de trânsito.

Se mais de um anel se cruzarem, eles são designados como um *nó de borda* e como *nó de borda assistente.* O papel de ambos no *anel mestre* é de nó de transição, no *sub-anel* é de nó de borda e de nó de borda assistente. O papel do *sub-anel* pode ser especificado pelo usuário. Não existe um requisito especial para distinguir os dois nós.

Papel da porta

Cada nó de um anel ERRP possui duas portas conectadas. O usuário pode especificar uma delas como a porta principal e a outra como a porta secundária. A porta principal do nó mestre é usada para enviar mensagem de detecção (mensagem de Hello), recebida pela porta secundária, as portas do nó de transição funcionam de formas similares. Para evitar que o circuito cause um broadcast storm, se o anel ERRP estiver normal, a porta secundária será bloqueada e todas as outras entrarão no estado de encaminhamento.

Se vários anéis de ERRP se cruzarem, as portas nos nós de intersecção que acessam o anel primário e o sub-anel (ou seja, a porta do anel primário e o link comum do sub -anel) são chamadas portas comuns. Somente as portas que acessam os sub-anéis são chamadas portas de borda. Conceitualmente, uma porta pública não é considerada como uma porta de um sub-anel, é considerada parte do anel principal. A alteração de estado do link público apenas é relatada ao nó mestre do anel primário. O nó mestre do sub-anel não precisa saber.

VLAN de controle

A VLAN de controle é usada para transmitir pacotes de protocolo ERRP.

Cada região ERRP possui duas VLANs de controle, chamadas *VLAN de controle primário* e *VLAN de controle secundário*. A mensagem de protocolo do anel primário é propagada na primeira e a mensagem de protocolo do sub-anel é propagada na segunda. O usuário precisa especificar a *VLAN de controle primário*, a VLAN com ID um número acima da ID especificada é usada como *VLAN de controle secundário*.

A única porta (porta ERRP) que conecta a Ethernet de cada switch pertence à *VLAN de controle*, as outras portas não podem se juntar a ela. A porta ERRP do anel primário pertence às duas VLANs. A porta ERRP do sub-anel pertence à *VLAN de controle secundário*. A VLAN de dados pode conter portas ERRP ou portas não-ERRP. O anel primário é considerado um nó lógico do sub-anel. Os pacotes de protocolo do sub-anel são transmitidos através do anel primário e processados neles como dados. Os pacotes de protocolo do anel primário são transmitidos somente nele mesmo. Não acesse os sub-anéis.

Função de solicitação de consulta

ERRP é usado em conjunto com IGMP-Snooping, se a topologia dele mudar, o estado de encaminhamento da porta será alterado. Neste caso, se o multicast não for atualizado, o encaminhamento multicast pode apresentar falhas. Quando ocorre uma alteração, o dispositivo envia uma mensagem de consulta IGMP geral para todas as portas para gerar um relatório de atualização da entrada de multicast.

Mensagem de protocolo

Message HELLO

A mensagem hello é iniciada pelo nó mestre e detecta a integridade do loop da rede. O nó mestre envia periodicamente a mensagem HELLO da sua porta primária e o nó de transição a a encaminha para o próximo, que é então recebido pela porta secundária. O período de envio é definido pelo timer Hello.

Mensagem de LINK_UP

A mensagem LINK_UP é iniciada pelo nó que recuperou o seu link. Ele informa ao nó mestre de que há recuperação de link no loop.

Mensagem de LINK_DOWN

A mensagem LINK_DOWN é iniciada pelo nó que apresentar uma falha no link. Ele informa o nó mestre esta falha de link no loop, abrindo-o.

Mensagem de COMMON_FLUSH_FDB

É iniciado pelo nó mestre e informa os outros nós para atualizarem suas respectivas tabelas de encaminhamento de endereço MAC. É enviado na falha ou na recuperação do link.

Mensagem de COMPLETE_FLUSH_FDB

É iniciado pelo nó mestre e informa os outros nós para atualizarem suas respectivas tabelas de encaminhamento de endereço MAC e bloqueia temporariamente o nó de trânsito e a VLAN de dados. É enviado quando a recuperação do link (ou seja, a porta secundária do nó mestre recebe os pacotes Hello) está concluída.

Mensagem de EDGE_HELLO

A mensagem EDGE_HELLO é iniciada pelo nó de borda do sub-anel para verificar a integridade do loop do anel principal no domínio.

Ela é enviada periodicamente pelas duas portas conectadas ao anel primário, que a processa como uma mensagens dados.

Mensagem de MAJOR_FAULT

A mensagem MAJOR_FAULT é originada pelo nó de borda assistente e informa ao nó de borda que o anel primário do domínio está com falha. Quando o nó de borda assistente do anel não receber a mensagem EDGE_HELLO, ele envia uma mensagem MAJOR_FAULT. Após o nó do sub-anel receber esta mensagem, ele a encaminha diretamente para o próximo nó até, finalmente, ele mesmo a receber. Esta mensagem é emitida periodicamente, o período de envio é o timer Edge Hello.

Principio de operação

Health status

O nó mestre envia periodicamente a mensagem hello da sua porta principal, que, por sua vez, viaja através dos nós de trânsito do anel. Se a porta secundária do nó mestre receber uma mensagem de Hello antes dela expirar, considera-se que o anel ERRP está em estado *health*. O estado do nó mestre reflete a integridade do anel. Quando a rede do anel está em um estado íntegro (*health*), ele bloqueia sua porta secundária para evitar que a mensagem de dados forme um loop de transmissão.

Falha no link

Dois mecanismos são fornecidos para detectar falhas de link:

» Escalonamento e processamento do LINK_DOWN:

Quando uma porta ERRP do nó de trânsito detecta uma porta em Link Down, é enviada uma mensagem LINK_DOWN para o nó mestre da porta ERRP conectada a falha.

Depois de receber a mensagem, o estado do nó é imediatamente alterado para FAULT. O bloqueio da porta secundária é desativado. A tabela FDB é atualizada e uma mensagem COMMON_FLUSH_FDB é enviada das portas primária e secundária para notificar os nós de trânsito para atualizarem suas respectivas tabelas FDB e aprenderem a nova topologia.

» Mecanismo de polling:

O mecanismo de relatório de falhas é iniciado pelo nó de trânsito. Para evitar que a mensagem LINK_DOWN se perca durante a transmissão, o nó mestre implementa o mecanismo de Polling. Este mecanismo é no qual o nó mestre detecta ativamente o estado da rede. Ele envia periodicamente a mensagem HELLO da sua porta principal e, em seguida, transmite-a através dos nós de transmissão.

Se o próprio nó mestre receber a mensagem HELLO da porta secundária a tempo, isso indica que a rede do anel está completo e manterá a porta secundária bloqueada. Se não receber a mensagem HELLO no tempo especificado, considera-se que ocorreu uma falha. O processo de tratamento de falhas é o mesmo que o mecanismo de processo do LINK_DOWN.

Recuperação do link

Há duas situações para lidar com a recuperação de link:

» Escalonamento e processamento do LINK_UP

Depois que as portas do nó de trânsito que pertencem à região ERRP são reconectadas, o nó mestre pode demorar para descobrir o link recuperado. Com isso, a rede pode formar um loop temporário, causando um broadcast storm.

Para evitar isso, o nó de trânsito move-se para o estado de pré-encaminhamento e bloqueia imediatamente a porta que acabou de ser recuperada, depois de encontrar a porta que acessa a reconexão da rede de anel. Ao mesmo tempo, o nó de transmissão envia uma mensagem LINK_UP para o nó mestre. Depois de receber a mensagem LINK_UP do nó transmissor, ele envia um pacote COMMON_FLUSH_FDB das portas principal e secundária para notificar todos os nós para se atualizarem. A porta recuperada pelo nó de trânsito apenas libera o estado bloqueado depois de receber o pacote COMPLETE_FLUSH_FDB ou depois do timer do pré-encaminhamento expirar.

A resposta do nó mestre para a mensagem LINK_UP não representa a recuperação da rede de anel. Se vários links falharem e, em seguida, um dos links for restaurado, o mecanismo de relatório LINK_UP e o mecanismo de resposta do nó mestre são introduzidos para atualizar rapidamente as tabelas FDB dos nós no anel.

» Processamento de recuperação de rede de anel:

O processamento de recuperação de rede de anel é iniciado pelo nó principal. O nó mestre envia as mensagens Hello periodicamente da porta principal. Depois que o link defeituoso na for restaurado, o nó mestre receberá suas próprias mensagens de teste. Neste caso, o nó mestre primeiro move o estado de volta para o estado completo, bloqueia a porta secundária e, em seguida, envia a mensagem COMPLETE_FLUSH_FDB. Então, o nodo de transição volta para o estado Link_Up, libera a porta temporariamente bloqueada e atualiza a tabela FDB.

Se a mensagem COMPLETE_FLUSH_FDB for perdida durante a transmissão, um mecanismo de backup é adotado para recuperar a porta temporariamente bloqueada. Se ela não for recebida no tempo especificado, a porta restaura a comunicação de dados.

Processamento de cruzamento de loops

O multi-anel e single-anel são quase os mesmos. A diferença entre eles é que no multi-anel vários anéis são introduzidos no mecanismo de detecção do estado do canal, depois que este é interrompido, a porta de borda é bloqueada antes que a porta secundária do nó mestre seja liberada, para impedir que o ciclo de dados se forme. Para obter detalhes, consulte o mecanismo de verificação do estado do canal do protocolo do subcanal no anel principal.

Além disso, quando um nó no anel mestre recebe uma mensagem COMUN-FLUSH-FDB ou COMPLETE-FLUSH-FDB do sub-anel, ele atualizará a tabela FDB. Isso não faz com que o nó de trânsito do sub-anel libere a porta temporariamente bloqueada.

Obs.: *antes que a interface comece IGMP, o protocolo multicast deve ser habilitado.*

22.2. Configuração do ERRP

Habilitar/desabilitar o ERRP

Por padrão, o ERRP está desativado e precisa ser configurado no modo *Global*.

» Habilitar/desabilitar o ERRP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/Desabilitar o ERRP	**[no] errrp**	Obrigatório

Configuração de domínio

Ao criar um domínio errp, o usuário precisa especificar o ID do domínio e deve configurar o mesmo ID em todos os nós dele. Crie até 16 domínios em um dispositivo.

» Configuração de domínio:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Criar e acessar o modo de configuração de domínio	**errp domain** domain-id	Obrigatório
Sair do modo de domínio	**exit**	Opcional
Remover o domínio	**no errp domain** domain-id	Opcional
Visualização da informação do domínio	**show errp domain** domain-id	Opcional

Configuração da VLAN de controle

A VLAN de controle é usada para transmitir mensagem de protocolo ERRP.

Cada domínio ERRP existem as: VLAN de controle primário e VLAN de controle secundário. As mensagens de protocolo do anel primário são propagadas na primeira, e as mensagens de protocolo do sub-anel são propagadas na segunda. O usuário precisa especificar apenas a VLAN de controle primário e o ID um acima será a outra.

Quando uma porta ERRP envia pacotes de protocolo, sempre toma as tags VLAN de controle, independentemente da porta ERRP estar no modo *Trunk*.

» Configuração da VLAN de controle:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da VLAN de controle	**[no] control-vlan** vlan-id	Obrigatório
Visulização da VLAN de controle	**show errp control-vlan**	Opcional

Configuração do anel

Para evitar conflitos entre ERRP e STP no cálculo do status de bloqueio / liberação de portas, eles são mutuamente exclusivos na porta. Antes de especificar uma porta ERRP, você deve desativar o STP na porta.

Se um dispositivo estiver em vários anéis ERRP do mesmo domínio, apenas um grande anel pode existir. A função de nó do dispositivo em outros sub-anéis pode ser apenas o nó de borda ou nó de borda assistente.

O campo ERRP só produz efeitos quando o protocolo e o anel estiverem ativados. Para isso, o usuário deve primeiro configurar a VLAN de controle.

O anel ERRP é dividido em anel principal e sub-anel. Respectivamente use 0,1.

» Configuração do loop:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de domínio	**errp domain** domain-num	-
Configuração do anel e d nível do anel	**ring** ring-id **role [master | transit] primary-port [ethernet port | channel-group** lacp-id **] secondary-port [ethernet port | channel-group** lacp-id **] level** level-number	Obrigatório
Habilitar o anel	**ring** ring-id **enable**	Obrigatório
Desabilitar o anel	**ring** ring-id **disable**	Opcional
Remover o anel	**no ring** ring-id	Opcional
Visualização das informações de anel	**show errp domain** domain-id **ring** ring-id	Opcional

Configuração do papel do nó

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de domínio	**errp domain** domain-num	-
Configuração do papel do nó	**ring** *ring-id* **role { master | transit } primary-port [ethernet** port-id **| channel-group** lacp-id **] secondary-port [ethernet** port-id **| channel-group** lacp-id **] level level-number**	Obrigatório
	ring ring-id **role {** edge **|** assistant-edge **common-port [ethernet** port-id **| channel-group** lacp-id **] edge-port [ethernet** port-id **| channel-group** lacp-id **]**	

Configuração do modo de trabalho

Para se conectar com o dispositivo de outros fornecedores, o usuário pode modificar o modo de trabalho no domínio ERRP e configurar vários domínios no mesmo dispositivo. Cada um pode ser configurado com diferentes modos de trabalho. Todos os nós no mesmo domínio ERRP devem funcionar no mesmo modo.

» Configuração do modo de trabalho:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de domínio	**errp domain** domain-num	-
Configuração do modo *Padrão*	**work-mode standard**	Opcional
Executar o modo de compatibilidade EIPS	**work-mode eips-subring**	Opcional
Executar o modo de compatibilidade RRPP	**work-mode huawei**	Opcional

Configuração de solicitação de consulta

Esta função é usada para cooperar com IGMP-Snooping. Quando a topologia da rede de endereços ERRP muda, ele imediatamente notifica o querier IGMP para reenviar a consulta geral de atualização do banco de dados a tempo. Atualmente, não existe um padrão relacionado. A mensagem de solicitação de consulta é privada e o tipo IGMP é 0xff.

A implementação é a seguinte:

1. A função de solicitação de consulta padrão é habilitada no nó mestre. O nó de trânsito a desativa;
2. A alteração da topologia do nó mestre é determinada por: o status do nó mestre é de *Health* para *Fault* ou vice-versa;
3. As alterações de topologia de outros nós são determinadas por: o status da porta primária e secundária é de encaminhamento para não-encaminhamento ou vice-versa;
4. Quando o nó detecta uma alteração de topologia: se ele em si é o querier IGMP, envia imediatamente uma mensagem de Consulta Geral para todas as portas. Caso contrário, é enviado imediatamente uma mensagem Query Solicit para todas as portas;
5. Depois que o querier IGMP receber a mensagem Query Solicit: ele responde imediatamente com uma consulta geral.

» Configuração do Query Solicit:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de domínio	**errp domain** domain-id	-
Configuração da função de consulta	**[no] ring ring-id query-solicit**	Opcional

Configuração dos parâmetros de tempo

Você pode modificar os parâmetros do timer ERRP como requisito, mas certifique-se de sejam os mesmos em todos os nós. É importante que o valor do timer de *Failed* não seja inferior a 3 vezes o valor do timer do Hello.

» Configuração dos parâmetros de tempo:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do contador de tempo da mensagem de *health*	**errp hello-timer** value	Opcional
Configuração das informações do contador de tempo de *timeout*	**errp fail-timer** value	Opcional
Configuração do contador de tempo do atraso de restauração	**errp preup-timer** value	Opcional

Configuração da função de descoberta de topologia

Configuração da função de descoberta de topologia

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de domínio	**errp domain** domain-id	-
Habilitar a descoberta de topologia	**[no]topo-collect**	Obrigatório
Visualização da informação da topologia	**show errp topology [domain** domain-id **| summary]**	Opcional

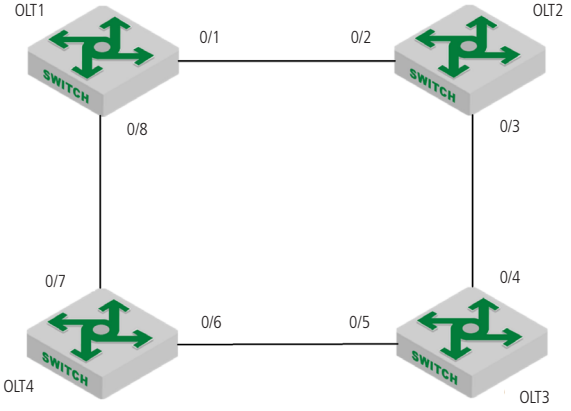
Limpar as estatísticas de mensagem de protocolo

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Limpar as estatísticas	**Clear errp [**domai-id **[ring** ring-id**]]**	Opcional

22.3. Exemplo de configuração de ERRP

» Requisitos de rede:

Como exibido na figura a seguir, os quatro OLTs formam um single-anel e estão com o ERRP ativo.



» Procedimento de configuração:

» A configuração do ERRP no OLT1 é conforme:

OLT1(config)# interface range ethernet 0/1 ethernet 0/8

OLT1(config-if-range)#no spanning-tree

OLT1(config-if-range)#exit

OLT1(config)#errp domain 0

OLT1(config-errp-domain-0)#ring 0 role master primary-port ethernet 0/1 secondary-port ethernet 0/8 level 0

OLT1(config-errp-domain-0)#control-vlan 100

OLT1(config-errp-domain-0)#ring 0 enable

OLT1(config-errp-domain-0)#exit

OLT1(config)#errp

» A configuração do ERRP no OLT2 é conforme:

OLT2(config)# interface range ethernet 0/2 ethernet 0/3

OLT2(config-if-range)#no spanning-tree

OLT2(config-if-range)#exit

OLT2(config)#errp domain 0

OLT2(config-errp-domain-0)#ring 0 role transit primary-port ethernet 0/2 secondary-port ethernet 0/3 level 0

OLT2(config-errp-domain-0)#control-vlan 100

OLT2(config-errp-domain-0)#ring 0 enable

OLT2(config-errp-domain-0)#exit

OLT2(config)#errp

» A configuração do ERRP no OLT3 é conforme:

OLT3(config)# interface range ethernet 0/4 ethernet 0/5

OLT3(config-if-range)#no spanning-tree

OLT3(config-if-range)#exit

OLT3(config)#errp domain 0

OLT3(config-errp-domain-0)#ring 0 role transit primary-port ethernet 0/4 secondary-port ethernet 0/5 level 0

OLT3(config-errp-domain-0)#control-vlan 100

OLT3(config-errp-domain-0)#ring 0 enable

OLT3(config-errp-domain-0)#exit

OLT3(config)#errp

» A configuração do ERRP no OLT4 é conforme:

OLT4(config)# interface range ethernet 0/6 ethernet 0/7

OLT4(config-if-range)#no spanning-tree

OLT4(config-if-range)#exit

OLT4(config)#errp domain 0

OLT4(config-errp-domain-0)#ring 0 role transit primary-port ethernet 0/6 secondary-port ethernet 0/7 level 0

OLT4(config-errp-domain-0)#control-vlan 100

OLT4(config-errp-domain-0)#ring 0 enable

OLT4(config-errp-domain-0)#exit

OLT4(config)#errp

» Validação dos resultados:

» Exiba a configuração da VLAN de controle:

OLT1(config)#show errp control-vlan

VLAN name : ERRP domain 0 primary-control-vlan

VLAN ID : 100

VLAN status : ERRP used only

VLAN member : e0/1,e0/8.

Static tagged ports : e0/1,e0/8.

Static untagged ports :

VLAN name : ERRP domain 0 sub-control-vlan

VLAN ID : 101

VLAN status : ERRP used only

VLAN member : e0/1,e0/8.

Static tagged ports : e0/1,e0/8.

Static untagged ports :

Total entries: 2 vlan.

» Exiba o status do loop ERRP:

OLT1(config)#show errp domain 0

ERRP state: enable

Time value: hlth 1, hlthFl 6, mjrFlt 5, preFwd 6, preup 0

domain 0 info: control-vlan 100, work-mode standard, topo-collect disable

ring 0 info:

status: active

role : master

level : 0

stm : COMPLETE

query solicit: enable

primary/common port: e0/1 forwarding

rcv-pkts: 0hlth,0comn,0cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt

snd-pkts: 6hlth,0comn,1cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt
secondary/edge port: e0/8 blocking
rcv-pkts: 6hlth,0comn,1cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt
snd-pkts: 0hlth,0comn,0cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt
Total 1 ring(s).

» O status de falha de loop deve ser:
OLT1(config)#show errp domain 0
ERRP state: enable
Time value: hlth 1, hlthFl 6, mjrFlt 5, preFwd 6, preup 0
domain 0 info: control-vlan 100, work-mode standard, topo-collect disable
ring 0 info:
status: active
role : master
level : 0
stm : FAULT
query solicit: enable
primary/common port: e0/1 forwarding
rcv-pkts: 0hlth,0comn,0cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt
snd-pkts: 99hlth,1comn,1cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt
secondary/edge port: e0/8 forwarding
rcv-pkts: 95hlth,0comn,1cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt
snd-pkts: 0hlth,0comn,0cmplt,0lnkdn,0lnkUp,0edgHlo,0mjrFlt

23. Configuração do ERPS

23.1. ERPS

Visão geral de ERPS

ERPS (*Ethernet Ring Protection Switching*) foi lançado pela ITU-T com a taxa de convergência do nível de telecomunicações. Se todos os dispositivos dentro do anel suportam este protocolo, eles podem comunicar-se entre si.

Conceito básico de ERPS

O ERPS inclui: o anel ERPS, o nó, a função de porta e o status da porta.

» Exemplo de ERPS.

A instância EPRS é formada pelo mesmo ID de instância, VLAN de controle e OLTs interligados.

» VLAN de controle.

A VLAN de controle transmite o protocolo ERPS, e seus pacotes carregarão a tag correspondente.

» RPL.

RPL (*Ring Protection Link*), Link designado pelo mecanismo que fica bloqueado enquanto estiver ocioso para evitar loop.

» Anel ERPS.

O anel é a unidade básica EPRS. Ele é composto por um conjunto de equipamentos interligado na mesma VLAN de controle.

» Nó.

O OLT adicionado no anel ERPS é chamado de nó. Cada nó não pode ser adicionado a mais de duas portas no mesmo anel ERPS. Eles são divididos em Proprietário RPL, vizinho, próximo vizinho e comum.

» Papel da porta.

No ERPS, as funções de porta incluem: proprietário RPL, vizinho, próximo vizinho e comum:

» **Proprietário RPL**: um anel ERPS possui apenas uma porta deste tipo configurada pelo usuário que evita loops no anel ERPS sendo bloqueada. O nó que possui a porta torna-se o nó *Proprietário RPL*.

» **Vizinho RPL:** um anel ERPS possui apenas uma porta deste tipo configurada pelo usuário e deve estar conectada à porta do *Proprietário RPL*. Se a rede estiver normal, esta porta também será bloqueada para evitar laços no anel ERPS. O nó que possui esta porta torna-se o nó *vizinho RPL*.

» **Próximo vizinho RPL:** um anel ERPS pode ter até duas portas deste tipo configuradas pelo usuário. Ela deve ser a porta que conecta o nó *Proprietário RPL* ou o nó Vizinho RPL. Para se tornar o nó do *Próximo vizinho RPL*, o OLT deve possuir estas portas.

