intelbras

Manual do usuário

OLT 8820 G

intelbras

OLT 8820 G

OLT GPON com 8 portas Gigabit Ethernet compartilhadas com 8 slots para módulos SFP, possui também 2 portas 10 Gigabit Ethernet e 8 slots para módulos SFP GPON

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

A OLT GPON Intelbras atende aos requisitos do padrão ITU-T G.984 e é o equipamento central utilizado em redes FTTx, atua como um concentrador de assinantes, distribuindo o acesso a clientes e serviços. Cada porta GPON atende até 64 clientes, disponibilizando 2.5 Gbps de largura de banda de downstream e 1.25 Gbps de upstream.

Índice

1. Convenções de estilo e notação

As convenções a seguir são usadas neste documento para alertar usuários com informações que são para instrução, que avisam sobre potenciais danos aos equipamentos ou aos dados do sistema. Leia atentamente e siga as instruções contidas neste documento.

☑	**Observação:** este alerta fornece informações complementares e/ou adicionais
⚠	**Cuidado:** este alerta informa ao usuário sobre condições ou ações que poderiam danificar o equipamento ou os dados do sistema
✎	**Dica:** este alerta fornece informações adicionais que permitem que os usuários concluam suas tarefas de modo mais rápido

2. Siglas

As abreviaturas a seguir são relacionadas aos produtos Intelbras e podem aparecer em todo o material.

Abreviatura	Descrição
802.1w	IEEE 802.1w rapid spanning tree protocol
802.3ad	IEEE 802.3ad physical layer specifications-aggregation of multiple link segments
AC	Alternating Current
APC	Angled physical contact (para conector de fibra)
ARP	Address resolution protocol
CPE	Consumer Premises Equipment
DC	Direct Current
DDM	Digital Diagnostic Monitoring
DHCP	Dynamic Host Configuration Protocol
GEM	GPON Encapsulation Method
GPON	Gigabit Passive Optical Network
GTP	GPON Traffic Profile
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPTV	IP (Internet Protocol) Television
LED	Diodo emissor de luz
MAC	Media Access Control
MIB	Management Information Bases
OLT	Optical Line Terminator
OMCI	ONT Management and Control Interface
ONT	Optical Network Terminator
ONU	Optical Network Unit
POTS	Plain Old Telephone Service
PPPoE	Point-to-Point Protocol Over Ethernet
QoS	Quality of Service
RF	Radio Frequency
RSSI	Received Signal Strength Indication
SC adaptor	Subscriber Connector adaptor
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
T-Conts	Transmission Containers
TFTP	Trivial File Transfer Protocol
UPC	Ultra Physical Contact (para conector de fibra)
UNIs	User Network Interfaces
VLAN	IEEE 802.1Q Virtual LANs
VoIP	Voice over IP (Internet Protocol)
Wi-Fi	Wireless local area network (marca registrada da Wi-Fi alliance)

Abreviaturas e suas descrições

3. Visão geral da OLT 8820 G

A OLT 8820 G oferece alta concentração de acesso a assinante com baixo custo e de alta densidade.

A OLT 8820 G é uma plataforma da próxima geração que possibilita a realização de serviços de dados, voz e vídeo sobre downlinks GPON e uplinks Gigabit Ethernet e 10 Gigabit Ethernet.

A OLT 8820 G pode ser implantada em ambientes como Data Center, CO (Central Office) e armários externos. Todos os casos devem possuir ambiente controlado e podem ser utilizados para aplicações de terminais remotos. A OLT 8820 G destina-se somente para locais com acesso restrito.

Conforme os prestadores de serviço buscam melhorar os rendimentos e oferecer novos serviços de multimídia, a disponibilidade da largura de banda e a qualidade do serviço tornam-se cruciais. A necessidade de oferecer serviços de vídeo de alta definição, de Internet mais rápida e de conteúdo sob demanda, combinam-se para exigir serviços à base de fibra óptica de alta velocidade. A tecnologia baseada na norma GPON torna-se a solução escolhida para oferecimento de redes Triple Play completas.

Historicamente, os altos custos necessários para construção e instalação de redes FTTx apresentaram uma barreira significativa para sua ampla adoção. De modo semelhante, o processo longo e custoso de cabear novamente casas com Ethernet para IPTV também atrasou a implantação. A fibra óptica normalmente é procurada para novas implantações e aplicações Greenfield, onde os custos para implantação de fibra não são superiores aos custos para implantação de uma nova rede de cobre. Entretanto, cada vez mais os prestadores de serviços estão começando a migração de FTTx em bairros existentes garantindo que a largura de banda necessária esteja disponível, oferencedo desta forma um conjunto de serviços competitivo. A Intelbras abordou esses desafios a partir de uma perspectiva dos prestadores de serviços e desenvolveu soluções para simplificar a instalação FTTx, minimizando custos operacionais e oferecendo redes totalmente capacitadas para serviços "Triple Play" sem a necessidade fiação nova e dentro das residências.

Para os conjuntos residenciais existentes, dispor a fibra óptica até as casas envolve grande construção e grande investimento. A tecnologia GPON (Gigabit Passive Optical Network) é considerada como a tecnologia mais econômica para FTTH (Fiber to Home), já que sustenta até 64 divisões passivas, otimizando o custo dos transceptores ópticos na OLT, possui capacidade largura de banda de downstream de 2.5 Gbps e 1.25 Gbps de upstream.

Serviços de entretenimento evoluíram rapidamente nos últimos anos, transmissão de alta definição (HDTV) aprimorados com novos recursos de interatividade e sob demanda, juntamente com novos padrões de compressão como MPEG-4 AVC reduzem a largura de banda de vídeo por transmissão pela metade em relação ao MPEG-2, ofertas maiores de canais em combinação com a quantidade crescente de televisões HD por residência estão, de modo geral, aumentando a demanda por largura de banda. Há alguns anos os serviços de IPTV, mais acesso à internet exigiam de 15 a 23 Mbps por residência para os serviço em duas a três TVs. Atualmente, a maioria dos prestadores de serviço esperam oferecer HD para três a cinco TVs e com velocidades mais rápidas de Internet para downloads de vídeo e jogos. Muitos prestadores de serviço agora acreditam que a largura de banda necessária por residência está chegando a 28 - 35 Mbps, excedendo as capacidades do DSL na maioria das linhas de cobre. Essas tendências em serviço de banda larga fizeram com que analistas e prestadores de serviço previssem que 100 Mbps serão necessários por residência nos próximos 10 anos.

A Intelbras oferece uma solução completa com OLT, ONU e ONTs para todo tipo de aplicação FTTx. A Intelbras permite a convergência inteligente e controlada de serviços de banda larga entre os prestadores de serviço e a rede residencial com até 100 Mbps de largura de banda em uma solução completa de FTTx.