Obs.: *os nós do* Próximo vizinho RPL *não são muito diferentes dos nós comuns. Eles podem ser substituídos por nós comuns.*

- » **Comum:** as portas que não pertencem a nenhuma das classificações citadas anteriormente são portas comuns. Se o nó tiver apenas portas comum, esse nó se tornará o nó comum.

» Status da porta.

No anel ERPS, o status da porta do protocolo ERPS é dividido em três tipos.

- » **Encaminhamento:** a porta encaminha o tráfego do usuário e recebe/encaminha os pacotes R-APS.
- » **Descarte:** no status de descarte, a porta só pode receber / encaminhar pacotes R-APS e não sim pode encaminhar pacotes R-APS de outros nós.
- » **Desativar:** porta no status Linkdown.

» **Modo de trabalho:** modo de operação ERPS.

O modo de trabalho inclui: reversível e não reversível.

- » **Reversível:** quando o link falhar, o link RPL está no estado de proteção de liberação e é protegido novamente depois que o link defeituoso for restaurado para evitar loops.
- » **Não reversível:** após a rectificação da falha, o nó defeituoso permanece com defeito (sem entrar no encaminhamento) e o link RPL permanece no estado de proteção de liberação.

Mecanismo de proteção do anel ERPS

ERPS usa ETH CFM para monitoramento de links. Quando a rede está normal, um link de bloqueio é configurado na rede de anel, evitando um loop. Se ocorrer uma falha, um deles é aberto para garantir uma ligação interrupta entre nós. O processo geral é o seguinte:

Conforme exibido na figura a seguir, quando seis dispositivos estão conectados em um anel e o link está no estado IDLE, o loop é removido através da configuração do link RPL e do bloqueio da porta (porta *Proprietário RPL*).

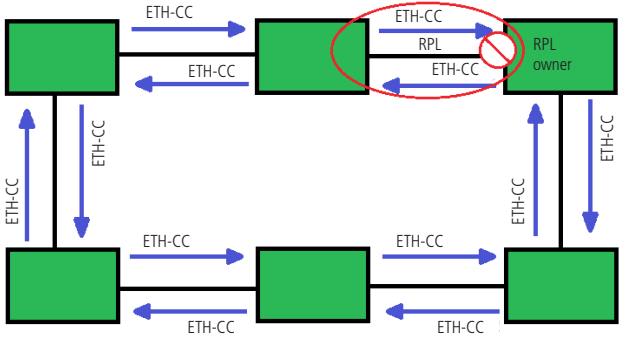


Diagrama de loop em estado ocioso

Quando um nó detecta uma falha, ele imediatamente bloqueia o nó defeituoso e relata a mensagem de falha (R-APS (SF)) para todos os outros dispositivos no anel.

Depois de receber a mensagem, todos os outros nós atualizam o FDB.

A porta do proprietário RPL recebe a mensagem de falha e a porta de recuperação entra no estado de encaminhamento.

O anel ERPS entra no estado de proteção. Conforme exibido na figura a seguir:

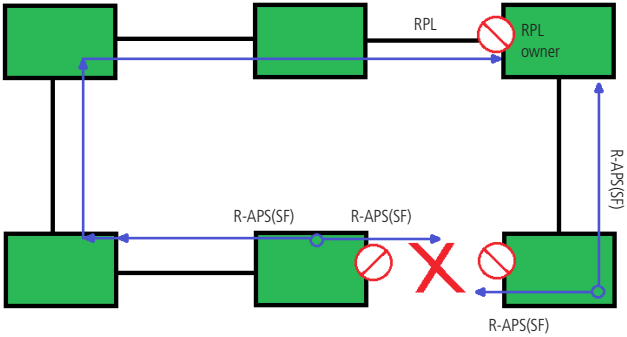


Diagrama de loop na falha de proteção de rede de anel (falha de link)

Conforme exibido na figura a seguir, quando o link se recupera, ele envia pacotes RAPS (NR) para outros dispositivos para informá-los. Quando o proprietário do RPL receber o pacote, bloqueará a porta e enviará a mensagem R-APS (NR, RB) novamente, após algum tempo. Depois de receber o pacote, os outros nós irão atualizar a entrada FDB e mais tarde, a porta do nó defeituoso será restaurada para o estado de encaminhamento.

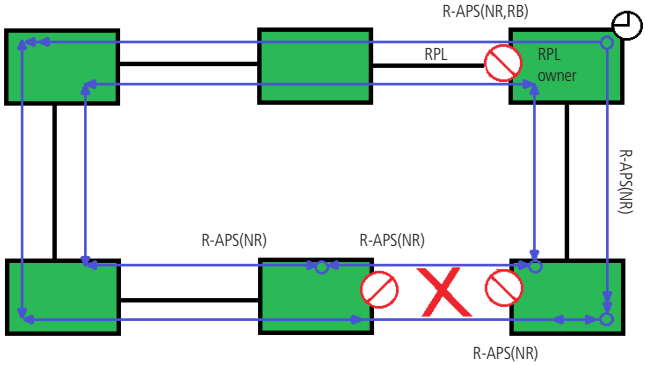


Diagrama de loop em estado de proteção de loop (recuperação de link)

23.2. Configuração do ERPS

Habilitar o ERPS1

» Habilitar o ERPS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o ERPS	**erps**	Obrigatório
Desabilitar ERPS	**no erps**	Opcional

Exemplo de configuração de ERPS

» Exemplo de configuração de ERPS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da instância ERPS	**erps instance** instance-id	Obrigatório
Configuração da VLAN de controle	**control-vlan** vlan id	Obrigatório
Configuração do modo de trabalho	**work-mode {**revertive**|**non revertive**}**	Opcional
Configuração do id do anel	**ring** ring id	Opcional
Configuração do nível do anel	**ring** level	Opcional, 0 refere-se a o anel principal, 1 refere-se a sub-anel
Configuração de porta do anel	**{Port0|port1} ethernet** interface-num {neighbour !next-neighbour |owner }	Obrigatório
Habilitar o anel	**ring enable/disable**	Obrigatório, antes de habilitar o anel, você deve configurar a porta e a VLAN de controle

Obs.: *sobre o ID do Anel: o último byte do DMAC na mensagem R-APS é o ID do Anel. Baseado no G.8032 ele pode ser o mesmo e a VLAN de controle precisa ser diferente. Seu valor em cada instância pode ser de 1 a 229.*

Para configurar a porta ERPS, você deve desativar o spanning tree.

Configuração da detecção de conectividade do link ERRP

No ERPS, não há mensagem HELLO para monitorar a conectividade do link em tempo real. Em vez disso, ele usa a função *CC* no ETH CFM para detectar a conectividade do link, enviando mensagens ETH-CC entre as duas portas. Portanto, você precisa configurá-lo para as portas no ERPS. Na instância ERRP, você precisa configurar o MEL (nível MEG, que deve ser consistente com a configuração CFM).

Para obter mais informações sobre o CFM, consulte o Manual do Usuário do CFM.

» Configurar a detecção de conectividade do link ERRP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da instância ERPS e acesse o modo de configuração de instância	**erps instance** instance-id	Opcional
Configuração do MEL	**mel** level	Opcional

Obs.: *função* CFM ETH-CC *serve para detectar falha de link, não LINK DOWN, como single-pass. Se você não usar a função* CFM ETH-CC*, o ERPS também pode funcionar normalmente entretanto não pode detectar a falha de single-pass.*

Configuração dos controles de tempo do ERPS

O ERPS tem dois timers: timer WTR e timer de proteção.

» **Timer WTR:** quando a porta proprietária RPL é restaurada para o estado de encaminhamento devido a uma falha, se ela for restaurada algumas portas podem não ter sido atualizadas a tempo, então inicia-se o timer WTR quando a porta recebe o pacote RAPS sem falhas para evitar o choque do ponto de bloqueio; se a falha for recebida antes do término, o timer é desativado. Se um pacote RAPS defeituoso de outra porta for recebido antes do término, o timer será desabilitado. Se não receber nenhum pacote RAPS defeituoso de outras portas, ele bloqueará a porta do Proprietário RPL e os enviará após o tempo limite. Depois de receber o pacote, as outras portas definem seus estados como encaminhamento.

» **Timer de Guard:** após a recuperação de falha, o equipamento envolvido na falha de ligação ou na falha do nó enviará o pacote R-APS aos outros dispositivos e ele iniciará o timer de Guard. O dispositivo não os processa até que o timer expire com o objetivo de evitar a recepção de pacotes desatualizados. Se o dispositivo receber depois que o timer expirar, o estado da porta mudará para encaminhamento.

» Configurar timeres do ERPS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da instância ERPS e acesse o modo de configuração de instância	**erps instance** instance-id	Obrigatório
Configuração do timer wtr-timer	**wtr-timer** timer value	Opcional, por padrão é de *5min*, varia entre 1 e 12min
Configuração do timer guard-timer	**guard-timer** timer value	Opcional

Visualização e manutenção do ERPS

Depois de completar as configurações acima, você pode usar os seguintes comandos para visualizar as configurações.

» Visualização e manutenção do ERPS:

Operação	Comando	Obrigatório/ opcional
Visualização das informações de ERPS	**show erps** [instance instance id]	Opcional
Visualização dos pacotes enviados e recebidos	**show erps** [instance instance id] **statistics**	Opcional
Limpar pacotes enviados e recebidos	**show erps** [instance instance id] **statistics**	Opcional

23.3. Exemplo de configuração

Demanda e ligações da rede

Os dois OLTs formam um único anel. O ETH CFM detecta a falha do link e elimina o loop através do ERPS. O diagrama de rede é o seguinte:

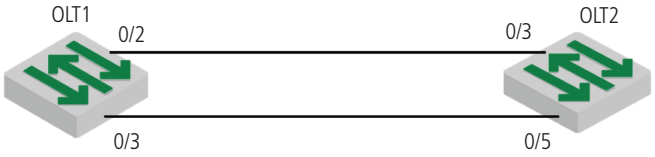


Diagrama de rede da configuração do ERPS

Configuração na proteção de rede de anel ERPS

» Configurar ETH CFM no OLT1 e OLT2:

» Configuração de CFM do OLT1:

```
OLT1(config)#s run cfm
![CFM]
cfm md 1
cfm md format string name test Erps level 1
cfm ma 1
cfm ma format string name test Erps primary-vlan 100
cfm mep 1 direction down interface ethernet 0/3
cfm mep 1 state enable
cfm mep 1 cc enable
cfm rmep 2 mep 1
exit
exit
```

» Configuração de CFM do OLT2:

```
OLT2(config)#s run cfm
![CFM]
cfm md 1
cfm md format string name test Erps level 1
```

cfm ma 1

cfm ma format string name test Erps primary-vlan 100

cfm mep 2 direction down interface ethernet 0/5

cfm mep 2 state enable

cfm mep 2 cc enable

cfm rmep 1 mep 2

exit

exit

» Configurar ERPS no OLT1 e OLT2:

» Configuração de ERPS do OLT1:

OLT1(config)#s running-config erps

![ERPS]

erps

erps instance 1

mel 1

ring level 1

control-vlan 100

port0 ethernet 0/2 owner

port1 ethernet 0/3

ring enable

exit

» Configuração de ERPS do OLT2:

OLT2 (config)#s run erps

![ERPS]

erps

erps instance 1

mel 1

ring 1

ring level 1

control-vlan 100

port0 ethernet 0/3 neighbour

port1 ethernet 0/5

ring enable

exit

Obs.: » *CFM MD formato teste nome da string teste ERPS nível 1.*

» *Aqui, o* nível *refere-se ao nível MEG, ou seja, o MEL no ERPS precisa ser configurado no mesmo.*

» *CFM MA teste de nome de string teste ERPS VLAN-primária 100.*

» *Aqui a VLAN-primária 100 precisa ser a mesma que a VLAN de controle ERPS.*

» *Mep e rmep precisam de correspondência um-para-um.*

Validação de resultados

A porta 0/2 do OLT1 e a porta 0/3 do OLT2 são bloqueadas e o loop é removido.

OLT1 (config)#show erps

ERPS state: enable

Instance Id : 0

Mel : 1

Work-mode : revertive

Time value : WTR 5 min, guard timer 500 ms, holdoff timer 0 s

Ring 1 info:

Control vlan: 100

Status : enable

Node Role : owner

Level : 1

Stm : Idle

portId role state nodeId BPR

port0 e0/2 owner Blocking 00:01:7f:00:00:11 0

port1 e0/3 Common Forwarding 10:7b:ef:fd:4b:cd 0

24. Configuração de rota estática

24.1. Visão geral de rota estática

O OLT possui tabela de roteamento para a camada 3, permitindo apenas entradas estáticas.

24.2. Configuração detalhada da tabela de roteamento estático

Adicionar/remover a tabela de roteamento estático

» Configurações básicas de roteamento estático:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**ip route** dst-ip mask gate-ip	-
Remover uma tabela de roteamento estático específico	**no ip route** dst-ipmask [gate-ip]	-
Remover todas as tabelas de roteamento estático	**no ip route static all**	-

Obs.: » ***GATE-IP:*** *o endereço do próximo salto do roteamento estático. Além disso, é um formato de notação ponto-decimal.*

» ***Dst-ip:*** *o endereço de destino do roteamento estático que você vai adicionar. Além disso, é um formato de notação ponto-decimal.*

» ***Máscara:*** *a máscara do endereço de destino. Além disso, é um formato de notação ponto-decimal.*

Visualização das informações da tabela de roteamento

Este comando é usado para exibir as informações relacionadas da tabela de roteamento especificada, incluindo o endereço do próximo salto, o tipo de roteamento e assim por diante.

» Visualização das informações da tabela de roteamento:

Operação	Comando	Obrigatório/ opcional
Visualização da tabela de roteamento	**show ip route** [ip-address [mask] | ecmp | static]	Opcional
Visualização da tabela de roteamento ECMP	**show ip route ecmp**[ip-address [mask] | static]	Opcional

Obs.: » ***ip-address:*** *o endereço de destino. Além disso, é um formato de notação ponto-decimal.*

» ***mask:*** *segmento de rede de destino apresentado com o endereço IP. Além disso, é um formato de notação ponto-decimal.*

» ***static:*** *exibe todas as tabelas de roteamento estático.*

24.3. Exemplo de configuração

» Adicione um roteamento de rede para 192.168.0.100, configure 10.11.0.254 como o próximo salto.
OLT4840E(config)#ip route 192.168.0.100 255.255.0.0 10.11.0.254

» Exclua um roteamento de rede para 192.168.0.100.
OLT4840E(config)#no ip route 192.168.0.100 255.255.0.0

» Exclua todo o roteamento estático.
OLT4840E(config)#no ip route static all

» Exiba as informações de roteamento ECMP de 192.168.0.100.
OLT4840E(config)#show ip route ecmp 192.168.0.100

» Exiba todas as informações de roteamento ECMP.
OLT4840E(config)#show ip route ecmp

» Exiba as informações de roteamento de 192.168.0.100.
OLT4840E(config)#show ip route 192.168.0.100

» Exiba todas as informações de roteamento.
OLT4840E(config)#show ip route

25. Configuração 802.1 X

25.1. Visão geral de 802.1 x

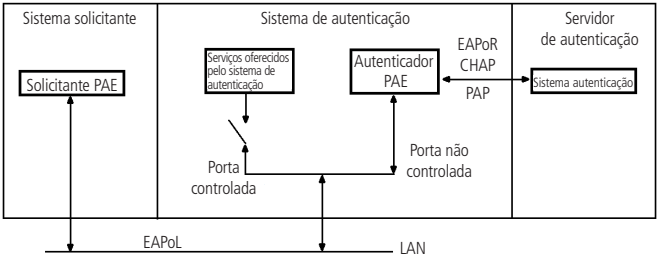
O IEEE 802.1X é o de protocolo de gerenciamento de acesso aprovado em junho de 2001. Uma rede LAN tradicional não fornece acesso à autenticação, é possível acessar os todos dispositivos e recursos apenas ao conectar-se à LAN, gerando uma lacuna de segurança. Para aplicação como de um escritório móvel e CPN, o provedor de dispositivos precisa controlar e configurar a conexão do usuário.

O IEEE 802.1X é uma tecnologia de controle de acesso à rede baseada na autenticação e controle de acesso de dispositivos por nível de conexão física de dispositivos LAN, ou seja, a interface dos dispositivos LAN OLT. Durante uma autenticação, o OLT é o intermediário entre cliente e o servidor. Este protocolo obtém a identidade do usuário do cliente e verifica a sua informação através do servidor de autenticação. Se as informações deste usuário forem válidas, este usuário tem permissão para acessar os recursos da LAN ou, se não, ele será recusado.

Autenticação 802.1x

O 802.1X opera no modelo de cliente / servidor típico e define três entidades: sistema solicitante, sistema de autenticação e sistema de servidor de autenticação:

- **Sistema solicitante:** precisa acessar a LAN e utilizar os serviços fornecidos pelo equipamento OLT (como o PC), o cliente deve suportar o acordo EAPOL e executar o software do cliente de autenticação IEEE 802.1X.
- **Sistema de autenticação:** no sistema Ethernet, o OLT de autenticação é usado principalmente para carregar e fornecer informações de usuários, controlando se a porta está disponível de acordo com o resultado da autenticação. Como se atuasse como proxy entre o cliente e o servidor.
- **Servidor de autenticação:** normalmente se refere ao servidor RADIUS. Este verifica a identidade do cliente (nome do usuário e senha) para determinar se ele tem permissão para acessar a rede. Após o final da autenticação, os resultados serão enviados para o OLT.



A Figura 1-1 mostra a relação entre as três partes

Os sistemas acima envolvem três conceitos básicos: PAE, porta controlada, direção de controle:

» PAE.

A entidade de acesso a porta (PAE) refere-se à entidade que executa o algoritmo 802.1x e operações de protocolo.

» PAE é responsável pela realização de algoritmos e operações do protocolo no mecanismo de autenticação. Ele usa o servidor para autenticar os clientes que precisam acessar a LAN e controla o status autorizado / não autorizado das portas de acordo com o seu resultado. O cliente PAE responde à solicitação de autenticação do dispositivo e envia as informações para o dispositivo. Ele também pode enviar o pedido de autenticação e a solicitação off-line para o dispositivo.

» Porta controlada e porta não controlada.

Um autenticador fornece portas para que os solicitantes acessem a LAN. Cada uma pode ser considerada como duas portas lógicas: uma porta controlada e uma porta não controlada.

» A porta não controlada sempre está habilitada tanto nas direções de entrada como de saída para permitir que os quadros de protocolo EAPOL passem, garantindo que o solicitante sempre possa enviar e receber quadros de autenticação.

» A porta controlada é habilitada para permitir o tráfego normal somente quando está no estado autorizado.

» A porta controlada e a porta não controlada são duas partes da mesma porta. Quaisquer quadros que chegam a elas são visíveis para ambos.

» Direção de controle.

No estado não autorizado, a porta é configurada para controle unidirecional: a implementação de controle unidirecional proíbe o envio de informações ao cliente, mas permite recebê-las.

» Modo de porta controlada.

» Autenticação baseada em porta:

Enquanto a primeira autenticação do usuário for bem-sucedida, outros usuários sem autenticação conectados a mesma porta também podem usar a rede, quando o usuário autenticado ficar offline, outros usuários não poderão mais acessar a rede.

» Autenticação baseada em endereço MAC:

Todos os usuários na porta física precisam ser autenticados separadamente.

Processo de autenticação do 802.1x

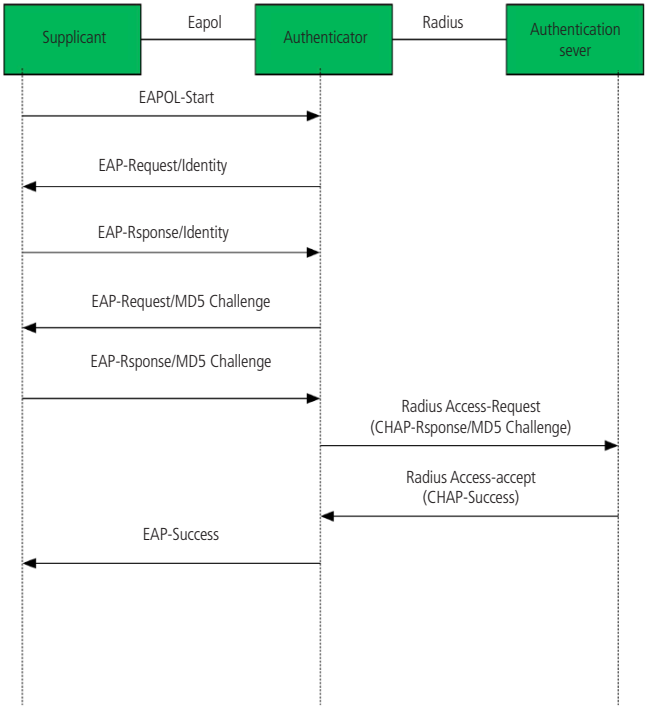
O sistema de autenticação 802.1x emprega o protocolo de autenticação extensível (EAP) para trocar informações entre o EAP do solicitante, o autenticador EAP e o servidor de autenticação.

No momento, o modo *EAP* suporta quatro métodos: *EAP-MD5*, *EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security)* e *PEAP (Protected Extensible Authentication Protocol).*

O OLT suporta o modo *EAP-Transfer* e o modo *EAP-Finish* para interagir com o servidor RADIUS para finalizar a autenticação.

» EAP-Transfer.

A seguir, é exibido um processo necessário para o exemplo de autenticação EAP-Transfer (solicitante; EAPO; Autenticador; RADIUS; Servidor de autenticação).



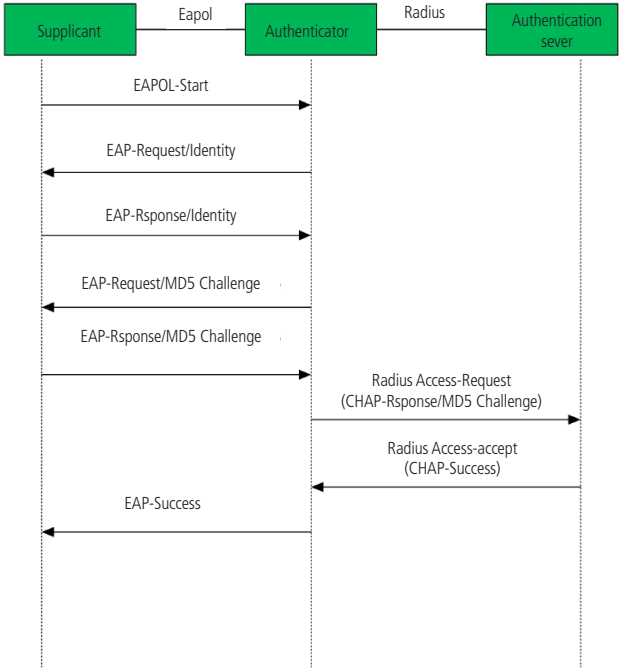
Processo de autenticação EAP-Transfer

O processo de autenticação é o seguinte:

1. Quando o usuário precisa acessar a rede, ele informa seu nome de usuário e a senha registrados pelo cliente 802.1X e inicia a solicitação de conexão (pacote EAPOL-Start). Neste ponto, o cliente envia a mensagem de solicitação ao dispositivo e inicia um processo de autenticação;
2. Depois de receber o quadro de dados solicitado, o dispositivo de acesso envia uma solicitação (EAP-Request / Identity packet) do nome do usuário;
3. O cliente responde enviando suas informações através do quadro de dados (pacote EAP-Response / Identity). O dispositivo encapsula o pacote RADIUS Access-Request e o envia para a autenticação ao servidor para processamento;
4. Depois de receber as informações, o servidor RADIUS compara o nome e a senha do usuário com sua tabela, encontra os dados correspondentes e os criptografa com uma chave gerada aleatoriamente. Então envia a senha criptografada para o dispositivo através de um pacote RADIUS Access-Challenge. A mensagem é encaminhada pelo dispositivo para o cliente;
5. Depois de receber o pacote EAP-Request / MD5 Challenge, o cliente criptografa a parte recebida (geralmente irreversível) e gera os pacotes EAP-Response / MD5 Challenge e passa os pacotes de autenticação para o servidor;
6. O servidor RADIUS compara as informações criptografadas recebidas (pacote RADIUS Access-Request) com as informações de senha criptografada local. Se forem a mesma, o servidor RADIUS considera que o usuário é um usuário válido e envia a mensagem -Accept e EAP-Success);
7. Depois de receber a mensagem de autenticação, o dispositivo altera a porta para o estado autorizado, permitindo ao usuário acessar a rede.

» EAP-Finsh.

Desta forma, os pacotes EAP são encerrados no terminal do dispositivo e são mapeados para pacotes RADIUS. O servidor RADIUS usa o protocolo padrão para completar autenticação, autorização e contabilidade. Podem ser adotados os métodos de autenticação PAP ou CHAP. Utilizamos o método de autenticação CHAP como um exemplo para descrever o fluxo de serviço básico, conforme exibido a seguir (solicitante; EAPO; Autenticador; Radius; Servidor de autenticação).



Processo de autenticação EAP-Finish

O modo de término EAP difere do processo de autenticação do modo de retransmissão EAP, na medida em que o dispositivo criptografa a informação de senha do usuário e o dispositivo criptografa o nome do usuário, a chave de criptografia aleatória e as informações da senha criptografada do cliente para o servidor RADIUS executam o processo de autenticação relacionado.

25.2. Configuração do 802.1x

Configuração do EAP

O padrão 802.1x encaminha os pacotes de autenticação (encapsulados com quadros EAP) do usuário para o servidor RADIUS sem nenhum processamento. No entanto, o servidor tradicional não suporta o recurso EAP. Portanto, o sistema realiza a conversão dos pacotes de autenticação enviados pelo usuário, para os quadros de dados encapsulados pelo protocolo RADIUS padrão e em seguida, encaminha os pacotes para o servidor.

» Configuração do EAP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Definir o modo de interação do protocolo entre o sistema e o servidor RADIUS	**dot1x { eap-finish | eap-transfer }**	Opcional, por padrão é *eap-finish*

Habilitar o 802.1x

O 802.1x fornece um esquema de autenticação de identidade do usuário. No entanto, 802.1x não pode implementar o esquema de autenticação sozinho. O RADIUS ou a autenticação local deve ser configurada para funcionar com 802.1x.

Depois de habilitar o 802.1X, os usuários conectados ao sistema podem acessar os recursos da LAN somente após terem passado pela autenticação. Ao ativá-la, você deve indicar se o modo de habilitação é baseado em interface ou endereço MAC.

» **Configuração baseada na autenticação da interface:** se um dos usuários da porta passar a autenticação, outros usuários da mesma porta poderão usar os recursos da rede mesmo sem autenticação; no entanto, se esse usuário terminar a sua sessão os outros usuários perderão seus acessos.

» **Configuração baseada em autenticação de endereço MAC:** cada usuário sob a porta deve executar uma autenticação separada. Somente aqueles que passaram a autenticação poderão usar os recursos da rede.

» Habilitar o 802.1x:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar o 802.1x	**dot1x method { macbased | portbased }** [interface-list]	Obrigatório

Configuração dos parâmetros de 802.1x para uma porta

Depois que a interface ativar o 802.1X, esta porta precisa ser autenticada enquanto a interface uplink e a que se conecta ao servidor não precisam. Para isso você precisa configurar essas portas para serem autorizadas manualmente ou desativar suas funções de autenticação.

» Configuração dos parâmetros de 802.1x para uma porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração dos parâmetros de 802.1x para uma porta	**dot1x method { auto | forceauthorized | forceunauthorized }** **[** interface-list **]**	Opcional

Configuração de re-autenticação

No modo *EAP-FINISH*, a porta suporta re-autenticação. Depois que o usuário é autenticado, a porta pode ser configurada para re-certificação imediata ou re-autenticação periódica.

» Configuração de re-autenticação:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Re-certificação imediata	**dot1x re-authenticate [** interface-list **]**	Opcional
Re-autenticação periódica habilitada em uma porta	**dot1x re-authentication [** interface-list **]**	Opcional
Configuração do tempo de re-autenticação periódica	**dot1x re-authperiod** time **[** interface-list **]**	Opcional

Configuração da função *Watch*

Depois de habilitar esta função, uma porta envia uma mensagem de clock periodicamente quando nenhum usuário está presente, fazendo com que os usuários executem a autenticação 802.1x.

Esta função é usada para oferecer suporte a clientes que não podem enviar pacotes EAPOL-Start, como clientes 802.1X. Nosso dispositivo envia um pacote EAP-Request / Identity para o cliente a cada N segundos para ativar a autenticação.

» Configuração da função *Watch*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar a função *Watch*	**dot1x daemon [** interface-list **]**	Opcional
Configuração do intervalo de visualização dos pacotes	**dot1x daemon time** time **[** interface-list **]**	Opcional, *60s* por padrão
Restaurar o valor padrão do intervalo de verificação de pacotes	**no dot1x daemon** time **[** interface-list **]**	Opcional

Configuração de usuários

Estas funções realizam principalmente as configurações para o número de usuários da porta, exclusão de usuários, operações de detecção de pulsação, etc.

» **Detecção de pulsação:** após esta função estar habilitada, o dispositivo envia periodicamente EAP-Request / Identity para as portas do cliente, o cliente conectado responde com a EAP-Rsponse / Identity. Se os quatro pacotes EAP-Request / Identity consecutivos não receberem uma respossta, o dispositivo considera o usuário offline e em seguida, apagará a sessão e alterará a porta para um estado não autorizado.

» **Função *Quiet*:** após a autenticação do usuário falhar, o dispositivo precisa de um período de tempo de recuperação (pode ser configurado através do *dot1x quiet -period-value*, por padrão, não é necessário). Durante este período, o autenticador não processa pedidos de autenticação.

» Configuração de usuários:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o número máximo de usuários que podem passar pela autenticação	**dot1x max-user [** interface-list **]**	Opcional
Remover o um usuário online específico	**dot1x user cut { username** name **| mac-address** mac **[vlan** vid **] }**	Opcional
Habilitar a deteção de pulsação	**dot1x detect [** interface-list **]**	Opcional, *25s* por padrão
Configuração de intevalo de deteção de pulsação	**dot1x detect interval** time	Opcional
Restaurar o intevalo padrão de deteção de pulsação	**no dot1x detect interval**	Opcional
Configuração da função de quiesce	**dot1x quiet-period-value** time	Opcional, *0* por padrão, quiet desativado
Restaurar o intervalo padrão da função de quiesce	**no dot1x quiet-period-value**	Opcional

Configurar o modo de host com base no modo de autenticação da porta

A configuração do modo de host só produz efeito no método de autenticação baseado em porta; se a porta for configurada para ter uma autenticação baseada em MAC, o modo *Host* automaticamente se tornará inválido. Modos de host:

» **multi-hosts:** quando uma autenticação de usuário é aprovada na porta, outros usuários da porta podem acessar a rede sem autenticação.

» **single-host:** permite que apenas uma autenticação passe e todos os outros usuários não poderão acessar a rede nem passar pela autenticação.

» Configuração do modo de host:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o modo de host com base no modo de autenticação da porta	**dot1x portbased host-mode { multi-hosts | single-host }[** interface-list **]**	Opcional

Configuração da guest VLAN

Depois de habilitar a autenticação 802.1X, os usuários podem acessar apenas os recursos de rede da VLAN se a guest VLAN estiver configurada na porta. Uma vez que a autenticação do usuário for bem-sucedida, a porta troca automaticamente sua VLAN. Depois que o usuário ficar offline, a porta retorna para a guest VLAN.

Para garantir que todas as funções possam ser usadas normalmente, atribua diferentes ID de VLAN para a VLAN de Configuração, a VLAN radius e a guest VLAN.

» Configuração da guest VLAN:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da Guest VLA	**dot1x guest-vlan** vlan-id **[** interface-list **]**	Opcional

Configuração da VLAN ativa padrão

A *default-active-VLAN* é a VLAN ativa padrão. O usuário 802.1X só pode acessar o recurso nela quando passar a autenticação do servidor radius.

» Configuração da VLAN ativa padrão:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração da VLAN ativa padrão	**dot1x default-active-vlan** vlan-id **[** interface-list **]**	Opcional
Remover a VLAN ativa padrão	**no dot1x default-active-vlan interface** {interface_type interface_num | interface_ name }	Opcional

Configuração da VLAN RADIUS

Quando o usuário 802.1X passa a autenticação via servidor RADIUS, ele transmitirá as informações de autenticação para o dispositivo. Se ele ativou a função *Radius* e o servidor está configurado para distribuir VLAN (adotando o atributo Tunnel-P-vt-Group-ID (81)), as informações de autenticação incluirão as VLANs distribuídas como consequência e o dispositivo irá adicionar a interface online de autenticação de usuário à VLAN distribuída por radius.

» Configuração da VLAN RADIUS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Aecsse o modo de configuração AAA	**aaa**	-
Habilitar a função de distribuição da VLAN RADIUS	**radius vlan enable**	Opcional, *desativado* por padrão

Obs.: » *Antes de usar esta função, você deve criar a VLAN correspondente e em seguida adicionar a interface do usuário nela, assim como a Guest VLAN e Default-active-VLAN.*

» *O RADIUS distribui a VLAN, mas não altera a configuração original da interface, assim como a Guest VLAN e Default-active-VLAN.*

» *A VLAN radius, a Guest VLAN e a Default-active-VLAN são efetivas tanto na autenticação baseada em porta quanto na autenticação baseada em MAC.*

Configurar a transmissão EAPOL

Quando uma porta desabilita a autenticação 802.1x, é preciso transmitir a mensagem 802.1x EAPOL do usuário. Assim, o equipamento funcionará como o relé, os usuários podem executar a autenticação 802.1x no equipamento superior. Esta função só pode lidar com o pacote EAPOL encaminhado para a CPU. Para pacotes que não se encaminham para a CPU, os pacotes são processados pelo hardware e não estão sujeitos a esta configuração. Você pode configurar a porta de transmissão transparente EAPOL e a porta de uplink correspondente somente quando a autenticação 802.1x estiver desabilitada. Ou seja, você não pode configurar a função de transmissão transparente quando a autenticação 802.1x está habilitada.

» Configurar a Transmissão EAPOL:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	
Habilitar a função de transmissão de mensagem EAPOL da porta	**dot1x eapol-relay [** interface-list **]**	Opcional
Configurar porta de uplink de transmissão de mensagem EAPOL	**dot1x eapol-relay uplink[** interface-list **]**	Opcional

Configuração do canal de segurança

Quando o usuário não está online, ele realiza o controle de acesso via canal de segurança para que o usuário possa acessar recursos específicos. Esta função deve configurar a ACL em primeiro lugar e depois aplicar a distribuição através do comando do *dot1x security-group*.

» Configuração do canal de segurança:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Ativação do ACL	**dot1x security-group [ip-group** name | num **] [link-group** name | num **] [subitem** num **]**	Opcional
Desativação do ACL	**no dot1x security-group [ip-group** name | num **] [link-group** name | num **] [subitem** num **]**	Opcional

Obs.: *ele deve ser configurado no modo de configuração global. Se você deseja que uma determinada interface entre em vigor, a configuração da ACL deve incluir as informações desta interface. Comparado com a ACL distribuída pelo grupo de acesso, a ACL distribuída pelo canal secreto 802.1X possui maior prioridade.*

ACL emitida

Quando um usuário faz logon no servidor RADIUS, se a ACL de autorização estiver configurada neste servidor (usando o atributo *filter-id (11)* para configurar a ACL emitida), o dispositivo controla o fluxo de dados da porta na qual o usuário está. Antes

de ativar uma ACL, você precisa configurar as regras correspondentes no dispositivo.

Quando o OLT não suporta o número de série distribuída pelo servidor, ele precisa usar a função de prefixo ACL. Depois de configurar um prefixo, o OLT pode converter automaticamente o número de série (adicione o prefixo na frente do número de série) para finalizar a ACL emitida.

» ACL emitida:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do formato de ACL	**dot1x radius-acl-format{** integer | string**}**	*String*, por padrão
Configuração do prefixo do ACL	**dot1x number-acl-prefix [**number-acl-prefix-name**]**	*"assignacl-"*, por padrão
Remover prefixo do ACL	**no dot1x number-acl-prefix**	Opcional

Obs.: *se você quiser usar a função de distribuição da ACL, você deve configurar a ACL relacionada primeiro. Ele precisa usar o atributo Filter-Id (11) do servidor radius.*

Visualização e manutenção do Dot1x

Operação	Comando	Obrigatório/ opcional
Visualização do status da função de autenticação 802.1X	**show dot1x**	Opcional
Visualização da configuração da função de watch da interface de autenticação 802.1x	**show dot1x daemon [interface** interface-num **]**	Opcional
Visualização das configurações das interfaces, como o modo de controle de interface, o estado de re-autenticação, o número máximo de usuários para a autenticação da interface	**show dot1x interface [** interface-num **]**	Opcional

Operação	Comando	Obrigatório/ opcional
Visualização da sessão 802.1x	**show dot1x session [{ interface** interface-num **}	{ mac-address** mac **}]**	Opcional estado "online" do usuário (número da porta, ID da VLAN, endereço MAC, nome de usuário, etc.)
Visualização da ACL emitida	**show dot1x radius-acl**	Opcional
Visualização da configuração de passagem de EAPOL	**show dot1x eapol-relay [interface** interface-num **]**	Opcional
Visualização da configuração da detecção de pulsasão	**show dot1x detect [interface** interface-num **]**	Opcional
Visualização das informações de guest VLAN	**show dot1x guest-vlan [interface** interface-num **]**	Opcional
Visualização do status da autenticação de interface	**show dot1x port-auth**	Opcional
Visualização do período de silêncio	**show dot1x quiet-period-value**	Opcional
Visualização das informações de configuração de canal de segurança	**show dot1x security-group**	Opcional
Depuração do recebimento e envio de pacotes e modulo de processamento do DOT1X	**debug dot1x**	Opcional

25.3. Exemplo de configuração

Requisitos de rede

O nome de usuário de acesso 802.1x local é u1, e a senha é 123. O usuário pode acessar a internet após o login com sucesso. O diagrama de rede é exibido a seguir:

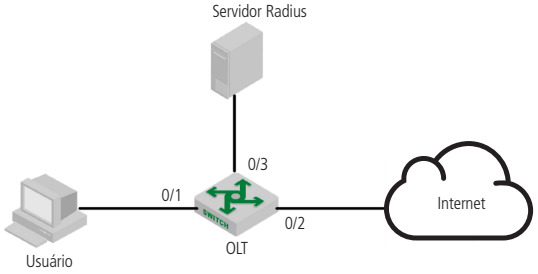


Diagrama de rede da configuração 802.1X

Etapas de configuração

» Ative a autenticação 802.1x da porta 0/1 da OLT:

OLT4840E(config)#dot1x method macbased interface ethernet 0/1

» Configure a função básica do servidor RADIUS (crie o usuário r1 no servidor RADIUS, configure o servidor de autenticação mestre para que seja 1.1.1.1, o servidor primário seja 1.1.1.2, a chave compartilhada de autenticação para ser 123456. Por favor, consulte *26. Configuração RADIUS* para maiores detalhes.)

OLT4840E(config-aaa)#radius host 1

OLT4840E(config-aaa-radius-1)#primary-auth-ip 1.1.1.1 1812

OLT4840E(config-aaa-radius-1)#primary-acct-ip 1.1.1.2 1813

OLT4840E(config-aaa-radius-1)#auth-secret-key 123456

OLT4840E(config-aaa-radius-1)#acct-secret-key 123456

OLT4840E(config-aaa)#domain abc.com

OLT4840E(config-aaa-domain-abc.com)#radius host binding 1

OLT4840E(config-aaa-domain-abc.com)#state active

OLT4840E(config-aaa)#default domain-name enable abc.com

Validação de resultados

O usuário insere o nome de usuário e a senha no cliente 802.1X para executar a autenticação. Através do comando de *show dot1x session*, ele exibe que o usuário atual passou a autenticação e o login com sucesso, ou seja, o usuário pode acessar a internet.

OLT4840E(config)#show dot1x session

port vid mac username login time

0/1 1 c8:3a:35:d3:e3:99 u1@abc.com 2000/01/01 05:13:42

26. Configuração RADIUS

26.1. Visão geral de RADIUS

Visão geral de AAA

AAA significa Authentication, Authorization and Accounting (Autenticação, Autorização e Contabilidade).

Ele é, na verdade um gerenciamento de segurança de rede. Aqui, a segurança da rede refere-se principalmente ao controle de acesso, incluindo os usuários que podem acessar o servidor de rede, quais serviços estão disponíveis para usuários e a utilização dos usuários para cobrança.

Esta função geralmente adota a estrutura cliente / servidor: o cliente é executado no lado do recurso gerenciado e o servidor armazena as informações do usuário centralmente. Portanto, o framework AAA possui uma boa escalabilidade e gerenciamento centralizado das informações do usuário.

Utilização do AAA

O diagrama de AAA é exibido na figura a seguir:

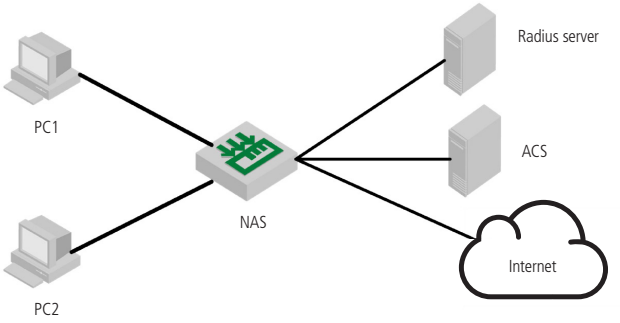


Diagrama de quadro AAA

Existem duas maneiras de perceber AAA:

- Via NAS.
- Via R ADIUS, TACACS +, etc.

Visão geral de RADIUS

O RADIUS cria um banco de dados de usuários exclusivo, armazena o nome e a senha do usuário para autenticar, armazenando o tipo de serviço e informações de configuração correspondentes que são passadas para o usuário para completar a autorização. Após este processo, o servidor RADIUS executa a função de contabilização de contas de usuário.

- RADIUS significa (*Remote Authentication Dial in User Service*) autenticação remota no serviço de usuário.
- RADIUS é um protocolo AAA para aplicações como Acesso à Rede ou Mobilidade IP.
- Funciona em ambas as situações, local e móvel.
- Ele usa protocolos de autenticação de senha (PAP), protocolos de autenticação de desafio Handshake (CHAP) ou protocolo de autenticação extensível (EAP) para autenticar usuários.
- Ele verifica no arquivo de texto, servidores LDAP, banco de dados para autenticação.
- Após a autenticação dos parâmetros de serviços são enviados de volta ao NAS.
- Ele notifica quando uma sessão começa e termina. Estes dados são utilizados para fins de faturamento ou estatística.
- O SNMP é usado para monitoramento remoto.
- Pode ser usado como um proxy.

Aqui está uma lista de todos os recursos principais do RADIUS:

- Modelo Cliente / Servidor.
  - O NAS funciona como um cliente para o servidor RADIUS.
  - O servidor RADIUS é responsável por obter solicitações de conexão do usuário, autenticando-o e retornando todas as informações de configuração necessárias para que o serviço seja entregue.
  - Um servidor RADIUS pode atuar como um cliente proxy para outros servidores RADIUS.
- Segurança de rede.
  - As transações entre um cliente e um servidor são autenticadas através do uso de uma chave compartilhada. Essa chave nunca é enviada pela rede.
  - A senha é criptografada antes ser enviada pela rede.

» Mecanismos de autenticação flexíveis.
  » Protocolo ponto a ponto - PPP.
  » Protocolo de autenticação de senha - PAP.
  » Protocolo de autenticação de desafio Handshake - CHAP.
  » Login UNIX simples.
» Protocolo extensível.
  » O RADIUS é extensível; a maioria dos fornecedores de hardware e software RADIUS implementam seus próprios protocolos.

26.2. Configuração do RADIUS

Configuração do servidor RADIUS

O servidor RADIUS salva a identidade do usuário válido. Após a autenticação, o sistema transfere a identidade do usuário para o servidor RADIUS e transfere a validação para o usuário. O acesso do usuário ao sistema libera os recursos da LAN somente após a autenticação do servidor RADIUS.

» Configuração do servidor RADIUS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo *AAA*	**aaa**	-
Criar e acessar o esquema de configuração RADIUS	**radius host** name	Obrigatório
Configuração de RADIUS primário	**primary-auth-ip** ipaddr port	Obrigatório
Configuração de RADIUS secundário	**secondary-auth-ip** ipaddr port	Opcional
Configuração do servidor de autenticação primária	**primary-acct-ip** ipaddr port	Opcional
Configuração do servidor decundário de autenticação	**primary-acct-ip** ipaddr port	Opcional
Configuração da chave compartilhada do RADIUS primário	**auth-secret-key** keystring	Obrigatório

Operação	Comando	Obrigatório/ opcional
Configuração da chave compartilhada do RADIUS secundário	**acct -secret-key** keystring	Opcional
Configuração do endereço NAS-RADIUS	**nas-ipaddress** ipaddr	Opcional, se não houver configuração, será utilizado o endereço IP do equipamento
Configuração se o nome do usuário deve ser carregado com o nome do domínio quando o sistema passa o pacote para o servidor RADIUS atual	**username-format { with-domain | without-domain }**	Opcional
Configuração da autenticação em tempo real	**realtime-account**	Opcional
Configuração do intervalo de autenticação em tempo real	**realtime-account interval***time*	Opcional

Troca de servidor RADIUS mestre e servidor RADIUS escravo

RADIUS oferece a função de redundância do servidor mestre / escravo, ou seja: o servidor mestre operam sempre que estiver funcionando; se houver algo errado com ele, o servidor escravo será habilitado; assim que o servidor mestre for recuperado, ele reassumirá a tarefa e o servidor escravo será desativado.

Mecanismos de realização:

Na autenticação do RADIUS, se o servidor mestre não puder executar o trabalho normalmente, basta configurá-lo como down, então o servidor escravo começará a funcionar; se o servidor mestre for recuperado, o timer de pré-emissão será ativado (o tempo é configurado como *Preemption-time*). Quando este timer atingir seu tempo limite, o servidor mestre será automaticamente ativado e as operações de autenticação serão realizadas através dele.