3.1. Características da OLT 8820 G

Suporte a dados

A OLT 8820 G oferece os seguintes serviços de dados:

- Encapsulação em bridge
- DHCP Relay
- Bridging transparente, bridging VLAN, intralinks e Transparent LAN Service (TLS)
- Type of Service (TOS) e Class of Service (COS)

Padrões suportados

A OLT 8820 G suporta os seguintes padrões:

- ITU-T G.984.1 - 984.4 OMCI

» IEEE 802.3 Ethernet
» IEEE 802.1p
» IEEE.802.1q
» IEEE 802.1w
» IEEE 802.3ad

Protocolos suportados

A OLT 8820 G suporta os seguintes protocolos:

» RFC 1483/2684
» DHCP Relay com Option 82
» Suporte a bridging 802.1D
» Suporte a VLAN 802.1p/q
» Suporte a RSTP 802.1w
» Suporte a MSTP 802.1s
» EAPS (Ethernet Automatic Protection Switching) - RFC 3619
» Agregação de link com suporte a LACP 802.3ad
» Proxy IGMPv2 e V3
» Controle de acesso integrado e proteção de conteúdo
» Autenticação Radius

Gerenciamento

A OLT 8820 G possui duas interfaces de gerenciamento out-of-band: 1 porta serial RS232 e 1 porta 10/100BASE-T Ethernet.

> **Observação:** a interface 10/100BASE-T Ethernet possui por padrão o endereço IP 192.168.10.1. Ao utilizar o comando *set2default* sem a opção de restauração, o endereço IP padrão é restabelecido

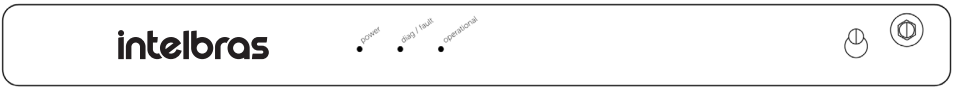
Após estabelecer conexão com a OLT 8820 G, os administradores podem gerenciar o dispositivo usando Command Line Interface (CLI), Web GUI, SNMP.

3.2. OLT 8820 G

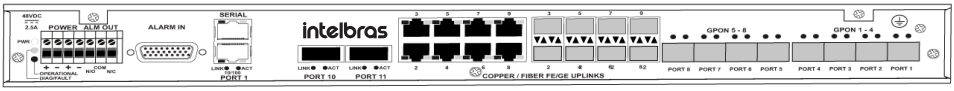
A OLT 8820 G suporta:

» Oito uplinks FE/GE
» Dois uplinks 10GE
» Entradas prara alimentação redundantes
» Entradas de alarme
» Saídas de alarme
» LEDs para as portas
» Bandeja da ventoinha removível

Os cabos e os conectores da OLT 8820 G são acessados pela parte posterior. O fluxo do ar passa pela unidade da direita para a esquerda.



Visualização frontal da OLT 8820 G



Visualização posterior da OLT 8820 G

Interfaces da OLT 8820 G

As interfaces são identificadas pelas seguintes linhas de comando:

- » Para as interfaces FE/GE, *1-1-x-0/eth*, onde x vai de 2 até 9.
- » Para as interfaces *10GE, 1-1-x-0/eth*, onde x é 10 ou 11.
- » Para as interfaces GPON, *1-1-x-y/gpononu*, onde x é de 1 a 8 e y varia de 1 a 64.

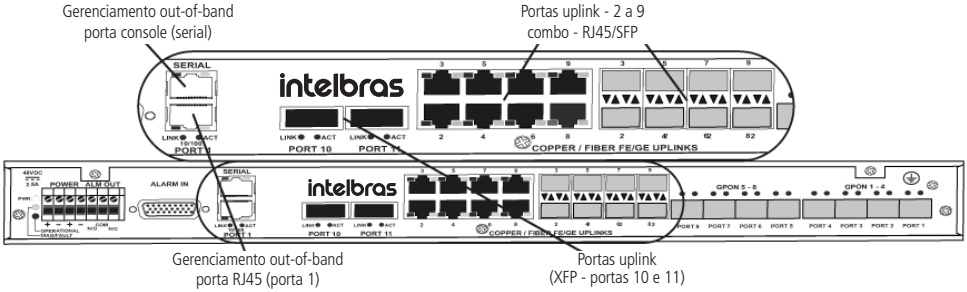
Gerenciamento e outras interfaces

A OLT 8820 G oferece as seguintes interfaces de gerenciamento:

- » Porta Ethernet full duplex 10/100 BaseT para gerenciamento local ou conectividade com a rede.
- » Porta serial RS232 para gerenciamento local.

Interfaces uplink FE/GE e 10GE

A OLT 8820 G oferece oito portas 100/1000 Ethernet RJ45 combo com oito slots SFPs, se um slot SFP for usado para uma porta, a porta RJ45 correspondente não poderá ser utilizada. Os módulos SFPs podem ser 1000baseT em par trançado ou fibra (SX, LX ou ZX). Os dois slots XFP possibilitam a adição de uplinks 10GE, conforme exibido na imagem a seguir.



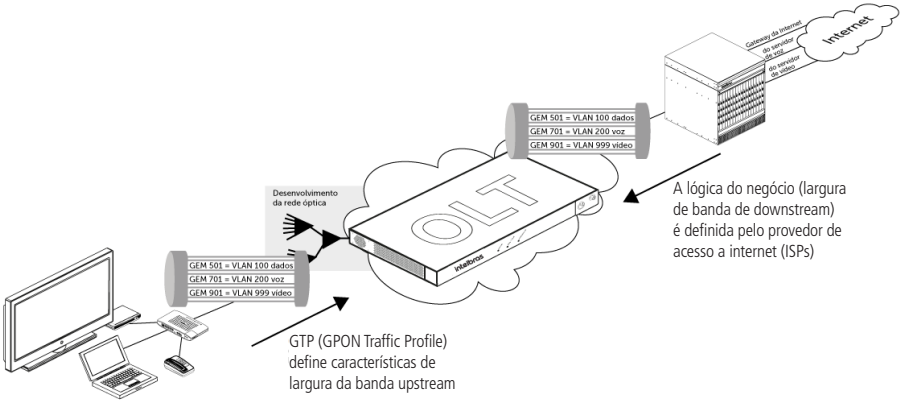
Portas do painel posterior da OLT 8820 G

As interfaces ópticas estão em conformidade com a Norma de Segurança Internacional de Laser IEC 825 categoria 1.

Interfaces GPON

A OLT 8820 G suporta oito portas GPON com base nos padrões ITU-T G.984.

O GPON oferece um tráfego máximo de 2,5 Gbps de downstream e 1,25 Gbps de upstream. GPON é uma arquitetura Ponto-Multipontos que pode ser dividida em 64 extremidades de assinantes por porta GPON, portanto os 2,5 Gbps downstream e 1,25 Gbps upstream são divididos entre os assinantes. Todas as informações são enviadas para todas as unidades. A criptografia mantém a privacidade das informações.



Quando a OLT 8820 G e a Rede de Implantação Óptica (ODN) se encaixam na solução de GPON

Conforme exibido na imagem anterior, a lógica do negócio, como a largura de banda de downstream, é definido no provedor de serviço à internet (BRAS). As características de largura de banda upstream são definidas nos perfis de tráfego GPON (GTP) da OLT.