» Troca de servidor RADIUS master e servidor RADIUS slave:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo *AAA*	**aaa**	-
Criar e acessar o esquema de configuração RADIUS	**radius host** name	Obrigatório
Configuração do timer de pré-emissão	**preemption-time** preemption-time	Opcional, intervalo de valor de 0-1440, unidade em minutos. Por padrão está definido como *0*

Configuração de usuário local

O cliente precisa configurar o nome do usuário local, a senha, etc.

» Configuração de usuário local:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo *AAA*	**aaa**	-
Configuração de usuário local	**local-user username** name **password** pwd [**vlan** vid]	Opcional

Configuração de domínio

O cliente precisa fornecer nome de usuário e senha durante a autenticação. O nome de usuário geralmente contém informações de domínio e do ISP do usuário correspondente. A informação mais importante do domínio é a autenticação do servidor RADIUS e a contabilização dos usuários nele.

» Configuração de domínio:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo *AAA*	**aaa**	-
Configuração do nome do domínio padrão	**default domain-nameenable** domain-name	Opcional
Desabilitar o nome do domínio padrão	**default domain-name disable**	Opcional
Criar e acessar um cenário de domínio	**domain** name	Obrigatório
Configuração para utilização de um servidor de autenticação radius	**schemeradius**	Opcional
Configuração para utilização de authenticação local	**schemelocal**	Opcional
Configuração para utilização de authenticação local após o radius falhar	**schemeradiusloca**	Opcional
Selecionar o servidor radius para o domínio atual	**radius host binding** radius-name	Opcional
Ativar o limite de número de usuários de autenticação no domínio e defina o limite de número de usuários permitidos	**access-limitenable** number	Opcional
Desativar o limite de número de usuários de autenticação no domínio	**access-limit disable**	Opcional
Ativar o domínio atual	**stateactive**	Obrigatório
Desativar o domínio atual	**state block**	Opcional

Configuração dos atributos RADIUS

Configuração das compatibilidade ou características únicas do RADIUS.

» Configure o recurso RADIUS:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo *AAA*	**aaa**	-
Configuração da função *Accounting-on*	**accounting-on { enable** sen-num **| disable }**	Opcional
Configuração da compatibilidade H3C Cams	**h3c-cams { enable | disable }**	Opcional
Habilitar a funçã de accounting	**radius accounting**	Opcional
Se o pacote de accounting não responder, o usuário é desligado	**radius server-disconnect drop 1x**	Opcional
Configuração de distribuição de prioridade de portas pelo RADIUS	**radius 8021p enable**	Opcional
Configuração para o RADIUS distribuir portas PVID	**radius vlan enable**	Opcional
Configuração para o RADIUS distribuir o número limite de endereços MAC	**radius mac-address-number enable**	Opcional
Configuração para o RADIUS distribuir o controle de banda	**radius bandwidth-limit enable**	Opcional

Obs.: » ***accounting-on:*** *após o dispositivo reiniciar, ele envia um pacote accounting-on para o servidor RADIUS, notificando-o a forçar o usuário a ficar offline.*

» ***Funcionalidade de compatibilidade h3c-cams:*** *neste recurso, você pode usar o comando de versão do cliente radius para encaminhar esta informação para o servidor RADIUS. Assim, você pode usar o comando de valor de uprate / valor de dnrate para configurar a largura de banda de upstream / downstream no Fabricante Específico.*

» ***Distribuição da prioridade da porta pelo RADIUS:*** *depois que esta função está habilitada, se o usuário se autenticar, a prioridade da porta onde o usuário está localizado é modificada. Esta função é realizada através do número de atributo 77 no Fornecedor específico, que pode ser modificado usando o atributo de configuração de radius.*

- » ***Distribuição do PVID pelo RADIUS:*** *depois que esta função está habilitada, se o usuário passar a autenticação, o PVID da porta onde o ele estiver localizado será modificado. Esta função é realizada usando o tunnel-Pvt-Group-ID, seu valor é uma string. Use esta sequência de caracteres para encontrar a descrição de nome da VLAN desejada.*
- » ***Distribuição do limite de número do endereço MAC pelo RADIUS:*** *depois que esta função é ativada, se o usuário passar pela autenticação, o limite de aprendizado do endereço MAC da porta onde o ele está conectado é modificado. Esta função pode ser modificado usando o uso do radius-config-attribute.*
- » ***Distribuição do controle de largura de banda pelo RADIUS:*** *após essa função estar habilitada, se o usuário passar pela autenticação, a largura de banda da porta onde ele estiver localizado será modificada. O controle de largura de banda de uplink é executado através do número de atributo 75 no Fornecedor Específico por padrão, que pode ser modificado usando o* **theradius***; o controle de largura de banda de downlink é realizado através do número de atributo 76 no Fornecedor Específico por padrão, que pode ser modificado usando o atributo de configuração theradius. A unidade é padrão em kbps e seu valor pode ser modificado através da* **radius config-attribute access-bandwidth unit**.
- » ***Distribuição do ACL pelo RADIUS:*** *esta função não possui comandos de controle. É habilitado por padrão. Configure através de 11 atributos de* **Filter-Id**.

Visualização e manutenção do RADIUS

Operação	Comando	Obrigatório/ opcional
Visualização dos atributos do radius	**show radius attribute**	Opcional
Visualização dos atributos do radius	**show radius config-attribute**	Opcional
Visualização das informações de configuração do serviço radius	**show radius host** hostname	Opcional
Habilitar a função de depuração do radius	**debug radius**	Opcional

26.3. Exemplo de configuração de RADIUS

Configuração da rede e requisitos

Conforme exibido a seguir, o PC do usuário está conectado à porta 0/1 da OLT, a porta 0/4 está conectada ao servidor radius (servidor radius integrado com o Windows 2003) e a autenticação 802.1x está habilitada na porta 0/1.

- Os requisitos específicos são os seguintes:
  - Utilizar a autenticação radius.
  - O PC do usuário deve ser autenticado antes de acessar a internet.
  - Após o usuário passar a autenticação, a ACL é distribuída através do servidor radius. Nesse caso, o usuário pode acessar a Internet, mas não pode acessar o servidor FTP.
  - Depois que o usuário passar a autenticação, distribua o controle de largura de banda através do servidor RADIUS para limitar a largura de banda de ligação upstream para ser 2M e a largura de banda a downstream para ser 1M.

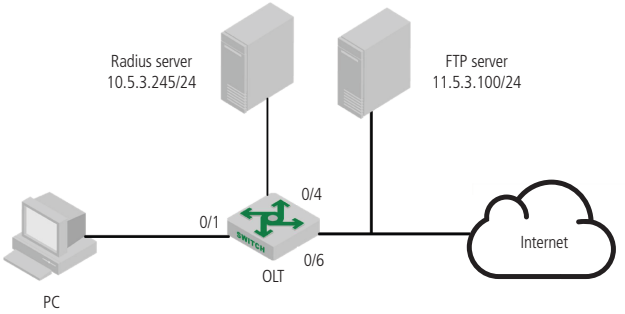


Diagrama de rede para exemplo de configuração de raio

- Passos de configuração:
  - Preparação inicial:
    - Instale o cliente 802.1X no PC.
    - Interface de usuário de configuração OLT IP 10.5.3.235/24 para garantir o ping ao servidor radius:

      OLT4840E(config-if-vlanInterface-1)#interface vlan-interface 1

      OLT4840E(config-if-vlanInterface-1)#ip address 10.5.3.235 255.255.255.0

      This ipaddress will be the primary ipaddress of this interface.

Config ipaddress successfully!

OLT4840E(config-if-vlanInterface-1)#

OLT4840E(config-if-vlanInterface-1)#

OLT4840E(config-if-vlanInterface-1)#exit

OLT4840E(config)#ping 10.5.3.254

PING 10.5.3.254: with 32 bytes of data:

reply from 10.5.3.254: bytes=32 time<10ms TTL=128

reply from 10.5.3.254: bytes=32 time<10ms TTL=128

----10.5.3.254 PING Statistics----

2 packets transmitted, 2 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

Control-C

- » O servidor radius adiciona o NAS IP e a chave compartilhada é 123456.
- » Configure o nome de usuário (teste) e a senha de autenticação do cliente 802.1x (123456) no servidor radius.
- » O valor do atributo 75 no Fornecedor Específico no servidor radius é definido como 2048 Kbps e o valor do atributo do 76 no Fornecedor específico é definido como 1024 Kbps.
- » O valor do atributo do atributo 11 do ID do Filtro no servidor radius é definido como 100.

» Acesse a porta OLT 0/1 para habilitar o dot1x, configure o serviço relacionado do RADIUS e configure os ACLs

OLT4840E(config)#dot1x method portbased interface ethernet 0/1 //habilite o 802.1X

OLT4840E(config)#aaa

OLT4840E(config-aaa)#radius host ngn

OLT4840E(config-aaa-radius-ngn)#primary-auth-ip 10.5.3.254 1812// Configure a função *Accouting*

authentication IP, and port number

OLT4840E(config-aaa-radius-ngn)#primary-acct-ip 10.5.3.254 1813

OLT4840E(config-aaa-radius-ngn)#auth-secret-key 123456 // Configure para compartilhar a chave

OLT4840E(config-aaa-radius-ngn)#acct-secret-key 123456

OLT4840E(config-aaa-radius-ngn)#exit

357

OLT4840E(config-aaa)#radius bandwidth-limit enable // Habilitar a função de envio de banda

OLT4840E(config-aaa)#domain ngn.com

OLT4840E(config-aaa-domain-ngn.com)#radius host binding ngn

OLT4840E(config-aaa-domain-ngn.com)#state active

OLT4840E(config-aaa-domain-ngn.com)#exit

OLT4840E(config-aaa)#default domain-name enable ngn.com

OLT4840E(config)#access-list 100 deny any 11.5.3.100 0.0.0.255 // Configure o ACL para negar acesso ao segmento de rede destino 11.5.3

OLT4840E(config)#access-list 100 permit any any

Validação de resultados

Use o cliente 802.1X PC e, em seguida insira o nome do usuário e a senha para autenticação.

Depois que a autenticação for bem-sucedida, o usuário pode acessar a rede externa normalmente. A informação dos usuários on-line pode ser encontrada no OLT. O comando do show dot1x radius-acl exibe o status do acl100 como habilitado e a largura de banda da direção de entrada da porta 0/1 é limitada a 2048 enquanto a direção de saída é limitada a 1024.

OLT4840E(config)#show dot1x session

port vid mac username login time

e0/1 1 c8:3a:35:d3:e3:99 test@ngn.com 2000/12/11 15:07:00

Total [1] item(s).

OLT4840E(config)#show dot1x radius-acl

The format of radius acl is string.

The prefix of radius acl is assignacl-.

Port acl Status

e0/1 100 enable

Total entries: 1.

OLT4840E(config)#show bandwidth-control interface ethernet 0/1

port Ingress bandwidth control Egress bandwidth control

e0/1 2048 kbps 1024 kbps

Total entries: 1.

27. Configuração de segurança de porta

27.1. Visão geral de seguraça de porta

A segurança da porta geralmente é aplicada na camada de acesso. Ele pode restringir o host de acessar a rede através do dispositivo e permitir que certos hosts acessem a rede, enquanto outros hosts não podem acessá-la.

A função de segurança da porta liga o endereço MAC do usuário, o endereço IP, a ID da VLAN e o número da PORTA com flexibilidade e evita que usuários ilegais acessem a rede. Isso garante a segurança dos dados da rede e os usuários legais podem obter largura de banda suficiente.

Os usuários podem restringir os hosts que podem acessar a rede através de três regras: *regra MAC*, *regra IP* e *regra MAX*. As regras de MAC são divididas em três métodos de ligação: *ligação MAC*, *ligação MAC + IP*, *ligação MAC + VID*; a regra MAX define o número máximo de endereços MAC que podem ser aprendidos em uma porta. Este endereço não inclui o número de regras MAC e as regras IP geradas pelo endereço MAC legítimo. Na regra MAX, existem regras Sticky. Se a regra de negação só estiver configurada na porta e a regra MAX não estiver configurada, os outros pacotes não podem ser reencaminhados (exceção: permitindo a verificação de regras).

O endereço MAC da regra Sticky pode ser aprendido automaticamente e configurado manualmente e salvo no arquivo de configuração em execução. Se o arquivo de configuração for salvo antes que o dispositivo seja reinicializado, o dispositivo não precisa ser configurado novamente após o dispositivo reiniciar e esses endereços MAC produzem efeito automaticamente. Quando a função *Sticky* está habilitada na porta, o endereço MAC dinâmico aprendido pela regra MAX é adicionado à regra Sticky e salvo no arquivo de configuração em execução. No caso da regra MAX não estar cheia, é permitido continuar a aprender o novo endereço MAC e formar a regra Sticky até que o número de regras Sticky atinja o máximo configurado pelo MAX.

As regras de MAC e as regras de IP podem especificar se as mensagens que correspondem às regras podem se comunicar. O endereço MAC do usuário e a VLAN, endereço MAC e endereço IP podem ser vinculados de forma flexível pela regra MAC.

Como a segurança da porta é baseada em software, o número de regras não está limitado pelos recursos de hardware, tornando a configuração mais flexível.

As regras da segurança da porta são acionadas pelas mensagens ARP do dispositivo terminal. Quando o dispositivo recebe uma mensagem ARP, a segurança da porta extrai várias informações de mensagens e combina com as três regras da configuração. A ordem de correspondência é o endereço MAC, endereço IP e regra MAC. A tabela de reencaminhamento da Camada 2 da porta é controlada pelo resultado correspondente, para controlar o comportamento de encaminhamento da porta.

Quando a mensagem de decisão de segurança da porta é ilegal, as mensagens são processadas em conformidade. Existem três modos: proteger, restringir e desligar. O modo de proteção descarta os pacotes. O modo de restrição descarta mensagens e alarmes de captura (Receba uma mensagem ilegal em dois minutos do alarme). O modo *Desligamento* desligará a porta além de restringir o modo de ação.

27.2. Configuração da segurança de porta

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface ethernet** port-number	-
Habilitar/desabilitar a segurança de porta	**port-security { enable | disable }**	Obrigatório
Configuração da regra de vínculo de MAC	**[no] port-security { permit | deny }** mac-address **mac-address { [vlan-id** vlan-id **] | ip-address** ip-address **}**	Opcional
Configuração de regras de IP	**[no] port-security { permit | deny } ip-address** start-ip **[to** end-ip]	Opcional
Configuração da regra MAC	**[no] port-security maximum** value	Opcional
Habilitar o Sticky	**[no] port-security permit mac-address sticky**	Opcional
Configuração de regra de MAC Sticky	**[no] port-security permit** mac-address **sticky mac-address [vlan-id** vlan-id **]**	Opcional
Configuração do tempo de envelhecimento do endereço	**[no] port-security aging time** value	Opcional
Habilitar a recuperação automática de desligamento	**[no] port-security recovery**	Opcional

Operação	Comando	Obrigatório/ opcional
Configuração do tempo de recuperação automática de desligamento	**[no] port-security recovery time** value	Opcional
Remover o endereço MAC ativo	**no port-security active-address {all | configured | learned }**	Opcional
Remover todas as configurações relacionadas à segurança da porta	**no port-security all**	Opcional
Visualização das informações de segurança	**show port-security [interface list]**	Opcional
Visualização das configurações de regras de MAC	**show port-security mac-address [interface ethernet** port-number **]**	Opcional
Visualização das configurações de regras de IP	**show port-security ip-address [interface ethernet** port-number **]**	Opcional
Visualização do endereço MAC ativo	**show port-security active-address [configured | learned | interface ethernet** port-number **]**	Opcional
Visualização da recuperação automática de desligamento	**show port-security recovery [interface ethernet** port-number **]**	Opcional

Obs.: » *Depois que a função de segurança de porta estiver habilitada, ela nega todas as mensagens por padrão. Portanto, você deve configurar uma das regras MAC \ IP \ MAX.*

» *Se a função* STICKY *for efetiva, é necessário que a segurança da porta seja ativada e o número da regra MAX não esteja configurado como 0. Quando esta função é ativada, os endereços dinâmicos aprendidos na regra MAX anterior são convertidos para regras Sticky e armazenadas no arquivo de execução. Quando a função está desativada, as regras Sticky aprendidas são excluídas. O número de entradas da regra Sticky de uma porta não pode exceder o número configurado de regras MAX. Se o arquivo de configuração for salvo antes do dispositivo reiniciar, a regra Sticky salva antes que as reinicializações da porta entram em vigor. Quando a porta está desligada, há duas maneiras de recuperação:*

» *Configurar a porta para desligamento e sem desligamento.*

» *Recuperação automática após a configuração do desligamento.*

» *Quando a mensagem ilegal é recebida, os alarmes de trap não produzem efeitos imediatamente. As traps são geradas dentro de dois minutos.*

» *Se um endereço MAC ou endereço IP for negado e se o limite superior de MAX não for atingido, o host não pode comunicar-se.*

» *A segurança da porta não pode ser ativada juntamente com a autenticação 802.1X ou MAC.*

» *A segurança da porta não pode ser ativada juntamente com inundações anti-ARP.*

27.3. Exemplo de configuração de segurança de porta

» Requisitos de rede:

» Configure a porta 1 para permitir apenas uma comunicação do PC A:

» Passos de configuração:

» Configure a segurança de porta:

OLT4840E(config)#interface ethernet 0/1

OLT4840E(config-if-ethernet-0/1)#port-security enable

OLT4840E(config-if-ethernet-0/1)#port-security permit mac-address 00:00:00:11:11:11

» Verifique os resultados:

» Usando tester emulation no PC A, configure duas placas de rede para obter endereço IP através do DHCP , configure DHCP-Snooping no OLT, acesse o IP da seguinte maneira:

OLT4840E(config)#show dhcp-snooping clients

DHCP client information:

d - days, h - hours, m - minutes, s - seconds

IPAddress mac vlan port LeaseTime ExceedTime

192.168.1.100 00:00:00:11:11:11 1 e0/1 1d0h0m0s 23h51m21s

192.168.1.101 00:00:00:54:20:71 1 e0/1 1d0h0m0s 23h55m37s

Total entries: 2. Printed entries: 2.

» Use o OLT para fazer ping nos dois clientes separadamente, obtenha a entrada ARP e habilite o OLT para estabelecer a tabela de ativação da segurança da porta.

OLT4840E(config)#show arp all

Informations of ARP

d - days, h - hours, m - minutes, s - seconds

IPAddress Mac_Address Vlan Port Type ExpireTime Status

192.168.1.100 00:00:00:11:11:11 1 e0/1 dynamic 17m52s valid

192.168.1.101 00:00:00:54:20:71 1 e0/1 dynamic 18m12s valid

Total entries:2

» Exibir os endereços MAC atualmente ativos. Somente são exibidas as entradas de regras dos MACs permitidos.

OLT4840E(config)#show port-security active-address

Acitve mac-address:

Port MAC address VID IP Addr Derivation Action Age(min)

E1/0/1 00:00:00:11:11:11 1 192.168.1.100 MAC permit 1

Total entries: 1

OLT4840E(config)#debug port-security

OLT4840E(config)#logging monitor 0

» Tente se comunicar com o OLT usando dois PCs, respectivamente: os resultados são os seguintes:

  » Use o IP = 192.168.1.100 (MAC = 00: 00:00:11:11:11 correspondem à segurança da porta de segurança) para executar ping no OLT. Pode se comunicar, o log é o seguinte:

  00:29:48: OLT: %PORT-SECURITY-7-debug: port e0/1 recv packet mac[00:00:00:11:11:11] vlan

  [1] type[0x0806]

  00:29:48: OLT: %PORT-SECURITY-7-debug: match with MAC RULE

  00:29:48: OLT: %PORT-SECURITY-7-debug: action: PERMIT

» Use a IP = 192.168.1.101 (MAC = 00:00:00:54:20:71 correspondem à regra de segurança da porta) para fazer ping no OLT. Pode se comunicar, o log é o seguinte:

00:30:07: OLT: %PORT-SECURITY-7-debug: port e0/1 recv packet mac[00:00:00:54:20:71] vlan

[1] type[0x0806]

00:30:07: OLT: %PORT-SECURITY-7-debug: match with MAX RULE

00:30:07: OLT: %PORT-SECURITY-7-debug: port e0/1 maxnum exceed

Maxnum rule por padrão é 0, então exceda, a mensagem é descartada.

28. Cliente SNTP

28.1. Introdução a função *SNTP*

A hora do sistema OLT pode ser alcançado de duas maneiras, uma é como cliente SNTP, o servidor sincroniza automaticamente os relógios; o outro é a configuração própria do administrador.

O protocolo de tempo de rede simples (SNTP – Simple Network Time Protocol) é usado para sincronização de tempo entre dispositivos de rede. Normalmente, um servidor SNTP existe na rede e fornece tempo de referência para vários clientes. Desta forma, existe uma sincronia do tempo entre todos os dispositivos conectados.

O SNTP pode funcionar em quatro modos: *Unicast, Broadcast, Multicast* e *Anycast*.

No modo *Unicast*, o cliente inicia uma solicitação para o servidor. Depois de receber o pedido, o servidor constrói uma mensagem de resposta com base na hora local e a envia de volta ao cliente.

No modo de *Broadcast* e multicast, o servidor envia periodicamente mensagens de broadcast ou multicast para os clientes.

No modo *Anycast*, o cliente inicia um endereço de broadcast local ou um endereço multicast para enviar uma solicitação. Nesse caso, o servidor da rede responde ao cliente, seleciona o servidor do qual recebeu a mensagem e descarta as mensagens enviadas por outros servidores. Depois disso, o padrão de trabalho é igual ao unicast.

Em todos os modos, o cliente recebe uma mensagem de resposta para analisar e obter o tempo padrão atual, calculando o atraso da transmissão da rede e a compensação do tempo local através de um determinado algoritmo.

28.2. Configuração do cliente SNTP

Habilitar/desabilitar o cliente SNTP

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o cliente SNTP	**[no]sntp client**	Obrigatório, *desabilitado* por padrão
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional
Visualização do horário do sistema	**show clock**	Opcional

Configuração do modo de trabalho do cliente SNTP

De acordo com a rede, os administradores podem usar comandos para modificar o modo de trabalho SNTP - unicast, broadcast, multicast ou anycast.

» Configure o modo de trabalho do cliente SNTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configure o Modo de Trabalho do Cliente SNTP	**sntp client mode {** broadcast | unicast | multicast | anycast [**key** key-id **] }**	Opcional, *broadcast* por padrão
Visualização da configuração do cliente SNTP	**show sntp client**	Opcional

Configuração do endereço do servidor SNTP

Quando um cliente SNTP funciona no modo *Unicast*, o usuário deve configurar o servidor SNTP especificado.

» Configuração do endereço do servidor SNTP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o endereço do servidor SNTP	**[no]sntp server** ip-address	Obrigatório
Configurar o backup do servidor SNTP	**[no]sntp server backup** ip-address	Opcional
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Modificar o atraso de transmissão de broadcast

Quando o cliente SNTP funciona no modo *Broadcast* ou *Multicast*, é necessário usar o parâmetro de atraso de transmissão. Neste modo, a hora do sistema local do cliente SNTP é igual ao tempo extra do servidor mais o atraso da transmissão. Os administradores podem modificar o atraso de transmissão com base na largura de banda real da rede.