O seguinte módulo SFP é usado nas portas GPON da OLT 8820 G:

» KPSD 1120 G: GPON-SFP-B+-RSSI

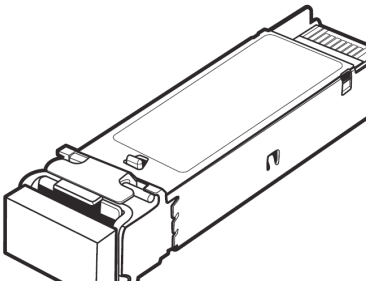
Este módulo SFP suporta o recurso de Received Signal Strength Indication (RSSI).

A criptografia AES de 128 bits é suportada no chipset GPON da OLT.

Small Form Factor Pluggables (XFPs e SFPs)

SFPs (transceptores ópticos) e XFPs são links de dados duplex integrados de alto desempenho para comunicação bidirecional sobre fibras ópticas multimodos ou monomodos. Todos os módulos SFPs possuem conectores compatíveis com o padrão da indústria de conectores LC. Todos os slots SFPs suportados são hot swap (alimentados a quente), o que permite que sejam facilmente inseridos ou substituídos independentemente de a energia estar ligada.

Além disso, esse módulo optoeletrônico são produtos a laser de categoria 1 em conformidade com as Normas de Desempenho de Radiação da FDA, 12 CFR Subcapítulo J. Este componente também está em conformidade com a categoria 1 de produtos a laser de acordo com a Norma de Segurança Internacional IEC 825-1.



Small Form Factor Pluggables (SFP)

SFPs e XFPs suportados

A OLT 8820 G suporta os seguintes SFPs Gigabit Ethernet, SFPs GPON e XFPs 10 Gigabit Ethernet:

Tipo de SFP/XFP	Descrição
SFPs Gigabit Ethernet	
Fast Ethernet/Gigabit Ethernet TP	Até 100 metros com conector RJ45
Gigabit Ethernet SX	Transmite 850 nm, recebe 850 nm, até 500 metros com conector LC duplo
Gigabit Ethernet LX	Transmite 1310 nm, recebe 1310 nm, até 10 quilômetros com conector LC duplo
Gigabit Ethernet EX	Transmite 1550 nm, recebe 1550 nm, até 40 quilômetros com conector LC duplo
Gigabit Ethernet ZX	Transmite 1310 nm, recebe 1310 nm, até 80 quilômetros com conector LC duplo
Gigabit Ethernet BX	Transmite 1310 nm, recebe 149 nm, até 10 quilômetros com conector LC único
Gigabit Ethernet BX	Transmite 1490 nm, recebe 1310 nm, até 10 quilômetros com conector LC único
Gigabit Ethernet BX20	Transmite 1310 nm, recebe 1490 nm, até 20 quilômetros com conector LC único
Gigabit Ethernet BX20	Transmite 1490 nm, recebe 1310 nm, até 20 quilômetros com conector LC único
Gigabit Ethernet BEX	Transmite 1310 nm, recebe 1490 nm, até 40 quilômetros com conector LC único
Gigabit Ethernet BEX	Transmite 1490 nm, recebe 1310 nm, até 40 quilômetros com conector LC único
SFPs GPON	
SFP GPON B+	Transmite 1490 nm, recebe 1310 nm com conector SC/UPC; Alcance de até 20 km; orçamento de potência de -28 dB; suporta RSSI digital; em conformidade com ITU-T G.984.2
XFPs 10GE	
XFP Long Reach 40	Transmite 1550 nm, recebe 1550 nm, até 40 km com conector LC/UPC duplo em fibra monomodo
XFP Long Reach 80	Transmite 1550 nm, recebe 1550 nm, aé 80 km com conecotr LC/UPC duplo em fibra monomodo
XFP Long Reach	Transmite 1310 nm, recebe 1310 nm, até 10 km com conector LC/UPC duplo em fibra monomodo
XFP Short Reach	Transmite 850 nm, recebe 850 nm, até 300 metros com conector LC/UPC duplo em fibra multimodo

SFPs e XFPs suportados

3.3. Limites e capacidade máxima de configuração do sistema

A tabela abaixo informa a capacidade máxima de configuração dos recursos do sistema.

OLT 8820G	Quantidade máxima
Endereços Mac	32768
Total de Bridges	1894
Bridge do tipo TLS	1792
Bridge do tipo Uplink	100
Bridge do tipo Downlink	1792
Bridge do tipo Intralink	1792
Bridge do tipo Wire	768
Canais Multicast	1024

Obs.: *para utilização superior a 100 bridges distintas do tipo Uplink, é necessário a utilização do recurso QinQ.*

Exemplo:

1. Configurar a interface uplink utilizando a VLAN 0 e SLAN 2000 e a palavra-chave "stagged".

iSH> bridge add 1-1-2-0/eth uplink vlan 0 slan 2000 stagged

2. Configurar cada interface downlink conforme sua respectiva VLAN, porém, utilizando o mesmo SLAN e a palavra-chave "stagged".

iSH> bridge add 1-1-1-1/gpononu downlink vlan 50 slan 2000 stagged eth 1

iSH> bridge add 1-1-2-5/gpononu downlink vlan 51 slan 2000 stagged eth 1

iSH> bridge add 1-1-3-8/gpononu downlink vlan 52 slan 2000 stagged eth 1

4. Preparação para instalação

4.1. Precauções de segurança gerais

O equipamento é projetado e fabricado em conformidade com as normas de segurança a seguir: UL 60950-1, EN 60950-1, IEC 60950-1, ACA TS001. Entretanto, as precauções adicionais a seguir devem ser observadas para garantir a segurança pessoal durante instalação ou serviço e para evitar danos ao equipamento ou aos equipamentos conectados.

Precauções de EMC

> ⚠ **Cuidado:** a utoridade responsável por operar este equipamento deve cumprir com a exigência de que nenhuma modificação seja feita ao equipamento exceto nos casos onde foram expressamente aprovadas pelo fabricante

Este é um produto da categoria A. Em um ambiente doméstico, este produto pode causar rádio interferência, caso no qual o usuário pode ter de tomar as medidas apropriadas.

Precauções de segurança de instalação e serviço

As precauções a serem tomadas antes de instalar ou realizar serviço no produto são as seguintes:

- Leia e siga todas as notas de advertência e as instruções marcadas no produto ou inclusas neste guia.
- Nunca instale fiação de telefone durante uma tempestade com raios.
- Nunca toque nos fios ou terminais de telefone não isolados, exceto no caso de a linha de telefone ter sido desconectada da interface de rede.
- Nunca instale este produto em um local úmido.
- Nunca tente realizar serviço neste produto exceto no caso de ser um técnico de serviço autorizado. Fazer isso pode expor você a pontos perigosos de alta tensão ou a outros riscos e pode resultar em lesão ou danos à unidade e anular todas as garantias.
- A OLT 8820 G exige uma conexão de aterramento dedicada. Se mais de uma OLT 8820 G for instalada em um bastidor, cada uma exige sua própria conexão de aterramento direta ao sistema de aterramento do local de instalação.
- Encaixes e aberturas no produto são fornecidos para ventilação. Para garantir uma operação confiável do produto e protegê-lo contra aquecimento, esses encaixes e aberturas não devem ser bloqueados ou cobertos.

» Um raro fenômeno pode criar um potencial de tensão entre os pontos de aterramento de dois ou mais edifícios. Se produtos instalados em edifícios separados são interconectados, o potencial de tensão pode causar uma condição perigosa. Entre em contato com um consultor elétrico qualificado para determinar se este fenômeno existe ou não e, se necessário, implemente ação corretiva antes de interconectar o produto.

» Instale a OLT 8820 G de acordo com os códigos elétricos nacionais e locais para atender às exigências do órgão regulador. Entre em contato com um consultor elétrico qualificado.

Informações de segurança do fornecimento de energia

Instale um condutor de aterramento do equipamento de tamanho não inferior aos conectores de alimentação do circuito de ramificação não aterrado como parte do circuito que alimenta o produto ou o sistema. Condutores de aterramento expostos, cobertos ou isolados são aceitáveis. Condutores de aterramento de equipamentos individualmente cobertos ou isolados devem ter um acabamento externo contínuo verde ou verde com uma ou mais faixas em amarelo. Conecte o condutor de aterramento do equipamento ao terra no equipamento de serviço.

4.2. Precauções de instalação

Evite criar uma condição perigosa mantendo distribuição de peso equilibrada no equipamento.

A temperatura operacional máxima não deve exceder 65°C (149°F). A temperatura ambiente do rack pode ser superior à temperatura ambiente quando o sistema for instalado em um bastidor fechado ou de unidades múltiplas. Observe a temperatura operacional máxima recomendada.

Não bloqueie as saídas de ar do sistema. Isso impossibilitará o fluxo de ar necessário para resfriamento adequado. Espaço livre suficiente deve existir em todos os lados do rack para permitir acesso ao equipamento.

A Intelbras recomenda usar dutos de cabeamento para direcionamento dos cabos no rack. Para evitar sobrecarregar nos suportes de montagem e danificar o sistema, não use a OLT 8820 G como suporte para outros equipamentos após ser montado no rack.

Conecte o sistema ao circuito de alimentação de energia conforme descrito neste documento. Não sobrecarregue o sistema ou o circuito de alimentação de energia.

Certifique-se de que o aterramento adequado do sistema seja realizado e mantido. Utilize conexões da alimentação de energia para aterramento em vez de circuito ramificados como réguas de energia).

4.3. Seleção do local do sistema

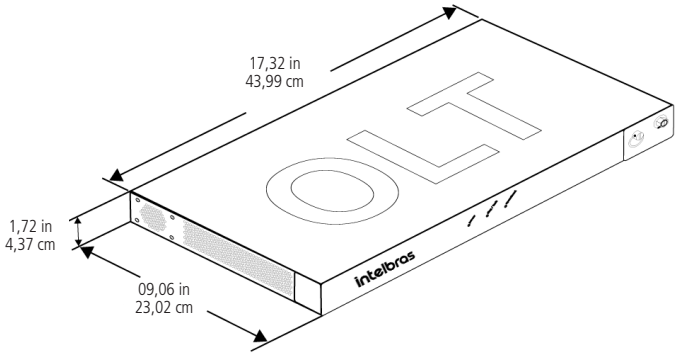
Certifique-se de que o ambiente esteja livre de poeira e umidade excessiva, não exposto a temperaturas extremas e que tenha ventilação suficiente.

Instale o sistema próximo a todos os equipamentos aos quais será conectado. Certifique-se de que os tipos de cabos utilizados sejam adequados para todas as conexões do sistema e da rede. Para melhores resultados, use cabos e conectores recomendados neste documento.

4.4. Especificações ambientais

Descrição	Especificação
Dimensões A × L × P	(1U) 4,37 × 43,99 × 23,02 cm
Peso	3,6 kg
Temperatura operacional	-40 °C a +65 °C
Temperatura de armazenamento	-40 °C a +70 °C
Umidade operacional relativa	5% a 85% sem condensação
Umidade relativa de armazenamento	Até 95% sem condensação
Fluxo de ar	Direita para esquerda

Especificações ambientais da OLT 8820 G



Dimensões da OLT 8820 G

4.5. Requisitos e especificações de alimentação

A OLT 8820 G utiliza uma ou duas fontes de alimentação de 48 Vdc. A utilização de duas fontes de alimentação somente é necessária nos casos onde se deseja redundância na alimentação.

Observação: o local de instalação deve incluir proteção contra sobrecorrente, como fusíveis ou disjuntores, que limitarão a corrente na entrada do sistema

4.6. Especificações de energia

Descrições	Especificações
Tensão nominal	48 Vdc nominal: mínimo 43,75 Vdc, máximo 59,9 Vdc
Consumo de energia	94 W; máximo: 109 W
Corrente nominal	2,5 A máximo
Cabo de entrada DC	AWG 12 (6 mm^2) máximo

Especificações de energia DC da OLT 8820 G

Especificações do sistema

Descrição	Especificação
Segurança	CSA 22.2 No. 60950-1 EN 60950-1 IEC 60950-1 UL 60950-1
Emissões de EMC	FCC Part 15 Class A GR-1089-Core Level 3 CE EN55022A
Imunidade de EMC	GR-1089-Core Level 3 EN 300 386 V1.4.1
Ambiental	GR-63-Core Level 3 ETS 300 019-2-x ISTA Transportation and Handling
Rede	FCC Part 68 CTR-12 CTR-13 NTR-4 TSO-16

Conformidade e especificações

Descrição	Especificação
Interfaces de gerenciamento	Porta serial RS232 Porta Ethernet 10/100BASE-T Ethernet (Out-of-band)

Interfaces de gerenciamento

Descrição	Especificação
Densidade	8 portas GPON – 512 assinantes (64 assinantes por interface)
Interfaces físicas	8 slots para conexão de módulos SFP GPON
Características	Comprimento de onda de recepção 1310 nm Comprimento de onda de transmissão 1490 nm
Taxa nominal	2,5 Gbps downstream 1,25 Gbps upstream
Suporte padrão	ITU-T G.984

Especificações de GPON

Descrição	Especificação
Densidade	8 portas Fast/Gigabit Ethernet
Interface física	8 slots SFP e 8 conectores RJ 45 (funcionam em modo combo)
Suporte Ethernet	100/1000 Mbps Ethernet

Especificações de uplink FE/GE

Descrição	Especificação
Densidade	2 portas 10 Gigabit Ethernet
Interface física	2 slots XFP
Suporte a Ethernet	10 Gbps Ethernet

Especificações de uplink 10GE

5. Cabeamento e conectores da OLT 8820 G

5.1. Orientações do cabeamento

Certifique-se de que as linhas de energia estão colocadas no mínimo duas polegadas de distância dos cabos de comunicação. Isso pode ser feito acondicionando e direcionando as linhas de energia atrás do bastidor (direcione os cabos de comunicação na frente do bastidor).