» Modificar o atraso de transmissão de broadcast:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o atraso de propagação de broadcast	**[no]sntp broadcastdelay** value	Opcional, *3ms* por padrão
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Configuração do TTL multicast

Quando um cliente SNTP opera no modo *Anycast* e usa endereços multicast para enviar pedidos, o usuário precisa configurar o valor TTL para limitar o alcance da mensagem multicast.

» Configuração do TTL multicast:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o TTL multicast	**sntp client multicast ttl** value	Opcional, *255* por padrão
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Configuração do intervalo de polling

O usuário precisa configurar o intervalo de polling quando o cliente SNTP funciona no modo *Unicast* ou *Anycast*. O cliente inicia uma solicitação ao servidor a cada intervalo de pesquisa para calibrar a hora local do sistema.

» Configurar o Intervalo de Polling:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o intervalo de polling	**[no]sntp client poll-interval** value	Opcional, *1000* por padrão
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Configuração de retransmissão de timeout

Como a mensagem de solicitação SNTP é uma mensagem UDP, não é possível garantir que o pacote de solicitação tenha chegado ao destino. O mecanismo de timeout de retransmissão é adotado. Este intervalo é necessário quando o cliente SNTP funciona no modo *Unicast* ou *Anycast*. Quando o cliente envia um pedido e fica sem receber resposta por um determinado período de tempo, será reenviado o pedido até o número de retransmissão exceder o valor definido. O mecanismo de timeout de restrasmissão configurado só produz efeitos no modo *Unicast* ou *Anycast*.

» Configure as tentativas de retransmissão de timeout e o intervalo de tempo:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o intervalo de retransmissão de timeout	**[no]sntp client retransmit-interval** value	Opcional, *5s* por padrão
Configurar o número de tentativas de retransmissão de timeout	**[no]sntp client retransmit** value	Opcional, *0* por padrão
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Configuração de horário de verão

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar o horário de verão	**[no]sntp client summer-time dayly** { start-month start-day start-time end-month end-day end-time }	Opcional
	[no]sntp client summer-time weekly { start-month start-week [Fri |mon| sat | sun | thu | tue | wed] start-time end-month end-week [Fri | mon | sat | sun | thu | tue | wed] end-time }	
Visualização da configuração do horário de verão	**show sntp client summer-time**	Opcional

Configuração de lista de servidores válidos

Quando um cliente SNTP funciona em modo *Broadcast* ou *Multicast*, ele confiará e receberá os pacotes de protocolo de qualquer servidor. Se houver um ataque malicioso (que fornece o tempo errado), a hora local não poderá ser sincronizada com o tempo padrão.

Depois que a lista de servidores válidos é configurada no cliente SNTP, ele só poderá receber mensagens cujos endereços de origem estão na lista, melhorando assim a segurança.

» Configurar a lista de servidores legais:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configurar lista de servidores legais	**sntp client valid-server** ipaddress wildcard	Opcional
Remover lista de servidores legais	**[no]sntp client retransmit** value	Opcional, *0* por padrão
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Configuração de autenticação

Para melhorar ainda mais a segurança, o usuário pode habilitar a autenticação MD5 entre o servidor SNTP e o cliente, assim o cliente recebe apenas mensagens autenticadas. A configuração de autenticação é a seguinte:

» Configuração de autenticação:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar autenticação	**[no] sntp client authenticate**	Opcional, *desligado* por padrão
Configuração de senha de autenticação	**[no]sntp client authentication-key** key-number **md5** value	Opcional
Configuração de um ID de senha confiável	**[no]sntp trusted-key** key-number	Opcional, apenas para modos *Multicast* e *Broadcast*, deve ser igual a chave de autenticação

Operação	Comando	Obrigatório/ opcional
Configuração do ID de senha utilizado pelo servidor	**[no]sntp server key** key-number	Opcional, deve ser igual a chave de autenticação
Configuração do ID de senha para configuração anycast	**sntp client mode anycast key** key-number	Opcional
Visualização das informações de configuração do cliente SNTP	**show sntp client**	Opcional

Manual de calibração do relógio do sistema

Além do OLT atuar como cliente SNTP e automaticamente sincronizar o tempo do servidor, a outra maneira é a calibração manual do administrador do relógio do sistema.

O OLT possui uma bateria de Lítio que garante que o relógio do sistema não pare de funcionar enquanto o OLT esteja desligado.

» Configurar o relógio do sistema:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de execução	**configure terminal**	-
Configuração do relógio do sistema	**clock set** HH:MM:SS YYYY/MM/DD	Obrigatório
Acesse o modo de configuração global	**configure terminal**	Opcional
Configure o fuso horário do sistema	**[no]clock timezone** zone-name hours-offset minutes-offset	Opcional
Configurar o horário de verão	**[no]sntp client summer-time dayly** { start-month start-day start-time end-month end-day end-time } **[no]sntp client summer-time weekly** { start-month start-week [Fri |mon| sat | sun | thu | tue | wed] start-time end-month end-week [Fri | mon | sat | sun | thu | tue | wed] end-time }	Opcional
Visualização da hora do sistema	**show clock**	Opcional

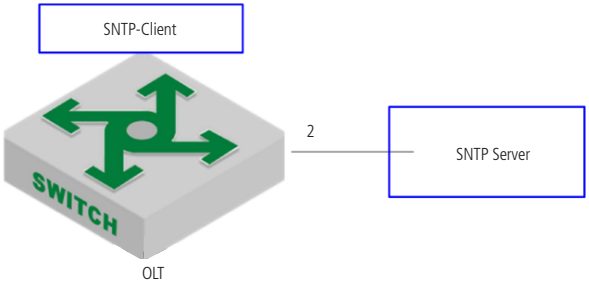
Exemplo:

» Configure o relógio do sistema:
OLT4840E#clock set 17:50:50 2015/11/25
Set clock successfully.
Clock will be reset to 2013/01/01 00:00:00 after system rebooting because there is no realtime clock chip.

OLT4840E#show clock
Wed 2015/11/25 17:51:03 CCT 08:00

Exemplo de configuração de cliente SNTP

» Requisitos de rede:
O OLT atua como o cliente SNTP para sincronizar o tempo do servidor.
Verifique se o OLT se comunica corretamente com o servidor SNTP.



» Passos de configuração:
  » OLT executa os modos *Broadcast*, *Multicast*, *Unicast* e *Anycast*, respectivamente.
  » Configuração do modo de autenticação e modo *Broadcast*.
    » Habilite o cliente *SNTP* e o configure no modo *Broadcast* (está ativado por padrão).
    OLT4840E(config)#sntp client mode broadcast
    » Configure o servidor confiável:
    OLT4840E(config)#sntp client valid-server 192.168.1.99 0.0.0.0
    OLT4840E(config)#sntp client

» Configure a chave de autenticação (verifique se a configuração é consistente com a do servidor):
OLT4840E(config)#sntp client authentication-key 1 md5 test

» Configure o ID da chave confiável:
OLT4840E(config)#sntp trusted-key 1

» Ativa a função de autenticação:
OLT4840E(config)#sntp client authenticate

» Exiba o resultado da sincronização do tempo:
OLT4840E(config)#show sntp client

Clock state : synchronized Current mode : broadcast

Use server : 192.168.1.99 State : idle

Server state : synchronized Server stratum : 1

Authenticate : enable Bcast delay : 3ms

Last synchronized time: THU NOV 26 06:07:44 2015

Summer-time is not set.

Valid server list:

Server address:192.168.1.99 wildcard:0.0.0.0

» Modo de multicast e configuração de autenticação.

» Habilite o cliente sntp e configure-o como o modo *Multicast*.
OLT4840E(config)#sntp client mode multicast

» Configure a liste de servidores confiáveis.
OLT4840E(config)#sntp client valid-server 192.168.1.99 0.0.0.0

OLT4840E(config)#sntp client

» Configure a chave de autenticação (verifique se a configuração é consistente com a do servidor)
OLT4840E(config)#sntp client authentication-key 1 md5 test

» Configure o ID da chave confiável.
OLT4840E(config)#sntp trusted-key 1

» Ativa a função de autenticação.
OLT4840E(config)#sntp client authenticate

» Exiba o resultado da sincronização de horário do OLT.
OLT4840E(config)#show sntp client

Clock state : synchronized Current mode : multicast

Use server : 192.168.1.99 State : idle

Server state : synchronized Server stratum : 1

Authenticate : enable Bcast delay : 3ms

Last synchronized time: THU NOV 26 06:20:59 2015

Summer-time is not set.

Valid server list:

Server address:192.168.1.99 wildcard:0.0.0.0

» Configure o modo de autenticação e o modo *Unicast*.
  » Ative o cliente sntp e configure-o como unicast.
  OLT4840E(config)#sntp client

  OLT4840E(config)#sntp client mode unicast
  » Configure o servidor SNTP.
  OLT4840E(config)#sntp server 192.168.1.99
  » Configure a chave de autenticação (verifique se a configuração é consistente com a do servidor).
  OLT4840E(config)#sntp client authentication-key 1 md5 test
  » Configure a ID da senha para o servidor.
  OLT4840E(config)#sntp server key 1
  » Ativa a função de autenticação.
  OLT4840E(config)#sntp client authenticate
  » Exiba o resultado da sincronização do tempo.
  OLT4840E(config)#show sntp client

  Clock state : synchronized Current mode : unicast

  Use server : 192.168.1.99 State : idle

  Server state : synchronized Server stratum : 1

  Retrans-times: 3 Retrans-interval: 30s

  Authenticate : disable PrimaryServer: 192.168.1.99

  Backup Server: 0.0.0.0 Poll interval : 1000s

  Last synchronized time: THU NOV 26 09:05:29 2015

  Last received packet's originateTime: TUE JAN 01 00:00:24 2013

  Summer-time is not set.

» Configure o modo de autenticação e o modo *Anycast*.

» Ative o cliente SNTP e configure-o para funcionar no modo *Anycast*.
OLT4840E(config)#sntp client mode anycast

» Configure o servidor SNTP.
OLT4840E(config)#sntp server 192.168.1.99

OLT4840E(config)#sntp client

» Configure a chave de autenticação (verifique se a configuração é consistente com a do servidor).
OLT4840E(config)#sntp client authentication-key 1 md5 test

» Configure o modo *Anycast* e a identificação da chave (se a autenticação não for necessária, você não configura).
OLT4840E(config)# sntp client mode anycast key 1

» Ative a função de autenticação.
OLT4840E(config)#sntp client authenticate

» Exiba o resultado da sincronização do tempo.
OLT4840E(config)#show sntp client

Clock state : synchronized Current mode : anycast

Use server : 192.168.1.99 State : idle

Server state : synchronized Server stratum : 1

Retrans-times: 3 Retrans-interval: 30s

Authenticate : enable Authentication-key: 1

Poll interval : 1000s

Last synchronized time: THU NOV 26 09:22:25 2015

Last received packet's originateTime: THU NOV 26 17:22:24 2015

Summer-time is not set.

29. PPPoE Plus

29.1. Visão geral de PPPoE Plus

O protocolo ponto a ponto sobre Ethernet (PPPoE) é um protocolo de tunelamento de rede que encapsula o protocolo ponto a ponto (PPP) em uma moldura Ethernet. Como o PPP está integrado no protocolo, ele pode implementar as funções de autenticação, criptografia e compressão que não podem ser fornecidas pela Ethernet tradicional. Também pode ser usado para arquitetura de protocolo que fornece serviços de acesso para usuários por protocolo Ethernet, como DSL e assim por diante.

A função *PPPoE Plus* significa que a informação física do lado do usuário (a porta conectada, a VLAN onde reside, o endereço MAC do OLT local e assim por diante) é adicionada ao campo Sub-tag no pacote de protocolo PPPoE pelo OLT diretamente conectado ao usuário final. Desta forma, o servidor de autenticação pode ler as informações para saber a localização do usuário na rede para gerenciar, manter e atender usuários. Observe que esta função requer um servidor que suporte PPPoE Plus para funcionar.

29.2. Configuração de PPPoE Plus

Habilitar/desabilitar o PPPoE Plus

Por padrão, a função *PPPoE Plus* está desabilitada. Quando você precisar usar a função, você deve configurá-lo da seguinte maneira:

1. Ative a função *PPPoE Plus* na porta;
2. A porta que se conecta ao PPPoE-Server é configurada como uma porta confiável (todas as portas não são confiáveis por padrão).

» Habilitar/desabilitar o PPPoE Plus:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-number	-
Habilitar/desabilitar o PPPoE Plus	**[no] pppoeplus**	Obrigatório, por padrão está desativado

Operação	Comando	Obrigatório/ opcional
Configuração da porta de uplink para porta confiável	**[no] pppoeplus trust**	Obrigatório, a porta não é confiável por padrão
Visualização de informações de configuração	**show pppoeplus interface {ethernet | pon}** port-number	Opcional

Configuração de estratégia de processamento de opção

Se a porta de downlink PPPoE estiver diretamente conectada a um PC ou a um OLT com PPPoE desativado, o OLT recebe o pacote PPPoE sem opções. O OLT processa o pacote de acordo com o padrão. Se a porta de dowlink estiver conectada a um OLT com PPPoE habilitado, o pacote PPPoE recebido pode já conter o conteúdo da opção. Nesse caso, o administrador precisa especificar como o OLT deve lidar com a opção. É possível permitir três estratégias de processamento: descartar, manter e substituir, o padrão é utilizar a estratégia de substituição.

» Configuração de estratégia de processamento de opção:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-number	-
Configuração de estratégia de processamento de opção	**[no] pppoeplus strategy { drop | keep | replace}**	Opcional, o comando *no* restaura a estratégia padrão de *substituir*
Visualização de informações de configuração	**show pppoeplus interface {ethernet | pon}** port-number	Opcional

Descartar pacotes padi/pado

Em alguns casos específicos, você pode não querer que a porta processe os pacotes PPPoE padi / pado recebidos. O OLT fornece a função de descartar, ela está desabilitada por padrão.

» Configuração do descarte de pacotes padi/pado:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-number	-
Configuração do descarte de pacotes padi/pado	**[no] pppoeplus drop {**padi **|** pado**}**	Opcional, por padrão está desativado
Visualização de informações de configuração	**show pppoeplus interface {ethernet | pon}** port-number	Opcional

Configuração de tipo de pacotes

O pacote PPPoE precisa ser adicionado com o conteúdo da opção antes do pacote ser encaminhado. O conteúdo da opção pode ser determinado de várias maneiras.

Você pode especificar o conteúdo da opção no modo de porta.

Se nenhum conteúdo for especificado, a configuração é realizada de acordo com as regras de configuração e o tipo é configurado usando o tipo PPPoE Plus. Quando o tipo é autodefinido, você precisa determinar se o formato está em formato binário ou formato de texto. O formato de texto também precisa determinar o formato dos caracteres de conexão.

O OLT fornece três modos para pacotes PPPoE Plus:

» **Modo *Padrão*:** as informações do lado do usuário incluem a porta conectada, a VLAN e o OLT MAC local. A codificação é a seguinte:
"0 0/0/0: 4096.VID Switch MAC / 0/0 / slot / subslot / port"

» **Modo *HuaWei*:** suporte de conexão com HuaWei BRAS. As informações do lado do usuário incluem a porta conectada, a VLAN, o nome do host do OLT local e o OLT MAC local. A codificação é a seguinte:
"0 0/0/0: 4096.VID Switch MAC / hostname / 0 / slot / sub-slot / port"

» **Modo *Autodefinido*:** suporte ao formato de mensagem definido pelo usuário.

» Configuração de tipo de pacotes:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do tipo de pacote	**[no]pppoeplus type { huawei | standard | self-defined { circuit-id { [**circuit-string**] [vlan] [port] [switch-mac] [hostname] [client-mac] } | remote-id { [**remote-string**] [switch-mac] [hostname] [client-mac] } }}**	Opcional, o comando *no* recupera o tipo padrão
Configuração de formato	**[no]pppoeplus format { binary | ascii }**	Opcional, o comando *no* recupera o tipo binário
Configuração de delimitação	**[no]pppoeplus delimiter { colon | dot | slash | space }**	Opcional, o comando *no* recupera o padrão: espaço
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-number	-
Configuração do circuit-id	**[no] pppoeplus circuit-id** circuit-string	Opcional
Visualização de informações de configuração	**show pppoeplus interface {ethernet | pon}** port-number	Opcional

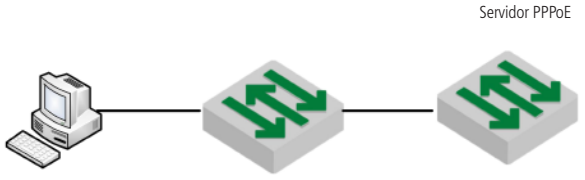
Obs.: *se o global e a porta estiverem configurados com o circuit-id, a porta tem precedência.*

Exemplo de configuração

» Requisitos de rede:

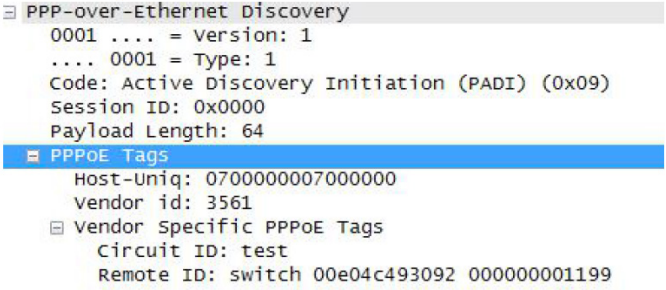
A função PPPoE + está habilitada no OLT e é configurada com o tipo autodefinido.

Configure o circuit-id e o remote-id e verifique se o PC faz a autenticação PPPoE e as opções no pacote PPPoE estão corretas.



PPPoE +

» Passos de configuração:
  » Ative a função *PPPoE Plus* na porta conectada ao PC cliente
    OLT4840E(config)#interface ethernet 0/1
    OLT4840E(config-if-ethernet-0/1)#pppoeplus
  » A porta conectada ao servidor está configurada como uma porta confiável PPPoE Plus:
    OLT4840E(config-if-ethernet-0/1)#interface ethernet 0/3
    OLT4840E(config-if-ethernet-0/3)#pppoeplus trust
  » Configure o tipo autodefinido e configure o circuit-id e o remote-id:
    OLT4840E(config-if-ethernet-0/3)#exit
    OLT4840E(config)#pppoeplus type self-defined circuit-id test
    OLT4840E(config)#pppoeplus type self-defined remote-id hostname client-mac switch-mac
    OLT4840E(config)#pppoeplus format ascii
» Validação de resultados:
  » PC obteve sucesso na discagem PPPoE.
  » Os campos circuit-id e remote-id do pacote de confiança e os pacotes padi espelhados são consistentes com a configuração:



30. Download e upload de arquivos

30.1. Função de download de arquivos

O download de arquivos é copiar arquivos de uma memória externa para o OLT, como o arquivo de atualização (arquivo de host, arquivo bootrom), o arquivo de configuração e o arquivo de chave SSH.

A extensão do arquivo de host deve ser .arj; a extensão do arquivo *bootrom* deve ser .bin; a extensão do arquivo de configuração deve ser .txt; a extensão do arquivo de chave SSH deve ser *.txt*.

O suporte para ferramentas de download inclui xmodem, TFTP, FTP.

Quando um arquivo externo é baixado para o OLT, ele é salvo na memória flash e não entra em vigor imediatamente, para isso você precisa executar os comandos de configuração relacionados. Depois de atualizar o host e o bootrom, você precisa reiniciar o OLT, quando você baixar o arquivo de configuração, ele irá substituir o arquivo original na flash. Você precisa usá-lo no modo *Privilegiado*: *copy startup-config running-config*. Consulte o manual do usuário do módulo SSH para obter o uso da chave.

Configuração de download de arquivo

Operação	Comando	Obrigatório/ opcional
Acesse o modo *Privilegiado*	-	-
Atualizar o arquivo mestre de host	**xmodem toolload application xmodem**	Opcional
	Tftp toolload application tftp inet[6] server-ipxxx.arj	Obrigatório
	Ftp toolload application ftp inet[6] server-ipxxx.arj **grn 123**	Opcional
Atualizar o arquivo de host de backup	**ftp toolload application ftp inet[6]** server-ipxxx.arj **grn 123**	Obrigatório
Atualizar o arquivo de bootrom	**xmodem toolload whole-bootrom xmodem**	Opcional
	Tftp toolload whole-bootrom tftp inet[6] server-ipxxx.bin	Obrigatório
	Ftp toolload whole-bootrom ftp inet[6] server-ipxxx.bin **grn 123**	Opcional
Download do arquivo de configuração	**xmodem toolload configuration xmodem**	Opcional
	Tftp toolload configuration tftp inet[6] server-ipxxx.txt	Obrigatório
	Ftp toolload configuration ftp inet[6] server-ipxxx.txt **grn 123**	Opcional
Download do arquivo de chave SSH	**tftp tool load keyfile private tftp[6] server-ip xxx.txt load keyfile public tftp[6]server-ip xxx.txt**	Obrigatório
	Tftp tool load keyfile private ftp[6] server-ipxxx.txt grn 123 load keyfile public ftp[6]server-ipxxx.txt grn 123	Opcional
Utilizar o programa backup de host para boot	**startup secondary application**	Opcional
Utilizar o programa de host para boot	**no startup secundary application**	Opcional

Obs.: *o padrão é utilizar no programa mestre de host para boot.*

Exemplo de configuração de download de arquivo

» Requisitos de rede:
O OLT se conecta ao servidor de arquivos para garantir uma comunicação adequada.

» Passos de configuração:

» Verifique se o OLT e o servidor de arquivos estão comunicando corretamente:
OLT4840E#ping 192.168.1.99
PING 192.168.1.99: with 32 bytes of data:
reply from 192.168.1.99: bytes=32 time<10ms TTL=64
reply from 192.168.1.99: bytes=32 time<10ms TTL=64
reply from 192.168.1.99: bytes=32 time<10ms TTL=64
reply from 192.168.1.99: bytes=32 time<10ms TTL=64

----192.168.1.99 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
Control-C

» Atualize o arquivo de host:
OLT4840E#load application tftp 192.168.1.99 host.arj
Downloading application via TFTP...
Download application via TFTP successfully.
EPON(onu-0/1/1)#onu-bandwidth unknown-ucast downstream 300000

» Atualize o arquivo de bootrom:
OLT4840E#load whole-bootrom tftp 192.168.1.99 bootrom_rom.bin

» Reinicie o dispositivo e utilize o arquivo baixado como host e bootrom:
OLT4840E#reboot

» Faça o dowload dos arquivos de configuração:
OLT4840E#load configuration tftp 192.168.1.99 test.txt
Startup config will be updated, are you sure(y/n)? [n]y
Downloading config file via TFTP...
Download config file via TFTP successfully.

» Utilize o arquivo de configuração baixado:

OLT4840E#copy startup-config running-config

Running config will be updated, are you sure(y/n)? [n]y

Start to load startup-config, please wait for a while ...