5.2. Descrições de cabos

Observação: a Intelbras recomenda utilizar cabos de cobre 24 AWG (CAT 5) ou cabos superiores para interfaces Ethernet 100BASE-T, obtendo assim um desempenho superior de transmissão além de melhorar o alcance do loop do assinante

Descrição de cabos	Interface da OLT 8820 G para	Tipo de cabo	Tipo de conector
Uplink FE/GE	Dispositivo uplink FE/GE	Fibra óptica (multimodo ou monomodo) ou cabo de cobre	Conector SFP para fibra óptica ou conector RJ45
Uplink 10GE	Dispositivo uplink de 10GE	Fibra óptica (multimodo ou monomodo)	Conector XFP para fibra óptica
GPON	Dispositivos ONU/ONT GPON	Fibra óptica monomodo	Conector SC/APC
Saída de alarmes	Contatos de relé de alarme na OLT 8820 G	Mínimo 20 AWG (0,8 mm) 24 AWG (0,5 mm) recomendado	Cabo branco para terminais de parafuso
Entrada de alarmes	Contatos de relé de alarme na OLT 8820 G	Mínimo 20 AWG (0,8 mm) 24 AWG (0,5 mm) recomendado	Conector D-sub macho 26 de pinos
Gerenciamento (IP)	Porta 10/100BASE-T Ethernet	Categoria 5 de 4 pares	Conector RJ45
Gerenciamento (porta serial)	RJ45 de 8 pinos	Mínimo 26 AWG de 4 cabos (0,4 mm)	Conector RJ45

Resumo das especificações de cabos

5.3. Pinagem da OLT 8820 G

Pinagens da porta FE/GE (RJ45)

Número do pino	Função
1	Tx+
2	Tx-
3	Rx+
4	Não usado
5	Não usado
6	Rx-
7	Não usado
8	Não usado

Pinos da porta Ethernet

Pinagens da porta serial

Número do pino	Função
1	Não usado
2	Não usado
3	Não usado
4	Terra
5	Transmissão de dados (em relação a OLT 8820 G) (para RS232, recebimento de dados em relação ao terminal (console))
6	Recepção de dados (em relação a OLT 8820 G) (para RS232, transmissão de dados em relação ao terminal (console))
7	Não usado
8	Não usado

Pinos da porta serial

Pinagens do conector de alarme

Número do pino	Função
5	NO (Normalmente Aberto - Normally Open)
6	Comum
7	NC (Normalmente Fechado - Normally Closed)

Pinos de saída do alarme (pinos 5, 6 e 7 do conector Power ALM OUT)

Número do pino	Função	Número do pino	Função	Número do pino	Função
1	(–) BAT 48 Vdc	10	5A	19	9B
2	1A	11	5B	20	10A
3	1B	12	6A	21	10B
4	2A	13	6B	22	11A
5	2B	14	7A	23	11B
6	3A	15	7B	24	12A
7	3B	16	8A	25	12B
8	4A	17	8B	26	+48 V RTN/GND
9	4B	18	9A		

Pinos de entrada do alarme

5.4. Conexão dos cabos ópticos

Cuidado: as interfaces de fibra óptica monomodo da OLT 8820 G emitem radiação de laser invisível, que pode causar danos. Quando um cabo óptico é conectado a um dispositivo, a radiação é confinada dentro do cabo óptico e não apresenta perigo. Entretanto, em caso de serviço nos módulos SFPs, sempre tome as seguintes precauções:

- » Desconecte a fibra da OLT 8820 antes de instalar ou remover cabos.
- » Certifique-se que as proteções de borrachas estejam encaixadas nos conectores SC ou LC dos módulos quando não estiverem em uso.
- » Nunca olhe diretamente para o interior dos conectores ópticos.

1. Desconecte os módulos SFPs da OLT 8820 G para garantir que a interface óptica não esteja emitindo radiação a laser;
2. Remova as proteções de borracha dos conectores SC ou LC da extremidade dos cabos de fibra óptica;
3. Remova as proteções de borracha dos conectores SC ou LC dos módulos SFPs;
4. Insira suavemente os conectores SC ou LC dos cabo ópticos nas conexões Tx e Rx dos módulos SFPs;
5. Conecte a outra extremidade do cabo óptico na respectiva porta (RX ou TX) do dispositivo remoto.

5.5. Manutenção e manuseio da fibra óptica

Radiação do laser

Os equipamentos da Intelbras e os conjuntos de teste óptico associados usam fontes de laser que emitem energia luminosa aos cabos de fibra óptica. Essa energia está dentro da região infravermelho (invisivel) do espectro eletromagnético vermelho (visível).

Produtos a laser são classificados em categorias (I, II, III ou IV) conforme caracteristicas da radiação emitida. Em termos de saúde e segurança, os produtos da Categoria I apresentam o menor perigo (nenhum perigo) e os produtos da Categoria IV apresentam o maior perigo.

Leia e observe as precauções a seguir para reduzir o risco de exposição à radiação a laser.

Cuidado: em todos os momentos durante o manuseio de fibras ópticas, siga os procedimentos de segurança recomendados pela sua empresa

Embora os produtos ópticos da Intelbras tenham certificação de Categoria I, a exposição perigosa à radiação a laser pode ocorrer quando cabos de fibra óptica conectando componentes do sistema estão desconectados ou partidos. Determinados procedimentos realizados durante os testes exigem o manuseio de fibras ópticas sem as tampas de proteção, portanto, aumentam o risco de exposição.

Durante serviços de manutenção, reparo ou a remoção de cabos ou equipamentos, siga as medidas a seguir:

- » Evite exposição direta a extremidades das fibras ou as extremidades dos conectores ópticos.

Siga as instruções do fabricante ao utilizar um conjunto de testadores ópticos. Configurações incorretas de calibragem ou controle podem resultar em níveis perigosos de radiação.

Manuseio das fibras ópticas

Ao trabalhar com fibras ópticas, você deve tomar as seguintes precauções:

- » Use óculos de segurança ao instalar fibras ópticas.
- » Limpe suas mãos após manusear fibras ópticas. Pequenos cacos de vidro não são sempre visíveis e podem danificar seus olhos. Se você tiver um caco de vidro nos seus olhos, busque cuidado médico imediatamente.
- » Nunca olhe diretamente na extremidade de uma fibra óptica ou na extremidade de um conector óptico quando a unidade está ativa ou energizada.
- » Evite a exposição direta a extremidade da fibra óptica ou extremidades dos conectores ópticos. Não manuseie peças de fibras ópticas com seus dedos. Use pinças ou fitas adesivas para tirar e descartar extremidades de fibras ópticas soltas.
- » Use luvas de borracha ao limpar conectores ópticos. As luvas evitam contato direto com o álcool isopropílico e evitam contaminação da fibra com óleos da pele.
- » Coloque todos os recortes da fibras ópticas em um recipiente de plástico fornecido para essa finalidade.
- » Manuseie as fibras ópticas com cuidado. Coloque as fibras ópticas em um local seguro durante a instalação.

» A fibra não pode ter uma dobradura muito acentuada. Ao causar uma dobradura muito acentuada (microcurvatura) na fibra óptica poderá degradar a transmissão do sinal óptico. Essas microcurvaturas também podem criar microfraturas no vidro da fibra, resultando em perda de sinal.
» Proteja todos os conectores de fibras ópticas com tampas de proteção contra poeira em todos os momentos.
» Siga as instruções do fabricante ao utilizar um conjunto de testadores ópticos. Configurações incorretas de calibragem podem resultar em níveis perigosos de radiação.

A fibra óptica precisa ser mantida limpa. Contaminantes podem obstruir a passagem de luz. Contaminantes notáveis incluem:

» Óleo das mãos.
» Partículas de poeira.
» Fibra de algodão.
» O resídio que pode ser deixado ao usar métodos de limpeza com umidade.
» Arranhões feitos por métodos de limpeza a seco ou fibra manuseada de modo inapropriado.

Seleção dos materiais de limpeza

Os materiais utilizados para limpeza dos equipamentos da Intelbras devem ser de alta qualidade e devem ser adequados para essa finalidade.

» Desconecte a extremidade do cabo a ser limpa.
» Usando gás de limpeza, sopre a poeira e os detritos acumulados para fora das superfícies cilíndricas e extremas do conector.
» Aplique álcool isopropílico de nível óptico a uma tecido apropriado de limpeza.
» Tampe novamente ou reconecte o conector imediatamente para evitar contaminação. Verifique se o sistema está funcionando apropriadamente.

Reparo de fibras ópticas

Quando uma ruptura acidental ocorrer no cabo de fibra óptica, execute as seguintes medidas:

» Notifique o pessoal do escritório central e técnicos de reparos sobre o problema.
» Identificar e informa ao escritório central quais fibras foram danificadas.
» Desligar todas as fontes de laser relacionadas às fibras danificadas (independentemente de estarem localizadas na unidade central, nas instalações do assinante ou em um local remoto).

6. Instalação da OLT 8820 G

6.1. Instalação em rack 19 polegadas

Instalação dos suportes de montagem

Importante: este produto deve ser instalado por um profissional qualificado.

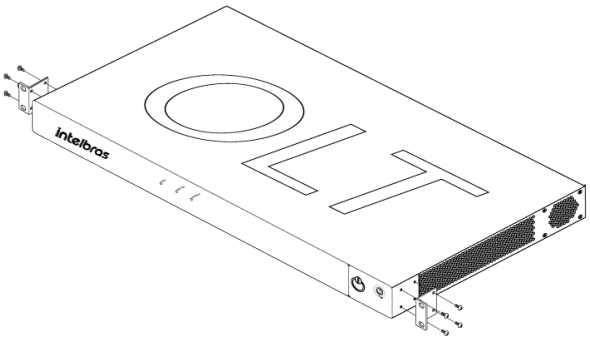
Os suportes de fixação da OLT 8820 G são projetados para uso em rack de 19 polegadas.

Instalação dos suportes de fixação

Para instalar os suportes de fixação da OLT 8820 G, siga os procedimentos a seguir:

1. Com cuidado, coloque a OLT sobre uma superfície de trabalho limpa, plana e firme;
2. Retire das embalagens individuais os dois suportes de fixação que acompanham o dispositivo e os 12 parafusos;
3. Instale os suportes de fixação, parafusando-os nas laterais da OLT.

☑	**Observação:** utilize os parafusos fornecidos junto com o kit de instalação
⚠	**Cuidado:** para evitar dano ao sistema, use somente os parafusos fornecidos no kit de instalação

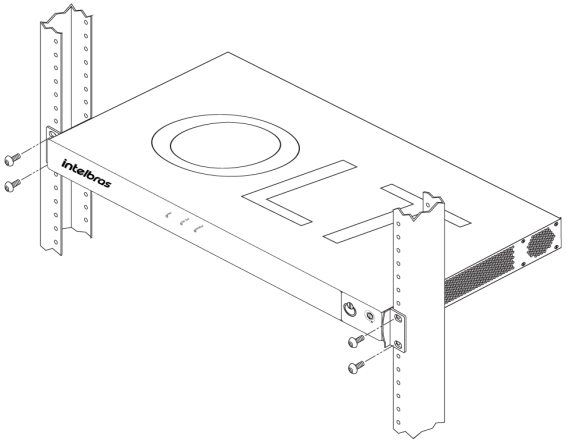


Instalação dos suportes laterais

Instalação em rack 19" (EIA)

A OLT pode ser instalada em rack de 19 polegadas que esteja conectado ao terra.

1. Escolha uma posição no rack para a fixação da OLT;
2. Insira cuidadosamente a OLT no rack com a parte frontal voltada para fora;
3. Fixe a OLT no rack utilizando os parafusos fornecidos no kit de instalação.



Instalação da OLT 8820 G em rack 19"

6.2. Alimentando e aterrando a OLT 8820 G

Requisitos de aterramento

Utilize as informações a seguir para prover um sistema de aterramento para a OLT 8820 G.

Antes de concluir a instalação da OLT, meça a impedância de referência de aterramento do local de utilização e garanta que ela seja inferior a 1 ohm. Se o aterramento for superior a 1 ohm, devem-se realizar melhorias no sistema de aterramento antes de instalar o produto. Um sistema mal-aterrado pode ocasionar queima ou mau funcionamento do produto.

A seguir, outras recomendações para o sistema de aterramento:

» Utilize fonte de alimentação dedicada para a OLT. Isso impede que o produto sofra possíveis interferências de outros dispositivos, como acontece quando utilizado com fonte de alimentação compartilhada. Caso contrário, você deve garantir um sistema de aterramento inferior a 1 ohm para um bom desempenho.

» Nunca conecte o ponto de aterramento da OLT à estrutura metálica ou aos eletrodutos do local de instalação.

» Recomenda-se evitar o uso de cabeamento perto de lâmpadas fluorescentes e de outras fontes de radiação de alta frequência, tais como transformadores.

» Utilize condutores contínuos, pois possuem baixa impedância e são mais confiáveis que os emendados.

O condutor de aterramento da OLT 8820 G deve atender aos seguintes requisitos:

» Não utilizar cabos com bitola inferior a 10 AWG em qualquer ponto do aterramento.

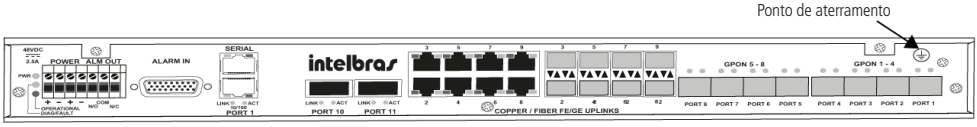
» Em condições normais de operação, o cabo de aterramento não pode conduzir corrente.

» Deve ser conectado fisicamente à referência principal do aterramento.

Aterramento da OLT 8820 G

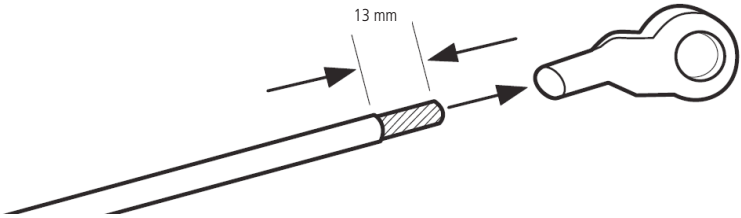
Você deve aterrar a OLT antes de alimentar o dispositivo.