Load successfully

30.2. Upload de arquivos

O upload de arquivos refere-se ao carregamento de arquivos da memória flash do OLT para servidores de arquivos externos, como arquivos de host, arquivos de configuração, arquivos de chaves SSH e arquivos de log no arquivo de atualização. Esta função pode ser utilizada para análise, backup ou migração para outros dispositivos compatíveis.

Recomenda-se que o nome do arquivo carregado tenha a mesma extensão que do arquivo original: a extensão do arquivo do host é .arj; a extensão do arquivo bootrom é .bin; a extensão do arquivo de configuração é .txt; a extensão do arquivo da chave SSH é *.txt*.

Suporta ferramentas de upload como TFTP, FTP.

Configuração de upload de arquivos

Operação	Comando	Obrigatório/ opcional
Acesse o modo *Privilegiado*	-	-
Upload do arquivo de host	tftp toolupload application tftp inet[6] **server-ip xxx.arj**	Obrigatório
	Ftp toolupload application ftp inet[6] **server-ipxxx.arj** grn 123	Opcional
Upload de arquivo de log	tftp toolupload logging tftp inet[6] **server-ip xxx.arj**	Obrigatório
	Ftp toolupload logging ftp inet[6] **server-ipxxx.arj** grn 123	Opcional
Salvar a configuração atual na memória flash	copy running-config startup-config	Obrigatório

Operação	Comando	Obrigatório/ opcional
Upload automático do arquivo de configuração	tftp toolupload automatically configuration tftp inet[6] **server-ip xxx.arj**	Obrigatório
	Ftp tool upload automatically configuration ftp inet[6] **server-ipxxx.arj** grn 123	Opcional
Upload do arquivo de chave SSH	tftp tool upload keyfile private tftp[6]server-ip xxx.txt upload keyfile public tftp[6]server-ip xxx.txt	Obrigatório
	Uptftp tool load keyfile private ftp[6]server-ipxxx.txt grn 123 load keyfile public ftp[6]server-ipxxx.txt grn 123	Opcional

Exemplo de configuração de upload de arquivo

» Requisitos de rede:
O OLT se conecta ao servidor de arquivos para garantir uma comunicação adequada.

» Passo de configuração:

» Verifique se o OLT e o servidor de arquivos estão comunicando corretamente:
OLT4840E#ping 192.168.1.99

PING 192.168.1.99: with 32 bytes of data:

reply from 192.168.1.99: bytes=32 time<10ms TTL=64

reply from 192.168.1.99: bytes=32 time<10ms TTL=64

reply from 192.168.1.99: bytes=32 time<10ms TTL=64

reply from 192.168.1.99: bytes=32 time<10ms TTL=64

----192.168.1.99 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

Control-C

» Faça o upload do arquivo de host:
OLT4840E#upload application tftp 192.168.1.99 host.arj

Uploading APP file via TFTP...

Upload APP file via TFTP successfully.

» Salve a configuração atual na memória flash:
OLT4840E#copy running-config startup-config
Startup config in flash will be updated, are you sure(y/n)? [n]y
Building, please wait...
Update startup config successfully.

» Faça o upload do arquivo de configuração em um servidor externo:
OLT4840E#upload configuration tftp 192.168.1.99 text.txt
Uploading config file via TFTP...
Upload config file via TFTP successfully.

» Faça o upload dos arquivos atuais da memória flash para o servidor de arquivos:
OLT4840E#upload logging tftp 192.168.1.99 logg.txt
Uploading syslog file via TFTP...
Upload syslog file via TFTP successfully

31. Configuração de decompilação

31.1. Visão geral da configuração de decompilação

A configuração do dispositivo pode ser dividida em duas fontes: a primeira é chamada de configuração padrão, que não requer configuração do usuário. Depois que o OLT é ligado pela primeira vez, ou após a configuração de inicialização ser restaurada, as configurações existentes, como o usuário admin, garantem que o OLT satisfaça o ambiente de uso simples. A segunda configuração são as feitas pelo usuário, como criar a VLAN 2, modificando PVID = 2.

A configuração do dispositivo pode ser dividida em três tipos: o primeiro é chamado de configuração de cache temporário ou a configuração de execução atual, como a criação da VLAN 2. Essa configuração não existe após o reinicilaização do OLT. A segunda configuração é chamada de configuração de inicialização, que pode ser carregada (automaticamente ou manualmente) depois que o OLT for reiniciado. A primeira configuração pode ser salva na configuração de inicialização. A terceira configuração é salva no flash. Na configuração, um pequeno número de configurações particularmente importantes serão salvos diretamente no flash: como configuração de empilhamento, configuração de nome de usuário;

a configuração de empilhamento não entrará na decompilação, ou seja, *show running* não será exibido, ele só pode ser exibido pelo comando "show" no módulo. A configuração do nome de usuário entrará na decompilação, ou seja, *show running* o exibirá, também pode ser exibido pelo comando "show" no módulo. A configuração no Flash é permanente e não precisa ser salva com comandos. Se você deseja excluir a configuração do flash, você pode excluí-lo somente através do comando [no] correspondente no módulo.

31.2. Comandos básicos de decompilação

Operação	Comando	Obrigatório/ opcional
Visualização a decompilação do atual arquivo de configuração	**show running-config [module| interface {ethernet | pon} port-number]**	Obrigatório
Visualização da configuração de inicialização	**show startup-config [module]**	Obrigatório
Salvar a configuração atual para a configuração de inicialização	**copy running-config startup-config**	Obrigatório
Carregar o arquivo de inicialização na reinicialização do sistema	**durante o processo de reinício, o padrão é carregar a configuração automaticamente após 6s. Pressione "enter" de acordo com a mensagem do prompt para carregar imediatamente**	Obrigatório
Não carregar o arquivo de inicialização na reinicialização do sistema	**durante o processo de reinício, pressione "ctrl + c" de acordo com a mensagem do prompt**	Opcional
Carregar o arquivo de configuração de boot em linha de comando	**copy startup-config running-config**	Obrigatório
Limpar as configurações de inicialização	**clear startup-config**	Obrigatório

31.3. Configuração do modo de execução

Você pode alterar o modo de execução do arquivo de configuração através da interface de linha de comando. O arquivo de configuração salvo no sistema pode ser executado nos modos *Interruptible* e *Non-interruptible*. Quando um erro é encontrado durante a execução do arquivo de configuração, a

execução no modo *Interruptible* pára imediatamente e faz notificação do erro. No modo *Non-interruptible*, a execução não é interrompida, o erro é repetido e o arquivo de configuração continua a ser executado.

O padrão é o modo *Non-interruptible*.

» Configuração do modo de alteração do arquivo de execução:

Operação	Comando	Obrigatório/ opcional
Definir o modo de execução como *interruptible*	**buildrun mode stop**	Opcional, executável no modo *Privilegiado*
Definir o modo de execução como *non-interruptible*	**buildrun mode continue**	Opcional, executável no modo *Privilegiado*

Exemplo de configuração de decompilação

» Exemplo de configuração:

» Visualize a configuração atual:

```
OLT4840E#show running-config
!LanSwitch BuildRun
enable
configure terminal
![DEVICE]
interface ethernet 0/1
exit
interface ethernet 0/2
exit
interface ethernet 0/3
exit
interface ethernet 0/4
exit
interface ethernet 0/5
exit
```

interface ethernet 0/6

exit

interface ethernet 0/7

400

exit

interface ethernet 0/8

exit

……

» Salve a configuração atual como configuração de inicialização:
OLT4840E#copy running-config startup-config

Startup config in flash will be updated, are you sure(y/n)? [n]y

Building, please wait...

Update startup config successfully.

» Utilize a configuração de inicialização
OLT4840E#copy startup-config running-config

Running config will be updated, are you sure(y/n)? [n]y

Start to load startup-config, please wait for a while ...

Load successfully.

32. Visão geral de alarme de utilização

A função de alarme de utilização do dispositivo é usada para monitorar a sua largura de banda, o consumo de recursos da CPU e gerar notificação de alarme em caso de congestionamento, para que o administrador possa se manter a par da rede e do equipamento em execução.

A função de alarme de utilização da porta pode definir dois limites de alarme de disparo. Sua descrição detalhada é a seguinte:

» **exceed:** quando a utilização da largura de banda da porta equivale ou excede o valor *exceed*, um alarme de congestionamento é disparado.

» **normal:** quando a utilização da largura de banda da porta cai abaixo do valor *normal*, o alarme recuperado é ativado.

A função de alarme de utilização da CPU também pode definir dois limites de alarme de disparo, descritos em detalhes da seguinte maneira:

» **busy:** quando a utilização da CPU é igual ou superior ao valor *busy*, um alarme é acionado, indicando que a CPU está ocupada.

» **unbusy:** quando a utilização da CPU é igual ou inferior ao valor *unbusy*, um alarme é disparado, indicando que a CPU está ociosa.

Obs.: *as informações de alarme são enviadas para Syslog por padrão. Se você deseja enviá-las para o terminal, você precisa habilitar o comando.*

32.1. Configuração de alarme de utilização

» Configuração de alarme de utilização de porta:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o alarme em todas as portas	**[no] alarm all-packets**	Obrigatório
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-number	-
Habilitar/desabilitar o alarme na porta	**[no] alarm all-packets**	Obrigatório
Configuração de limiar	**alarm all-packets threshold exceed** value **normal** value	Opcional
Visualização de informações de alarme	**show alarm all-packetsinterface [ethernet** port-number**]**	Opcional

» Configuração de alarme de utilização de CPU:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o alarme de CPU	**[no] alarm cpu**	Obrigatório
Configuração de limiar	**alarm cpu thresholdexceed** value **normal** value	Opcional
Visualização de informações de alarme	**show alarm cpu**	Opcional

Exemplo de configuração de alarme

» Requisitos de rede:

Quando a utilização da porta 0/2 é de até 50M, as informações do alarme são enviadas.

Quando a utilização da CPU atinge 90%, as informações de alarme são enviadas.

» Etapas de configuração:

» Configure a função de alarme da porta:

OLT4840E(config)#alarm all-packets

OLT4840E(config)#interface ethernet 0/2

OLT4840E(config-if-ethernet-0/2)#alarm all-packets

OLT4840E(config-if-ethernet-0/2)#alarm all-packets threshold exceed 50 normal 40

» Configure o alarme de CPU:

OLT4840E(config)#alarm cpu

OLT4840E(config)#alarm cpu threshold busy 90 unbusy 85

» Resultados de validação:

» Habilite o registro de saída serial:

OLT4840E(config)# logging monitor 0

» Quando a CPU atinge o limite configurado, as seguintes informações de alarme são exibidas:

02:44:02: Switch: %OAM-5-CPU_BUSY: cpu is busy.

OLT4840E(config)#show alarm cpu

CPU status alarm : enable

CPU busy threshold(%) : 90

CPU unbusy threshold(%) : 85

CPU status : busy

» Quando a utilização da CPU retornar ao normal, será exibido da seguinte maneira:

02:47:05: Switch: %OAM-5-CPU_UNBUSY: cpu is not busy.

OLT4840E(config)#show alarm cpu

CPU status alarm : enable

CPU busy threshold(%) : 90

CPU unbusy threshold(%) : 85

CPU status : unbusy

33. Alarme de e-mail

33.1. Visão geral de alarme de e-mail

O OLT envia o log do sistema por e-mail para o endereço especificado.

33.2. Configuração do alarme

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o alarme via e-mail	**[no] mailalarm**	Obrigatório
Configuração do servidor smtp	**[no] mailalarm server** ip-address	Obrigatório
Configuração da indentidade smtp	**mailalarm smtp authentication** username name **passwd** password	Obrigatório
Configuração do e-mail remetente	**[no]mailalarm sender s**ender@exemplo.com.br	Obrigatório
Configuração do e-mail destinatário	**[no]mailalarm receiver** receiver@exemplo.com.br	Obrigatório
Configuração do e-mail cc	**[no]mailalarm ccaddr** ccaddr@exemplo.com.br	Opcional
Configuração do nível de log do alarme	**[no] mailalarm logging level** value	Opcional
Visualização das configurações	**show mailalarm**	Opcional

Obs.: » *O alarme de e-mail está desativado por padrão.*

» *O nível de log padrão é 0 e, quando configurado para 'n', os logs do nível 0 até 'n' são enviados para o email especificado pelo mailalarm.*

33.3. Exemplo de configuração do alarme de e-mail

» Descrição da rede:

Deixe o OLT enviar registros de nível 0-3 para receive@126.com. O remetente é teste/teste e caixa de correio é test@126.com, o servidor de email é 183.222.100.112.

» Passos de configuração:

» Configuração:

OLT4840E(config)#mailalarm

OLT4840E(config)#mailalarm server 183.222.100.112

OLT4840E(config)#mailalarm smtp authentication username test passwd test

OLT4840E(config)#mailalarm sender test@126.com

OLT4840E(config)#mailalarm receiver receive@126.com

OLT4840E(config)#mailalarm ccaddr cc@126.com

OLT4840E(config)#mailalarm logging level 3

» Exiba as informações:

OLT4840E(config)#show mailalarm

mailalarm state : on

smtp authentication : on

smtp server address : 11.1.1.1

mailalarm logging level : 3

sender e-mail address : test@126.com

receiver e-mail address : receive@126.com

ccaddr : cc@126.com

34. Log do sistema

34.1. Visão geral do log de sistema

O Syslog é o centro das informações do sistema, para completar o processamento unificado e a saída de informações.

Os outros módulos do sistema enviarão as informações de saída a ele. O Syslog determina o formato de saída das informações de acordo com a configuração do usuário e as emite para o dispositivo de exibição, de acordo com as regras de swtiching e filtragem de informações de cada saída configurada pelo usuário.

Com este sistema, você não precisa exportar informações para o console, terminal Telnet ou servidor de log, basta enviá-las para o Syslog. Ao configurar as regras de filtragem apropriadas, os consumidores de informações, que são console terminal, Telnet, buffer de histórico, log host e agente SNMP, podem escolher o que eles querem receber e descartar.

34.2. Configuração do sistema de log

Habilitar/desabilitar o Syslog

» Habilitar/desabilitar o Syslog:

Operação	Comando	Obrigatório/ opcional
Acessar o modo de configuração global	**configure terminal**	-
(des) Habilitar a função de log	**[no] logging**	Opcional
Visualizar informações de configuração	**show logging**	Opcional

Obs.: *por padrão, a função de log está habilitada e armazenada no buffer.*

Configuração do log número de série

» Configuração do log do número de série:

Operação	Comando	Obrigatório/ opcional
(des) Habilitar o número de série do log	**[no] loggin sequence-numbers**	Obrigatório

Obs.: *a função* Log *está habilitada por padrão.*

Configuração do timestamp

» Configuração do timestamp no Syslog:

Operação	Comando	Obrigatório/ opcional
Configuração do tipo de timestamp	**logging timestamps {** notime | uptime | datetime **}**	Opcional
Restaura a configuração padrão do timestamp	**no logging timestamps**	Opcional

Obs.: » *Não existe uma opção de timestamp separada (ativar / desativar). Existem três tipos de timestamp:*
- » ***notime:*** *não exibe a hora.*
- » ***uptime:*** *exibe o tempo de inicialização.*
- » ***datetime:*** *exibe a data e a hora.*
- » *O padrão é o* uptime.

Saída do terminal

No modo *Privilegiado*, configure o log para a saída no terminal do OLT. No modo *Global*, você pode configurar a exibição de informações e as regras de filtragem. Por padrão, os registros do dispositivo não são enviados para o terminal, mas saem para o buffer. Existe uma ligeira diferença entre o comando para o terminal serial e o terminal Telnet ou SSH.

» Saída para o terminal:

Operação	Comando	Obrigatório/ opcional
Modo de configuração privilegiado	**end**	Obrigatório
(Des)Habilitar a saída para o terminal	**[no] terminal monitor**	Opcional
Modo de configuração global	**configure terminal**	Obrigatório
Visualização do estado do log (habilitado / desabilitado)	**[no] logging monitor { all |** monitor-num **}**	Opcional
Configuração das regras dos filtros	**logging monitor { all |** monitor-num **} {** level-value **| none | level-list {** start-leve**l to** end-level **|** value **} } [module** module-name **]**	Opcional
Visualizar as regras dos filtros	**show logging filter** monitormonitor-num	Opcional
Remover regras dos filtros	**no logging monitor { all |** monitor-num **} filter**	Opcional

» **Saída de log para o terminal:** no console serial, a configuração padrão é terminal monitor habilitado; em outro console do terminal, o padrão é terminal monitor desabilitado.

» **Exibição de informações de registro:** na configuração do terminal não-console, somente afeta esse destino do terminal atual, os outros terminais, o próximo desembarque do terminal atual é inválido.

» monitor-num é 0 para o console e de 1 a 5 para terminais Telnet e SSH.

» **Regra padrão do log de saída:** todos os módulos, nível de log 0-5,7. A exclusão da regra de filtragem restaura a regra padrão.

Saída para o buffer

Operação	Comando	Obrigatório/ opcional
Modo de configuração global	**configure terminal**	-
(Des)Habilitar a saída para o buffer	**[no] terminal buffered**	Opcional
Configuração das regras dos filtros	**logging buffer {** level-value **| none	level-list {** start-level **to** end-level **|** value **} } [module** module-name **]**	Opcional
Visualizar as regras dos filtros	**show logging filter buffered**	Opcional
Remover regras dos filtros	**no logging buffered filter**	Opcional
Visualizar as informações de log no buffer	**show logging buffered [** level-value **| level-list {** start-level **to** end-level **| value }] [module** module-name **]**	Opcional

Obs.: *o padrão é saída de log para buffer. A regra padrão é exibir todos os módulos e logs no nível 0-6. A exclusão da regra de filtragem restaura a regra padrão.*

Saída para a flash

No modo *Global*, você pode configurar o Syslog para salvar na Flash, que não é salvo na memória flash por padrão.

Operação	Comando	Obrigatório/ opcional
Modo de configuração global	**configure terminal**	-
(Des)Habilitar a saída para o flash	**[no] logging flash**	Obrigatório
Configuração das regras dos filtros	**logging flash {** level-value **| none	level-list {** start-level **to** end-level **|** value **} } [module** module-name **]**	Opcional
Visualizar as regras dos filtros	**show logging filter flash**	Opcional
Remover regras dos filtros	**no logging flash filter**	Opcional
Visualizar as informações de log no buffer	**Show logging flash filter**	Opcional
Configuração do período de armazenamento	**[no] logging flash interval** value	Opcional

Operação	Comando	Obrigatório/ opcional
Configuração do tamanho do log para cada vez que é salvo	**[no] logg flash msg-number** value	Opcional
Verificar informações de log na flash	**show logging flash {** level-value **| none | level-list {** start-level **to** end-level **|** value **} }** **[module** module-name **]**	Opcional

Obs.: » *Quando o log é emitido para a flash, a regra padrão é enviar todos os módulos e o nível do log é 0-5. A exclusão da regra de filtragem restaura as regras padrão.*

» *Quando log sai para flash, o ciclo padrão é 30M. Por padrão, 100 logs são salvos ao mesmo tempo.*

Saída para servidor externo

Configuração do endereço do servidor especificado para saída de log, troca de informações de saída, regra de filtragem e ferramenta de registro e endereço de origem no modo *Global*.

Operação	Comando	Obrigatório/ opcional
Modo de configuração global	**configure terminal**	-
Configuração de servidor de log	**[no] logging** ip-address	Obrigatório
(Des)Habilitar o servidor de log	**[no] logging host { all |** ip-address **}**	Obrigatório
Configuração das regras dos filtros	**logging host { all |** ip-address **}{** level-value **| none | level-list {** start-level **to** end-level **|** value **} } [module** module-name **]**	Opcional
Restaurar as regras dos filtros	**no logging host { all | ip-address } filter**	Opcional
Configuração do nome da ferramenta de log	**[no] logging facility { clock1 | clock2 | ftp | kernel | Optional lineprinter | localuse0 | localuse1 | localuse2 | localuse3 | localuse4 | localuse5 | localuse6 | localuse6 | localuse7 | logalert | logaudit | mail | networkknews | ntp | security1 | security2 | syslogd | system | userlevel | uucp }**	Opcional

Configuração do sip para os pacotes de log	**[no] logging source {** ip-address **| loopback-interface** if-id **}**	Opcional

Obs.: » *O sip de mensagens de log deve ser a interface dispositivo. O dispositivo usa o endereço IP da interface correspondente do servidor de log por padrão.*

» *O nome da ferramenta de log padrão usa localeuse7.*

Saída para o agente SNMP

Configure a saída Syslog para o agente SNMP no modo *Global*. Para enviar mensagens de Syslog para estação de trabalho SNMP em mensagens de trap, você também deve configurar o endereço do host trap. Consulte as instruções de configuração SNMP.

Por padrão, esta função não está habilitada.

» Saída do Syslog para o agente SNMP:

Operação	Comando	Obrigatório/ opcional
(Des)Habilitar a saída para o terminal	**[no] loggin snmp-agent**	Obrigatório
Visualização do estado do log (habilitado / desabilitado)	**[no] logging monitor { all |** monitor-num **}**	Opcional
Configuração das regras dos filtros	**logging snmp-agent {** level-value **| none | level-list {** start-level **to** end-level **|** value **} } [module** module-name **]**	Opcional
Visualizar as regras dos filtros	**show logging filter snmp-agent**	Opcional
Remover regras dos filtros	**no logging snmp-agent filter**	Opcional

Saída de log para o agente snmp, a regra padrão: saída de todos os módulos, o nível de log é 0-5.

Depuração

No modo *Global*, você pode configurar a função de depuração para imprimir as informações de depuração do módulo correspondente. Por padrão, as informações de depuração de todos os módulos estão desabilitadas.

» Configuração da depuração (debug):

Operação	Comando	Obrigatório/ opcional
(Des)Habilitar função de debug	**[no] debug { all |** module-name **}**	Obrigatório

Visualização as informações de configuração	**show debug**	Opcional

Exemplo de configuração de Syslog

» Requisitos de rede:

Exiba a saída dos logs do módulo STP e do módulo do dispositivo nos níveis 0-4 no terminal de console; ligar a exibição do número de série; timestamp como datetime; o log é exibido para a memória flash; as informações de registro dos níveis 3 e 4 são emitidas para buffer; logs de saída para o servidor externo: 192.168.1.3; abrir informações de depuração do ARP.

» Passos de configuração:

» Habilite a função de saída para o terminal:
OLT4840E#terminal monitor

OLT4840E#configure terminal

» Habilite a função de log:
OLT4840E(config)#logging

» Habilite a visualização do terminal:
OLT4840E(config)#logging monitor all

» Saída dos logs do módulo STP e do módulo do dispositivo nos níveis 0-4 para o terminal de console:
OLT4840E(config)#logging monitor all level-list 0 to 4 module stp device

» Habilite a visualização do número serial:
OLT4840E(config)#logging sequence-numbers

» Configure o timestamp como datetime:
OLT4840E(config)#logging timestamps datetime

» Habilite a saída do log para a flash:
OLT4840E(config)#logging flash

» Configure a regra de filtragem do registro de buffer:
OLT4840E(config)#logging buffered level-list 3 4

» Configure servidor de log:
OLT4840E(config)#logging 192.168.1.3

» Habilitar o servidor de log:
OLT4840E(config)#logging host 192.168.1.3

» Configure o FTP:
OLT4840E(config)#logging facility ftp

» Habilite a função de depuração do módulo ARP:
OLT4840E(config)#debug ARP

» Ver as informações de configuração:
OLT4840E(config)#show logging

state: on;

logging sequence-numbers: on;

logging timestamps: datetime;

logging language: english

logging monitor:

Console: state: on; display: off; 96 logged; 0 lost; 0 overflow.

Logging buffered: state: on; 249 logged; 0 lost; 0 overflow.

Logging flash: state: on; 37 logged; 0 lost; 0 overflow.

Logging loghost:

logging facility: ftp;logging source: off

192.168.1.3: state: on; 23 logged; 0 lost; 0 overflow.

Logging SNMP Agent: state: off; 0 logged; 0 lost; 0 overflow.

35. Manutenção do sistema

35.1. Visualização do status do sistema

Esta seção descreve alguns dos dos comandos *show* para o sistema.

Operação	Comando	Obrigatório/ opcional
Visualização da versão do sistema	**show version**	Opcional
Visualização das informações do sistema	**show system**	Opcional
Visualização das informações de memória	**show memory**	Opcional

Operação	Comando	Obrigatório/ opcional
Visualização da utilização de CPU	**show cpu-utilization**	Opcional
Visualização das estatísticas de pacotes da CPU	**show cpu-statistics** {ethernet | pon} port-number	Opcional, de acordo com a estatística da porta
Visualização das estatísticas de tipos de pacotes da CPU	**show cpu-classification** interface {ethernet | pon} port-number	Opcional
Visualização das informações do administrador que logaram ao sistema	**show users**	Opcional
Visualização do relógio do sistema	**show clock**	Opcional
Visualização de todas as tabelas fdb	**show ip fdb**	Opcional
Visualização da tabela fdb especificada por IP	**show ip fdb** ip	Opcional
Visualização das tabelas fdb especificadas por segmento de endereço	**show ip fdb** ipmask	Opcional

Obs.: *a tabela Fdb é uma tabela ARP que é emitida para o switch de três níveis, que é a tabela ARP de hardware.*

35.2. Configuração do nome do host do OLT

Execute o comando hostname e configure o prompt da interface da linha de comando do sistema no modo de configuração global.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração privilegiado	**enable**	-
Acesse o modo de configuração global	**configure terminal**	-
Configure o prompt da interface da linha de comando do sistema	**hostname** host-name	Opcional

Cancele o prompt da interface da linha de comando do sistema	**no hostname**	Opcional

35.3. Configuração do relógio do sistema

O dispositivo possui um relógio que pode ser calibrado por comandos. Defina o relógio do sistema utilizando o comando de ajuste do relógio no modo de usuário privilegiado.

Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração privilegiado	**enable**	-
Configure o relógio	**clock set** HH:MM:SSYYYY/MM/DD	Obrigatório
Acesse o modo de configuração global	**configure terminal**	-
Configure o fuso horario	**clock timezone** name hour minute	Opcional
Visualização do relógio do dispositivo	**show clock**	Opcional

» Exemplo de configuração:

» Configure o relógio do dispositivo:
OLT4840E#clock set 13:12:33 2014/08/10

Set clock successfully.

» Configure o fuso horário como o de Brasilia:
OLT4840E(config)#clock timezone Brasilia -3

Set timezone successfully.

» Exiba o relógio do dispositivo:
OLT4840E(config)#show clock

Sun 2014/08/10 13:19:15 Brasilia 03:00

35.4. Comando de teste de rede

O ping é usado para verificar se a conexão de rede e o host são acessíveis. Operar as seguintes configurações em modo de usuário privilegiado ou modo de usuário normal.

» Comando de ping para teste:

Operação	Comando	Obrigatório/ opcional
Execute o comando ping	**ping {- i** ttl|**-l** packetlength|-**n** count |**-s** sourceip | -**t** timeout} **host**	Opcional
Execute o comando ping6	**ping6 {-a** ipv6 source-address **|-c** count **|-h** hop_limit **| -s** packetlength **|-t |-w** time_out**}**	Opcional

Descrição dos parâmetros de ping IPv4

» **- i ttl:** TTL valor enviado.
» **-l packetlength:** tamanho do pacote enviado em bytes.
» **-n count:** número de pacotes enviados.
» **-s sourceip:** endereço de IP da origem dos pacotes enviados.
» **-t timeout:** tempo de timeout após envio de um pacote, em segundos.

Descrição dos parâmetros de ping IPv4

» **-a source address:** endereço IP de origem dos envios.
» **-c count:** número de pacotes enviados.
» **-h hop limit:** limite de hop.
» **-s packet length:** tamanho do pacote enviado em bytes.
» **-w time out:** tempo de timeout após envio de um pacote, em segundos.

35.5. Comando de rastreamento de rota

Tracert é usado principalmente para rastreamento de rotas e verificação de conexões de rede. Operar as seguintes configurações em modo de usuário privilegiado ou modo de usuário normal.

» Comando de rastreamento de rota:

Operação	Comando	Obrigatório/ opcional

Execute o rastreio de rota IPv4	**tracert { -u | -c } { -p** udpport **| -f** first_ttl **| -h** maximum_hops **| -w** time_out } target_name	Opcional
Execute o rastreio de rota IPv46	**tracert6** { -c |-**h** maximum_hops| -**w** time_out }**ipv6_host_address**	Opcional

Descrição de parâmetros

- **-u:** envio de pacotes.
- **-c:** envio de pacotes icmp echo (padrão).
- **udpport:** endereço da porta de destino para enviar pacotes udp. Ele varia de 1 a 65535, a porta padrão é *62929*.
- **first_ttl:** valor inicial TTL dos pacotes enviados, no intervalo de 1 a 255. O padrão é *1*.
- **maximum_hops:** valor máximo TTL dos pacotes enviados, no intervalo de 1 a 255. O padrão é *30*.
- **Time_out:** o tempo limite de timout após o envio do pacote, no intervalo de 10 a 60, em segundos. O valor padrão é *10 segundos*.
- **target_name:** endereço de host ou roteador de destino.

35.6. Banner

Depois de configurar o banner, as informações do fabricante aparecerão quando o dispositivo estiver conectado.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilite o banner	**banner**	Opcional
Desabilite o banner	**no banner**	Opcional
Personalize a primeira linha do banner	**banner line1** string	Opcional
Personalize a segunda linha do banner	**banner line2** string	Opcional

Operação	Comando	Obrigatório/ opcional
Personalize a terceira linha do banner	**banner line3** string	Opcional
Personalize a quarta linha do banner	**banner line4** string	Opcional

O dispositivo possui um banner padrão, mas a função de banner é desativada por padrão.

Exemplo:

» Ative a função de banner, faça o login novamente depois de sair, exibirá o banner.

```
OLT4840E(config)#banner
witch(config)#exit
OLT4840E#quit
Username:admin
Password:*****
**********************************************************************
* It's XX owner of this equipment, please remember for legal
* liability.
**********************************************************************
```

35.7. O número de linhas exibidas ao visualizar informações

Você pode exibir até 25 linhas de informações ao mesmo tempo (por padrão) quando visualiza informações do dispositivo.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configure as informações que serão exibidas	**screen-rows per-page** inter	Opcional

O intervalo por página é de 0 a 256 e 0 significa que todas as informações são exibidas. Não há limite; a configuração por página como 0 pode coletar informações de forma eficiente.

35.8. Reiniciar o OLT

Comando para reiniciar o OLT imediatamente

Você pode usar os seguintes comandos para reiniciar o OLT imediatamente.

Operação	Comando	Obrigatório/ opcional
Reinicie o OLT imediatamente	**reboot**	Opcional, executar o comando no modo *Privilegiado*

Comando para reiniciar o OLT periodicamente

O dispositivo permite que o cliente configure o tempo para reinicialização.

Operação	Comando	Obrigatório/ opcional
Reiniciar o OLT periodicamente	**auto-reboot { in** { minutes min | hours hour} **| at**{ YYYY/MM/DD hh:mm:ss **|** hh:mm:ss daily | hh:mm:ss weekday weekly } }	Opcional, executar o comando no modo *Global*
Cancelar o reinício periodico	**no auto-reboot**	Opcional

Visualização do tempo para reinício	**show auto-reboot**	Opcional

Obs.: *no modo de reinicialização automática, configure o relógio do sistema para ser usado em conjunto.*

» Exemplo de configuração:

» Configure o OLT para reiniciar em 3 minutos:
OLT4840E(config)#auto-reboot in hours 0 minutes 3

Enable auto-reboot successfully.

» Exiba o tempo para reinício do OLT:
OLT4840E(config)#show auto-reboot

Auto-reboot setting

Type: one-off/in

Time: 2014-01-02 00:47:35

Auto-reboot in 0 hours, 2 minutes and 24 seconds. // The configuration starts with a

Countdown

» Reinício do OLT:
OLT4840E(config)#

It's time to reload, ready to reboot.....

0

Count down to auto-boot...

0

boot default application from flash.....

Loading image...OK

Unarj image...OK

36. Configuração de sFlow

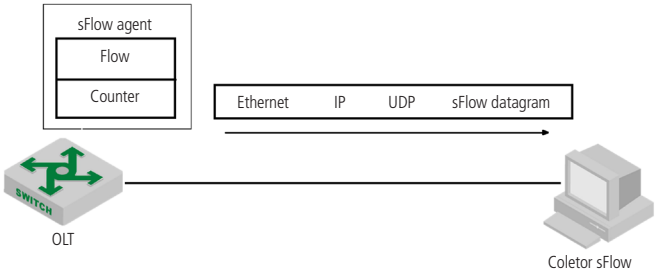
36.1. Introdução ao sFlow

sFlow é uma tecnologia de monitoramento de tráfego de rede baseada na amostragem de pacotes, que é usada principalmente para análise estatística do tráfego de rede.

Conforme exibido na figura, o sistema sFlow consiste no agente incorporado no dispositivo e no coletor remoto. O agente sFlow obtém as estatísticas e informações de pacotes da interface através do mecanismo de amostragem, então encapsula a informação em pacotes sFlow. Quando o buffer de pacote sFlow está cheio ou o tempo de envio de pacote sFlow (o intervalo de tempo é fixo para 1 segundo) expira, o pacote é encapsulado no pacote UDP e enviado ao coletor especificado. O coletor sFlow analisa o pacote e exibe o resultado da análise. Um colector sFlow pode monitorar vários agentes.

O sFlow utiliza os dois mecanismos de amostragem a seguir:

- **Amostragem de fluxo:** a amostragem de fluxo baseada em pacotes é usada para obter informações sobre o conteúdo do pacote.
- **Amostragem de contadores:** a amostragem de estatísticas da interface baseada em tempo é usada para obter as estatísticas da interface.



36.2. Configuração de sFlow

Configuração do IP do agente sFlow

O endereço IP do agente sFlow é o endereço IP de origem que o OLT se comunica com o coletor remoto. O endereço IP deve ser o endereço do próprio OLT. Você pode configurar apenas um endereço IP para o agente sFlow no dispositivo. O IP recém-

configurado substitui a configuração existente.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do IP do agente sFlow	**sflow agent ip**A.B.C.D	Obrigatório
Remover o IP do agente sFlow	**no sflow agent ip**	Opcional

Por exemplo:

» Configure o endereço IP do agente do sFlow para 1.1.1.1.
OLT4840E(config)#sflow agent ip 1.1.1.1

Configuração do coletor sFlow

O coletor sFlow é usado para monitorar o tráfego do dispositivo. O OLT deve ser configurado com o IP e o número da porta do coletor sFlow.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do IP e a porta do sFlow collector	**sflow collector id ip** ip-address **[port** port-number**]**	Obrigatório
Remover o sFlow collector	**no sflow agent ip**	Opcional

Descrição dos parâmetros

» **ID:** número do coletor (no intervalo de 1-10).
» **IP-address:** o endereço IP do coletor.
» **port-number:** a porta onde o coletor escuta os pacotes sFlow (*6343* por padrão).

Por exemplo:

» Configure o coletor com o número 2, endereço IP 1.1.1.2 e número da porta 6345:
OLT4840E(config)#sflow collector 2 ip 1.1.1.2 port 6345

Configuração da taxa de amostragem do sFlow

Esse comando é usado para configurar a taxa de amostragem de pacotes para a amostragem de fluxo. A Amostragem de Fluxo usa o modo de amostragem aleatória.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de porta	**interface ethernet** interface-num	-
Configure a taxa de amostragem do pacote de Fluxo	**sflow sampling-rate** rate	Obrigatório
Remover a amostragem do pacote de Fluxo	**no sflow sampling-rate**	Opcional

Por exemplo:

» Configure a taxa de amostragem do fluxo da porta 2 para ser em 3000 pacotes:
OLT4840E(config-if-ethernet-0/2)#sflow sampling-rate 3000

Configuração do max-reader do sFlow

Esse comando é usado para configurar o número máximo de bytes que podem ser copiados do cabeçalho do pacote original quando a amostragem Flow copiar o conteúdo do pacote. Por padrão, o número máximo de bytes que podem ser copiados é de 128 bytes.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de porta	**interface ethernet** interface-num	-
Configuração do comprimento da cópia de conteúdo dos pacotes Fluxo	**sflow flow max-header** length	Obrigatório
Restaurar o padrão	**no sflow flowmax-header**	Opcional

Descrição dos parâmetros

» **length:** número máximo de bytes permitidos a serem copiados (no intervalo 18-512).

Por exemplo:

» Configure o número máximo de bytes que podem ser copiados para 200 para

amostragem de fluxo na porta 2:

OLT4840E(config-if-ethernet-0/2)#sflow flow max-header 200

Configuração do sFlow collector

A amostragem de fluxo e o coletor sFlow são vinculados pelo número do coletor:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de porta	**interface ethernet** interface-num	-
Configuração	**sflow flow collector** id	Obrigatório
Restaurar o padrão	**no sflow flow collector**	Opcional

Configuração do intervalo de contagem do sFlow

O OLT também pode ser amostrado em intervalos regulares.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de porta	**interface ethernet** interface-num	-
Configuração do contador de intervalo de amostragem	**sflow counter interval time**	Obrigatório
Restaurar o padrão	**no sflow counter interval**	Opcional

Configuração do coletor de contador do sFlow

Este comando é usado para configurar o número do coletor da amostragem do contador. O argumento "no" deste comando cancela essa configuração.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de porta	**interface ethernet** interface-num	-

Configuração do número do contador de amostragem	**sflow counter collector** id	Obrigatório
Remover o número do contador de amostragem	**no sflow counter collector**	Opcional

Por exemplo:

» Defina o número do coletor da amostragem do contador de portas para 1:
OLT4840E(config-if-ethernet-0/2)#sflow counter collector 1

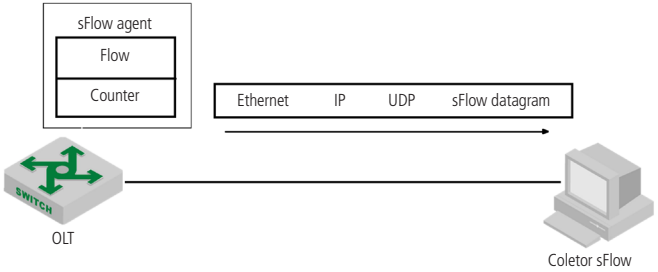
O comando para visualização do sFlow

Este comando é usado para exibir a configuração do sFlow.

Operação	Comando	Obrigatório/ opcional
Em qualquer modo	**show sflow**	Opcional

36.3. Exemplo

IP do dispositivo = 192.168.2.1; PC como cletor sFlow, IP =192.168.2.100



» Configure o IP do dispositivo:
OLT4840E(config)#interface vlan-interface 2
Create vlan-interface successfully!
OLT4840E(config-if-vlanInterface-2)#ip address 192.168.2.1 255.255.255.0
This ipaddress will be the primary ipaddress of this interface.
Config ipaddress successfully

» Definir o IP do agente sFlow:

OLT4840E(config)#sflow agent ip 192.168.2.1

» Configure IP do sFlow collector
OLT4840E(config)#sflow collector 1 ip 192.168.2.100 port 6000

Configuração da porta

OLT4840E(config-if-ethernet-0/3)#sflow counter collector 1

37. Configuração de CFM

37.1. Introdução ao CFM

O CFM (Connectivity Fault Management Protocol), definido pelo padrão IEEE 802.1ag, é um mecanismo OAM de lado a lado baseado em VLAN no link Layer 2 para gerenciamento de falhas na Ethernet.

Conceito de CFM

Conceito	Descrição
Domínio de manutenção	O domínio de manutenção indica a rede coberta pela detecção de falha de conectividade, cujos limites são definidos por uma série de pontos finais de manutenção configurados na porta. O domínio de manutenção é identificado pelo nome do domínio. De acordo com o planejamento da rede, o domínio de manutenção pode ser classificado em oito níveis. Diferentes domínios de manutenção podem ser adjacentes uns aos outros ou alinhados, mas não podem ser cruzados. O assentamento só pode ser realizado no domínio de manutenção de alto nível para domínio de manutenção de baixo nível. Ou seja, um domínio de manutenção de baixo nível deve ser incluído em um domínio de alto nível.

Conceito	Descrição
Associação de manutenção	Você pode configurar múltiplas associações de manutenção, conforme exigido no domínio. Cada associação de manutenção é uma coleção de pontos no domínio. A associação de manutenção é identificada pelo "Nome de Domínio + Nome da Associação". A associação de manutenção serve uma VLAN. Os pacotes enviados pelo ponto de manutenção na associação são marcados com a VLAN. O ponto de manutenção na associação de pode receber os pacotes enviados de outros pontos na associação.
Ponto de manuntenção	O ponto de manutenção está configurado em uma porta e pertence a uma associação. Podem ser classificado em dois tipos: pontos finais de manutenção e pontos intermediários de manutenção. Um ponto final é identificado por um ID MEP, que determina o escopo e os limites do domínio. Os pontos finais são direcionais e são classificados em UP MEP e DOWN MEP. A direção do ponto final indica a localização do domínio de manutenção em relação à porta. O DOWN MEP envia um pacote para a porta em que ele reside. Em vez de enviar um pacote para a sua porta, o UP MEP envia um pacote para a outra porta do dispositivo. O ponto intermediário de manutenção está localizado dentro do domínio, não pode enviar pacotes de protocolo CFM ativamente, mas pode processar e responder a pacotes de protocolo CFM.

Funções principais do CFM

A aplicação eficaz da detecção de falhas de conectividade baseia-se na implantação e configuração de rede razoável. Sua função é implementada entre os pontos de manutenção configurados. As principais funções são as seguintes:

Função	Descrição
Deteção de continuidade	É uma função *OAM* ativa usada para detectar a conectividade entre os pontos finais da manutenção. A falha na conexão pode ser causada por uma falha do dispositivo ou por um erro de configuração.
Função de loopback	É uma função *OAM* sob demanda usada para verificar o status da conexão entre o dispositivo local e o dispositivo remoto.

Função de rastreamento de links	É uma função *OAM* sob demanda que determina o caminho entre o dispositivo local e o dispositivo remoto para localizar a falha do link.

Configuração do CFM

Antes de configurar a função *CFM*, faça o seguinte planejamento para a rede:

- » O domínio de manutenção de toda a rede é classificado para determinar os limites dos domínios em cada nível.
- » Identifique os nomes dos vários domínios de manutenção. Os nomes do mesmo domínio de são os mesmos em diferentes dispositivos.
- » Determine a associação de manutenção em cada domínio de acordo com a VLAN a ser monitorada.
- » Determine o nome de cada associação de manutenção. A mesma associação de no mesmo domínio de tem o mesmo nome em dispositivos diferentes.
- » Determine a lista de pontos finais de manutenção para a mesma associação no mesmo domínio, que deve ser o mesmo em dispositivos diferentes.
- » Os pontos finais de manutenção podem ser planejados nas portas de fronteira do domínio de e da associação. Os pontos intermediários de manutenção podem ser planejados nos dispositivos ou portas não da borda.

Depois de concluir o planejamento da rede, execute a seguinte configuração.

37.2. Configuração de CFM

Configuração do MD

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Crie um domínio de manutenção e acesse o modo de configuração do domínio de manutenção	**cfm md** md-index	Obrigatório

Configuração do nome do nível do domínio de manutenção

Para distinguir os vários domínios de manutenção, você pode especificar diferentes nomes para cada domínio de manutenção. O nome de domínio consiste em duas partes: formato de nome e conteúdo de nome. É preferencial que o nome de domínio seja exclusivo em toda a rede. Para indicar relacionamentos aninhados entre

domínios de manutenção, você também deve especificar o nível de domínio de manutenção. Somente um domínio de manutenção com um alto nível pode aninhar um domínio de manutenção com um pequeno nível.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm md** md-index	Quando o domínio não existe, ele é criado
Remover o MD	**no cfm md** md-index	Opcional
Configuração do domínio de manutenção sem nome e especificação do nível do domínio de manutenção	**cfm md format** none **level** md-level	Obrigatório
Configuração do nome do domínio de manutenção e especificação do nome e do nível do domínio de manutenção	**cfm md format** { dns-name | mac-uint | string } **name**md-name **level** md-level	Obrigatório

Configuração da associação de manutenção

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Crie uma associação de manutenção e entre no modo de configuração da associação de manutenção	**cfm md** md-index	Obrigatório
Excluir a configuração da associação de manutenção	**no cfm md** md-index	Opcional

Configuração do nome da associação de manutenção e a VLAN associada

Para distinguir a associação de manutenção em cada domínio, você pode especificar nomes de instâncias diferentes para cada associação. O nome da instância consiste em duas partes: formato de nome e conteúdo de nome. O nome do domínio e o nome da instância do domínio de manutenção onde a associação está localizada devem ser exclusivos de toda a rede.

» Configuração do nome da associação de manutenção e a VLAN associada:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Configure o nome do MA e da VLAN primária	**cfm ma format** { primary-vid | string | uint16 | vpn-id } **name** ma-name **primary-vlan** vlan-id	Obrigatório

Configuração do MEP

A função *CFM* é usada principalmente para várias operações nos pontos finais de manutenção. Você pode configurar os pontos finais nas portas da borda da rede de acordo com o planejamento da rede.

» Configuração do MEP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Criar uma MEP e especificar a sua porta associada	**cfm mep** mep-id **direction** { up | down } [**primary-vlan** vlan-id] **interfaceethernet** port-id	Obrigatório
Habilitar o estado de gerenciamento do MEP	**cfm mep** mep-id **state** enable	Obrigatório, por padrão está desligado
Fechar o estado de gerenciamento do MEP	**cfm mep** mep-id **state** disable	-
Configuração da prioridade que o MEP envia para CCM e LTM	**cfm mep** mep-id **priority** priority-id	Opcional, por padrão a prioridade é *0*

Configuração do MEP remoto

O MEP remoto é relativo ao MEP local. Em toda a associação de manutenção, todos os MEPs diferentes dos MEPs do local devem ser configurados como MEPs remotos no local.

» Configure o MEP remoto:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-

Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Criar o MEP remoto e especificar o MEP local relativo	**cfm rmep** rmep-id **mep** mep-id	Obrigatório

Configuração do MIP

Os MIPs são usados para responder a vários pacotes de teste CFM. Você pode configurar os MIPs em dispositivos ou portas que não sejam de borda com base no planejamento de rede.