1. Coloque o fio terra no parafuso de aterramento, que está no canto superior direito da OLT;



Aterramento da OLT 8820 G

2. Utilize um cabo de aterramento de no mínimo 10 AWG da OLT até o quadro de aterramento. Certifique-se de que todos os conectores do cabo de aterramento sejam feitos com metal exposto (metal nu);
3. Decape aproximadamente 13 mm do cabo de aterramento e crimpe o terminal de conexão;



Colocar a lingueta de aterramento

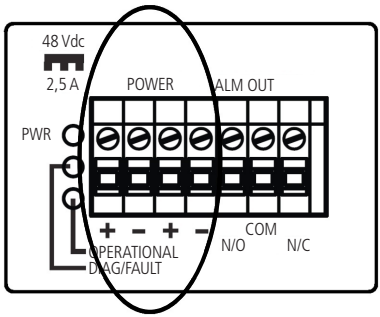
4. Conecte o cabo de aterramento à OLT e aperte o parafuso para fixá-lo.

Conectando a alimentação 48 Vdc à OLT 8820 G

Observe o procedimento a seguir para conectar a fiação entre o bloco de terminais da OLT e as duas fontes de alimentação.

1. Conecte o fio positivo da fonte de alimentação A ao terminal marcado com +. Em seguida, conecte o cabo negativo da fonte de alimentação A ao terminal marcado com -;

> ⚠ **Cuidado:** utilize fio de cobre que suporte pelo menos 5 ampères de corrente a 60 Vdc



DC 48 Vdc redundante (entradas duplas/redundantes na OLT 8820 G)

2. Conecte o fio positivo da fonte de alimentação B ao terminal marcado com +. Em seguida, conecte o fio negativo da fonte de alimentação B ao terminal marcado com -;

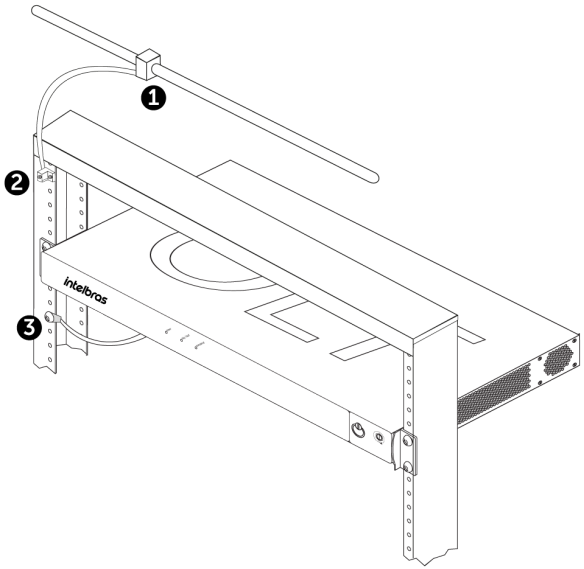
> ⚠ **Cuidado:** utilize fio de cobre que suporte pelo menos cinco ampères de corrente a 60 Vdc

3. Aperte os parafusos do terminal para que os fios fiquem fixos.

Verificação do aterramento

O aterramento adequado reduz o efeito de surto na linha e limita as tensões e interferência de RF que podem afetar a comunicação entre dispositivos de rede.

1. Teste a impedância das ligações entre o terra do quadro central (ponto 1) e o rack (ponto 2). A impedância deve ser inferior a 1 ohm;



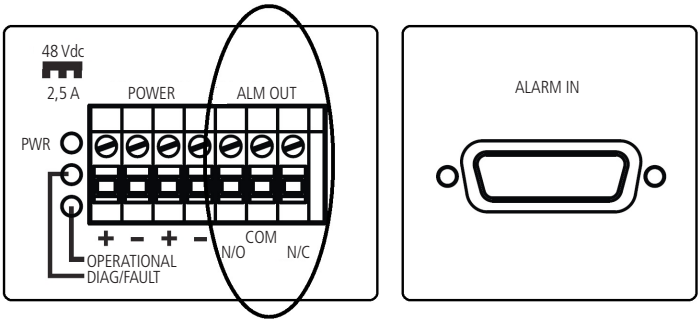
Teste de impedância

2. Teste a impedância das ligações entre o terra do rack (ponto 2) e a OLT (ponto 3). A impedância deve ser inferior a 1 ohm.

Conexão dos alarmes

A OLT 8820 G é equipada com terminais de entrada e saída de alarme. Os terminais de saída de alarme fornecem monitoramento para a central de alarme ao ocorrer um alarme crítico ou perda de energia do dispositivo. O alarme suporta contatos Normalmente Fechado (NC), Comum (COM) e Normalmente Aberto (NO).

A corrente máxima suportada pelos contatos é de 1 A a 30 Vdc.

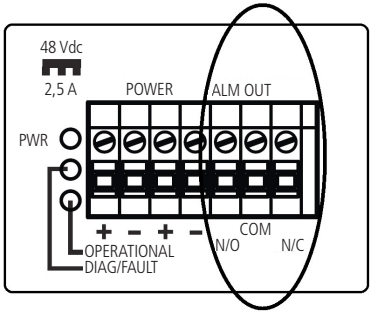


Terminais de alarme da OLT 8820 G

Conexão dos alarmes de saída

Utilize dois fios não blindados para conectar as saídas Comum e NC ou Comum e NO.

1. Descasque o revestimento plástico do fio até cerca de 6 mm;



Saídas de alarme

2. Insira a extremidade de cobre do cabo no ALARM N/C ou no ALARM N/O, dependendo do tipo de alarme (Normalmente Fechado ou Normalmente Aberto) suportado. Conecte a outra extremidade do cabo ao sistema de alarme CO;
3. Insira a extremidade de cobre do outro cabo no terminal marcado com ALARM COM e conecte sua extremidade oposta ao terminal de alarme comum CO;
4. Aperte o parafuso do terminal na parte superior de cada conector do terminal.

Número do pino	Descrição
1-4	Usado para alimentação, não para alarmes de saída
5	NO (Normalmente Aberto - Normally Open)
6	Comum
7	NC (Normalmente Fechado - Normally Closed)

Pinagem de saída de alarme (pinos 5, 6 e 7 do conector Power ALM OUT)

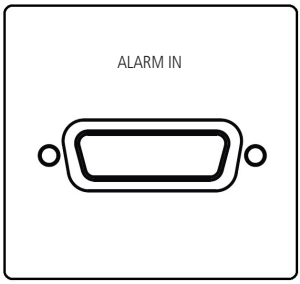
Conexão dos alarmes de entrada

A OLT 8820 G oferece um conector de entrada de alarme para a coleta de até 12 contatos NO e NC a partir de dispositivos externos (por exemplo, porta do gabinete aberta, falha no retificador, falha no sistema de ventilação, etc.). O conector de entrada do alarme aceita 48 volts. Todas as entradas do alarme são optoacopladoras metalicamente isoladas.