» Configurar o MIP:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Criar um ponto intermediário de manutenção e especificar sua porta associada	**cfm mip** mip-id **interface ethernet** port-id	Opcional

Configuração da função de verificação de continuidade

Ao configurar a função de verificação de continuidade, você pode habilitar os MEPs para enviar pacotes CCM entre eles para detectar a conectividade entre esses MEPs e assim gerenciar a conectividade do link.

» Configuração da função de verificação de continuidade:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-

Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Configuração do intervalo no qual CCMs são enviados pelo MEP	**cfm cc interval** { 1 | 10 | 60 | 600 }	Opcional, *1s* por padrão
Habilitar a função de envio ccm no MEP	**cfm mep** mep-id **cc** enable	Obrigatório, por padrão, está desligado
Cancelar a função de envio ccm no MEP	**cfm mep** mep-id **cc** disable	Opcional

Obs.: *o intervalo de tempo para o envio de CCMs deve ser o mesmo nos pontos finais de manutenção no mesmo domínio e na associação em diferentes dispositivos.*

Configuração da função de loopback

Ao configurar a função de loopback, você pode verificar o status do link entre os MEPs de origem e de destino ou os MIPs para verificar a conectividade do link.

» Configurar a função *Loopback*:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Habilitar a função de loopback	**cfm loopback mep** mep-id { **dst-mac** mac-address | **dst-mep** rmep-id } [**priority** pri-id | **count** pkt-num | **length** data-len | **data** pkt-data]	Opcional

Configuração da função de rastreamento de links

Ao configurar a função de rastreamento de links, você pode localizar o caminho entre os MEPs de origem e de destino ou os MIPs e localizar as falhas do link.

» Configuração da função de rastreamento de links:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Habilitar o rastreamento de link	**cfm linktrace mep** mep-id { **dst-mac** mac-address | **dst-mep** rmep-id } [**timeout** pkt-time | **ttl** pkt-ttl | **flag** { use-mpdb | unuse-mpdb }]	Opcional

Função de medição de atraso de quadro Y.1731

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração do domínio de manutenção	**cfm ma** ma-index	-
Acesse o modo de configuração da associação de manutenção	**cfm md** md-index	-
Executar a medição de atraso de quadros	**cfm eth-2dm mep** mep-id **{ dst-mac** mac-address **| dst-mep** rmep-id **} [timeout** pkt-time **| priority** priority-identifier **| interval** second**|count** packet-num**]**	Opcional

Visualização e manutenção do CFM

Depois de completar a configuração acima, você pode usar os seguintes comandos para exibir a configuração CFM.

» Visualização e manutenção do CFM:

Operação	Comando	Obrigatório/ opcional
Limpar as estatísticas de CCM	**clear cfm cc**	Opcional, modo de configuração global
Limpar as informações do banco de dados do CCM	**clear cfm cc database**	
Visualização das informações do domínio de manutenção	**show cfm md [** md-index **]**	Opcional, pode ser executado em qualquer modo
Visualização das informações de associação de manutenção	**show cfm ma**	
Visualização das informações de pontos de manuntenção local	**show cfm mp local**	
Visualização das informações do ponto de manutenção remota	**show cfm mp remote**	
Visualização das estatísticas de CCM	**show cfm cc**	
Visualização das informações de banco de dados	**show cfm cc database**	
Visualização das informações de alarme CFM	**show cfm errors**	

37.3. Exemplo de configuração

OLT4840E(config)#cfm md 1 // Crie um domínio de mautenção

OLT4840E(config-cfm-md-1)#cfm md format none level 1 // Digite o modo de configuração do domínio de manutenção, configure um domínio sem nome e o nível de domínio é 1.

OLT4840E(config)#cfm md 1 // Acesse o modo de configuração do domínio de manutenção

OLT4840E(config-cfm-md-1)#cfm ma 1 // Digite o modo de configuração da associação de manutenção e defina o nome da associação de manutenção como 1

OLT4840E(config-cfm-md-1-ma-1)#cfm ma format primary-vid name 1 primary-vlan 2 // A VLAN associada é a 2

OLT4840E(config-cfm-md-1-ma-1)#cfm mep 1 direction up primary-vlan 2 interface ethernet 0/2 // Crie o MEP 1 e especifique a porta associada como VLAN 2

OLT4840E(config-cfm-md-1-ma-1)#cfm mep 1 state enable

OLT4840E(config-cfm-md-1-ma-1)#cfm mep 1 priority 1 // Defina a prioridade de enviar CCMs e LTMs para 1 pelo MEP

38. Configuração de EFM

38.1. Introdução ao EFM

O EFM (Ethernet of First Mile), conhecido como Ethernet de primeira milha, é definido pelo padrão IEEE 802.3ah para gerenciamento e manutenção de ligações Ethernet ponto a ponto entre dois dispositivos.

Função principal do EFM

O EFM pode efetivamente melhorar o gerenciamento e a manutenção da capacidade de Ethernet para garantir o funcionamento estável da rede, suas principais funções incluem:

» Função principal do EFM:

Função	Descrição
Função de auto-descoberta EFM	A função *EFM* é estabelecida com base na conexão EFM. O processo de estabelecimento de conexão é realizado pela função de descoberta automática. Entre as entidades conectadas, as informações sobre a configuração e a capacidade suportada pelo EFM local são notificadas através das informações OAMPDUs. Depois que a entidade recebe os parâmetros de configuração do lado oposto, determina se deve estabelecer a conexão EFM. Existem dois modos *EFM*: modo *Ativo* e modo *Passivo*. Uma conexão só pode ser iniciada por uma entidade no modo *Ativo*. Uma entidade no modo *Passivo* só pode aguardar uma solicitação de conexão de uma entidade oposta. As conexões EFM não podem ser estabelecidas entre duas entidades no modo *Passivo*.

Função	Descrição
Função de indição de falha remota	Quando o dispositivo detecta um evento de link de emergência, a entidade EFM defeituosa relata as informações de falha (ou seja, o tipo de evento de link de emergência) para a entidade remota através do campo Flag na Informação OAMPDU. Desta forma, o administrador pode aprender dinamicamente o status do link, observando as informações do registro e processando os erros correspondentes no tempo. Os tipos de evento de link de emergência incluem Link Fault, Dying Gasp e Critical Event.
Função de monitoramento de link	A função de monitoramento de links é usada para detectar e descobrir as falhas da camada de link em vários ambientes. O EFM monitora os links trocando o Notificação de Evento OAMPDUs: Quando uma entidade EFM detecta um evento geral, envia uma OAMPDU de notificação, os administradores podem monitorar o status da rede de forma dinâmica, observando as informações do registro. Os tipos de evento geral incluem errored-symbol-period, errored-frame, errored-frame-period e errored-frame-seconds.
Loopback remoto	O loopback remoto significa que uma entidade EFM no modo *Ativo* envia todos os pacotes, exceto as OAMPDUs para o lado remoto. Depois de receber o pacote, o dispositivo remoto não encaminha de acordo com seu endereço de destino. Em vez disso, ele envia o pacote de volta ao local. A função de loopback remoto controla o lado remoto para executar a função de loopback ou cancelar a operação através do controle de loopback OAMPDU. Esta função pode ser usada para detectar a qualidade do link e localizar a falha do link.
Aquisição de variáveis de MIB remota	A entidade EFM pode obter o valor da variável MIB da entidade remota trocando o OAMPDU de Solicitação de Variável / Resposta. As variáveis MIB contêm todos os parâmetros de desempenho e estatísticas de erro no link Ethernet. Ele fornece à entidade EFM local um mecanismo de detecção comum para o desempenho e o erro da entidade remota.

Descrição:

A porta habilitada para EFM é chamada de entidade EFM.

Pacote de protocolo EFM

A EFM trabalha na camada de enlace de dados e seu pacote de protocolo é chamado OAMPDU (OAM Protocol Data Units). A EFM relata o status do link periodicamente trocando OAMPDUs entre dispositivos para que o administrador possa gerenciar a rede de forma eficaz.

Tipo de pacote	Efeito
Informação OAMPDU	Ele é usado para enviar as informações de status da entidade EFM (incluindo informações locais, informações remotas e informações personalizadas) para a entidade remota para manter a conexão EFM.
Notificação de evento OAMPDU	Geralmente, é usado para monitoramento de links e alarme de falhas no link que liga as entidades EFM locais e remotas.
Controle de loopback OAMPDU	É usado principalmente para controle de loopback remoto. Ele é usado para controlar o status de loopback EFM de um dispositivo remoto. Este pacote contém informações sobre como ativar ou desativar a função de loopback. A função de loopback remoto é habilitada ou desativada com base nessas informações.
Requisição/resposta de variável OAMPDU	Ele é usado para obter o valor da variável MIB do dispositivo remoto para monitorar o status remoto.

38.2. Configuração do EFM

Configuração básica de EFM

O EFM funciona no modo *Ativo* e no modo *Passivo*. Quando o EFM está habilitado, a porta Ethernet começa a usar o modo de trabalho padrão para estabelecer conexões EFM com suas portas opostas.

» Configuração básica de EFM:

Operação	Comando	Obrigatório/ opcional
Operação	**Comando**	**Obrigatório/ opcional**
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	Obrigatório
Iniciar o EFM	**efm**	Obrigatório, por padrão o EFM está desativado
Fechar o EFM	**no efm**	Opcional
Configuração do modo de trabalho do EFM	**efm mode { passive | active }**	Opcional, por padrão o EFM trabalha no modo *Ativo*

Configuração dos parâmetros de tempo do EFM

Depois que uma conexão EFM é estabelecida, as entidades em ambos os lados enviam informações OAMPDUs em intervalos de um determinado tempo para verificar se a conexão é normal. O intervalo é chamado de intervalo de envio de pacotes de handshake. Se uma entidade EFM não receber um OAMPDU de informações da entidade remota dentro do período de tempo de conexão, a conexão é considerada interrompida.

Ajustando o intervalo de envio de pacote de handshake da EFM e o tempo limite de conexão, você pode alterar a precisão de detecção da conexão. Configure o tempo limite para respostas de dispositivos remotos para pacotes de solicitação OAMPDU, se a resposta expirar, os pacotes de resposta recebidos são descartados.

» Configuração dos parâmetros de tempo do EFM:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	Apenas em portas ethernet
Definir o intervalo de envio de pacotes de handshake	**efm pdu-timeout** time	Opcional, o valor padrão é de *1s*
Definir o tempo de timeout para as conexões EFM	**efm link-timeout** time	Opcional, o valor padrão é de *5s*
Definir o tempo de resposta de timeout	**efm remote-response-timeout** time	Opcional, o valor padrão é de *2s*
Recuperar o tempo de resposta de timeout	**no efm remote-response-timeout**	Opcional, restaura o valor padrão

Obs.: *após a conclusão da conexão EFM, a entidade EFM local envelhece a conexão com a entidade EFM oposta e desativa a conexão EFM. Portanto, o tempo de espera da conexão deve ser maior do que o intervalo de envio do pacote de handshake (recomendado para ser 3 vezes ou mais). Caso contrário, a conexão EFM se tornará instável.*

Configuração da função de detecção de falha remota

» Configuração da função de detecção de falha remota:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função de detecção de falha remota	**efm remote-failure { link-fault | dying-gasp | critical-event }**	Opcional, por padrão está ativado
Desabilitar a função de detecção de falha remota	**no efm remote-failure { link-fault | dying-gasp | critical-event }**	Opcional

Configuração da função de monitoramento de link

» Configuração da função de monitoramento de link:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função de monitoramento de link	**efm link-monitor { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds }**y	Opcional, por padrão está ativado
Desabilitar a função de monitoramento de link	**no efm link-monitor { errored-symbol-period | errored-frame | errored-frame-period | errored-frame-seconds }**	Opcional
Configuração do intervalo de decção de evento de errored-symbol-period	**efm link-monitor errored-symbol-period window high** win-value1 **low** win-value2	Opcional
Configuração do limiar de decção de evento de errored-symbol-period	**efm link-monitor errored-symbol-period threshold high** th-value1 **low** th-value2	Opcional
Configuração do intervalo de decção de evento de errored-frame	**efm link-monitor errored-frame window** win-value	Opcional

Operação	Comando	Obrigatório/ opcional
Configuração do limiar de decção de evento de errored-frame	**efm link-monitor errored-frame threshold** th-value	Opcional
Configuração do intervalo de decção de evento de errored-frame-period	**efm link-monitor errored-frame-period window** win-value	Opcional
Configuração do limiar de decção de evento de errored-frame-period	**efm link-monitor errored-frame-period threshold** th-value	Opcional
Configuração do intervalo de decção de evento de errored-frame-second	**efm link-monitor errored-frame-second window** win-value	Opcional
Configuração do limiar de decção de evento de errored-frame-second	**efm link-monitor errored-frame-second threshold** th-value	Opcional

Descrição:

O período de detecção e o limite do evento de errored-symbol-period é um valor inteiro de 64 bits. Os valores dos parâmetros após alta e baixa representam os 32 bits superiores e os 32 bits inferiores deste valor, respectivamente, isto é, o valor inteiro = (alto * (2 ^ 32)) + baixo.

Habilitar o loopback remoto

Por padrão, a função de loopback remoto está desabilitada. apenas em dispositivos que oferecem suporte ao loopback remoto.

» Habilitar o loopback remoto:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Habilitar a função de loopback remoto	**efm remote-loopback**	-
Desabilitar a função de loopback remoto	**no efm remote-loopback**	-

Rejeitar solicitação de loopback remoto

Para evitar o problema de que os serviços normais sejam afetados pela função de loopback remoto, você pode usar a configuração para evitar que a porta local seja controlada pelo OAMPDU de Controle de Loopback do lado oposto, rejeitando assim a solicitação de loopback remoto iniciada pelo lado oposto.

» Rejeitar solicitação de loopback remoto:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Rejeitar o loopback remoto	**efm remote-loopbackignore**	Opcional, por padrão a solicitação de loopback remoto é negada
Processar o loopback remoto	**efm remote-loopbackprocess**	Opcional

Iniciar uma solicitação de loopback remoto

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Iniciar uma solicitação de loopback remoto	**efm remote-loopback start stop**	Opcional
Parar uma solicitação de loopback remoto	**efm remote-loopback stop**	Opcional

Descrição:

Somente quando a conexão EFM é estabelecida na porta e o modo de funcionamento está no modo *Ativo*, a solicitação de loopback remoto pode ser iniciada na porta.

Somente as portas locais e remotas no link full-duplex suportam loopback remoto.

Quando o loopback remoto está ativado, todo o tráfego de dados será interrompido. Quando a está desabilitada, as portas locais e remotas voltarão ao normal.

Os motivos para que a porta saia do loopback remoto incluem: use o comando no EFM para desativar a função *EFM*. Use o comando EFM remote-loopback stop para sair ou tempo limite de conexão EFM.

Habilitar a função de aquisição de variável de MIB remota

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Acesse o modo de configuração de porta	**interface ethernet** interface-num	-
Obter o valor da variável MIB da porta do dispositivo remoto	**show efm port** port-id-list **remote-mib { phyadminstate | autonegadminstate }**	Opcional
Obter o valor da variável MIB global do dispositivo remoto	**show efm remote-mib { fecability | fecmode }**	Opcional

Descrição:

Somente quando a conexão na porta é estabelecida, o modo de trabalho EFM está ativo e a porta remota suporta a função de aquisição de variável MIB remota, neste caso, a solicitação de aquisição pode ser iniciada na porta.

Atualmente somente a capacidade FEC, o modo *FEC*, o estado habilitado para a porta e o estado ativo de auto-negociação de porta podem ser consultados. Outras variáveis MIB podem ser complementadas de acordo com os requisitos.

Visualização e manutenção do EFM

Depois de completar a configuração acima, você pode usar o seguinte comando para exibir a configuração do EFM.

Operação	Comando	Obrigatório/ opcional
Visualizaçao do status de execução do protocolo EFM	**show efm status interface [** interface-name **]**	Opcional, executável em todos os modos
Visualização do resumo de informações do EFM	**show efm summary**	
Visualização das informações de descoberta	**show efm discovery interface** [interface-name]	
Visualização das estatisticas de pacotes do protocolo EFM	**show efm statistics interface** [interface-name]	
Limpar as estatisticas de pacotes do protocolo EFM	**clear efm statistics interface** [interface-name]	Opcional, modo de configuração global

Exemplo de configuração

OLT4840E(config)#i e 0/2

OLT4840E(config-if-ethernet-0/2)#efm //Inicie EFM

OLT4840E(config-if-ethernet-0/2)#efm mode passive //Defina o modo de trabalho do EFM como passivo

OLT4840E(config-if-ethernet-0/2)#efm pdu-timeout 1 //Defina o intervalo de envio de pacote de handshake EFM para 1s

OLT4840E(config-if-ethernet-0/2)#efm link-timeout 5 //O período de timeout de conexão é 5s

OLT4840E(config-if-ethernet-0/2)#efm remote-response-timeout 2 // O tempo de resposta de timeout é 2s

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-symbol-period // Habilitar a função de monitoramento de link

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame-period

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame-seconds

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-symbol-period window high 1 low 3

//Set the errored-symbol-period detection period to 1 to 3

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-symbol-period threshold high 1 low 3

// The detection threshold is from 1 to 3

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame window 20 // O período de detecção de errored-frame é 20

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame threshold 2 // O limitar de detecção é 2

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame-period window 2 // O período de detecção de errored-frame-oeriod é 2

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame-period threshold 2 // O limitar de detecção é 2

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame-seconds window 200 // Defina o intervalo de detecção de errored-frame-second para 200

OLT4840E(config-if-ethernet-0/2)#efm link-monitor errored-frame-seconds threshold 2

39. LLDP

39.1. Visão geral do LLDP

LLDP (*Link Layer Discovery Protocol*) é um protocolo de descoberta de camada 2 definido no IEEE 802.1AB. Através do uso da tecnologia LLDP, quando a escala da rede é expandida rapidamente, o sistema de gerenciamento de rede pode entender rapidamente as informações de topologia da rede Layer 2 e as informações de mudança de topologia.

O princípio básico do LLDP é o seguinte: um dispositivo em uma rede envia uma notificação de suas informações de status para seus dispositivos vizinhos e cada porta de cada dispositivo armazena suas próprias informações. Se um dispositivo local tiver uma mudança de estado, ele também pode enviar informações atualizadas para o dispositivo vizinho diretamente conectado a ele. O dispositivo vizinho armazena as informações na MIB SNMP padrão. O sistema de gerenciamento de rede pode informar a situação de conexão da segunda camada atual da MIB SNMP. Observe que LLDP é um protocolo remoto de descoberta de informações de estado de dispositivo. Não pode executar as funções de configuração do dispositivo de rede e controle de porta.

39.2. Configuração do LLDP

Habilitar/desabilitar o LLDP

Por padrão, o LLDP está desabilitado.

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Habilitar/desabilitar o LLDP	**[no] lldp**	Obrigatório

Configuração do modo de trabalho

Modo de trabalho LLDP:

- **TxRx:** envia e recebe pacotes LLDP, a porta funciona neste modo por padrão.
- **Tx:** somente envia pacotes LLDP, mas não recebe.
- **Rx:** somente recebe pacotes LLDP, mas não envia.
- **Desativado:** os pacotes LLDP não são enviados nem recebidos.

Quando o modo de trabalho LLDP de uma porta muda, a porta inicializa a máquina de estado do protocolo.

Mecanismo de envio

Quando a porta funciona no modo *TxRx* ou *Tx*, o dispositivo envia periodicamente pacotes LLDP para o vizinho. Se a configuração local do dispositivo mudar, os pacotes LLDP são enviados imediatamente para notificar os dispositivos vizinhos das alterações nas informações locais. No entanto, para evitar que uma grande quantidade de pacotes LLDP sejam enviados devido a mudanças frequentes de informações locais, depois de enviar um pacote LLDP, ele deve atrasar por um período de tempo antes do próximo envio.

Mecanismo de recepção

Quando a porta funciona no modo *TxRx* ou *Rx*, o dispositivo verifica a validade dos pacotes LLDP recebidos e TLVs transportados nos pacotes. Após a verificação, as informações do vizinho são salvas no dispositivo local e o tempo de envelhecimento das informações do vizinho no dispositivo local é definido de acordo com o valor TTL (*Time To Live*) no TLV. Se o valor for zero, a informação do vizinho é envelhecida imediatamente.

- Configuração do modo de trabalho:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-num	-
Configuração do modo de trabalho	**lldp [rxtx | tx | rx]**	Opcional
Desabilitar a função	**no lldp**	Opcional

Obs.: *não há nenhum comando separado para desligar o modo de trabalho.*

Configuração dos parâmetros de tempo

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-
Configuração do Hello Time	**[no] lldp hello-time** value	Opcional
Configuração do Hold Time	**[no] lldp hold-time** value	Opcional

Configuração do endereço de gerenciamento

Por padrão, o dispositivo usa o endereço IP da interface PVID. Se não houver IP de interface correspondente para o VLAN correspondente, o endereço de gerenciamento TLV não é enviado no LLDPDU. Use o seguinte comando para modificar. A interface de loopback atualmente não é suportada.

» Configuração do endereço de gerenciamento:

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração de porta	**interface {ethernet | pon}** port-num	-
Configuração do endereço de gerenciamento	**[no] lldp management-address { supervlan-interface** value **| vlan-interface** value **}**	Opcional

Visualização de informações e manutenção

Operação	Comando	Obrigatório/ opcional
Acesse o modo de configuração global	**configure terminal**	-

Visualização de informação	**show lldp interface [{ethernet | pon}** port-number**]**	Opcional

39.3. Exemplo de configuração

» Requisitos de rede:

OLT1 e OLT2 são conectados diretamente pela porta 1 e em seguida abra a função LLDP.

» Passos de configuração:

» Configuração OLT1:

OLT1(config)#lldp

» Configuração OLT2:

OLT2(config)#lldp

» Validação de resultados:

» Exiba as configurações e a informação do vizinho LLDP:

OLT1(config)#show lldp interface ethernet 0/1

System LLDP: enable

LLDP hello-time: 30(s) LLDP hold-time: 4 LLDP TTL: 120(s)

Interface Ethernet 0/1

Port LLDP: rxtx Pkt Tx: 158 Pkt Rx: 160

Total neighbor count: 1

Neighbor (1):

TTL: 106(s)

Chassis ID: 00:0a:5a:20:4d:ad

Port ID: port e0/1

System Name: SW2

System Description: New GreenNet Switch

Port Description: NULL
Management Address: 192.168.4.52
Port Vlan ID: 4
Port SetSpeed: auto
Port ActualSpeed: FULL-1000
Port Link Aggregation: support ,not in aggregation

Termo de garantia

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo este de 90 (noventa) dias de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca expressa de produtos que apresentarem vício de fabricação. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.

5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

O processo de fabricação deste produto não é coberto pelos requisitos da ISO 14001.

Todas as imagens deste manual são ilustrativas.

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: intelbras.com.br/suporte-tecnico
Suporte via e-mail: suporte@intelbras.com.br
SAC: 0800 7042767
Onde comprar? Quem instala?: 0800 7245115

Produzido por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

01.18
Origem: China