No conector do alarme de entrada está disponível um pino de 48 Vdc, pois ele é útil aos clientes que utilizam alarme com contato seco.

Utilize dois fios não blindados para conectar as entradas A e B, conforme recomendações a seguir.

1. Descasque o revestimento de plástico do fio até cerca de 6 mm;



Entrada de alarmes

2. Conecte o fio da tensão negativa (-48 Vdc) a uma das 12 posições B. Conecte a outra extremidade do fio a um dos contatos NO ou NC do dispositivo que irá gerar o evento de alarme;

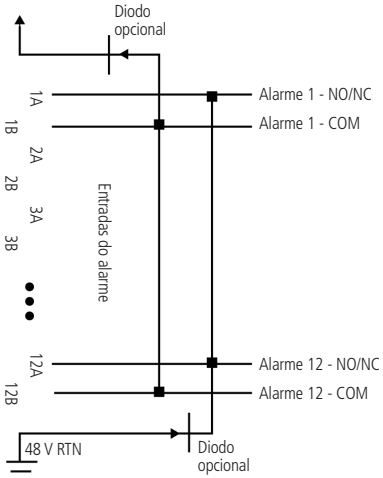


Diagrama da pinagem de entradas de alarme

3. Conecte o fio da tensão positiva (48 Vdc) à respectiva posição A e conecte a outra extremidade do fio ao respectivo contato COM do dispositivo que irá gerar o evento de alarme;
4. Após a conexão dos alarmes, é possível criar um modelo de envio de mensagens SNMP Trap quando uma condição de alarme ocorrer no dispositivo externo. Este modelo pode ser configurado através do comando *update num2str-profile*. O comando *update num2str-profile* segue o seguinte formato: *shelf/slot/282/posição-do-alarme.*

Adicione uma descrição para o primeiro contato do alarme, conforme o modelo a seguir:

```
iSH> update num2str-profile
Please provide the following: [q]uit.
name: ------->     {Relay 1}: cabinet door open
.............................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated
```

Observação: ao utilizar a alimentação de -48 V do alarme de entrada, verifique se os dispositivos estão desligados durante a inserção ou remoção do conector DB-26. Caso contrário, você poderá danificar o circuito de alarme ou os próprios dispositivos

A tabela a seguir exibe a pinagem do conector de entrada de alarmes.

Número do pino	Função	Número do pino	Função	Número do pino	Função
1	(–) BAT -48 Vdc	10	5A	19	9B
2	1A	11	5B	20	10A
3	1B	12	6A	21	10B
4	2A	13	6B	22	11A
5	2B	14	7A	23	11B
6	3A	15	7B	24	12A
7	3B	16	8A	25	12B
8	4A	17	8B	26	+48 V RTN/GND
9	4B	18	9A		

Pinos de entrada de alarme

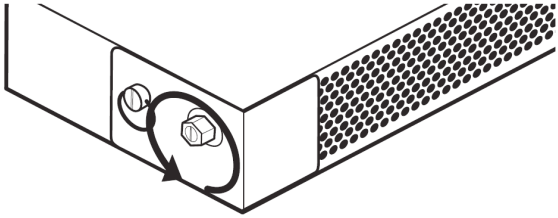
Sistema de ventilação removível

A OLT 8820 G possui um sistema de ventilação que pode ser removido através de um único slot hot swap.

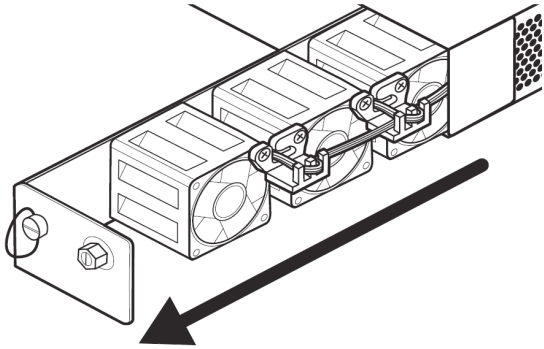
> ⚠ **Cuidado:** o produto não deve permanecer em funcionamento por um longo período sem o slot de ventilação

Removendo o slot de ventilação

1. Gire o parafuso de bloqueio no sentido anti-horário com uma chave de fenda para destravar o slot de ventilação;

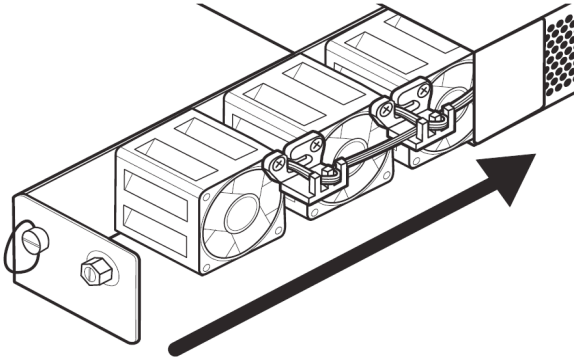


2. Puxe a alça para remover o slot de ventilação do gabinete da OLT. Por favor, aguarde até que a rotação dos ventiladores tenha terminado.

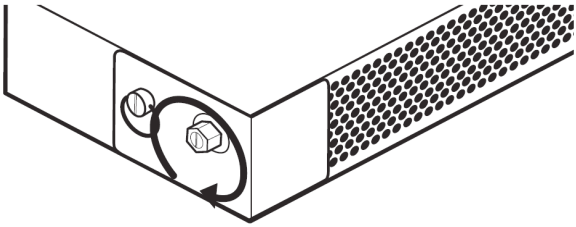


Inserindo o slot de ventilação

1. Para inserir o slot de ventilação, alinhe o slot e deslize-o para dentro do gabinete;

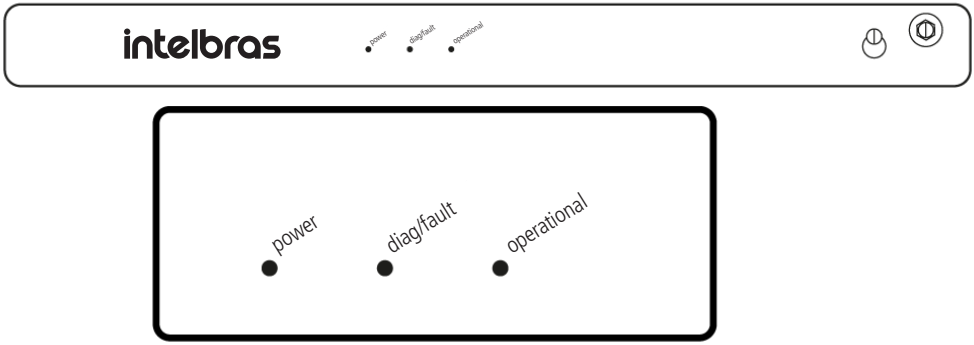


2. Gire o parafuso de bloqueio no sentido horário com uma chave de fenda para travar o slot de ventilação.



6.3. LEDs da OLT 8820 G

Os LEDs de monitoramento estão localizados no painel frontal da OLT, conforme imagem a seguir:



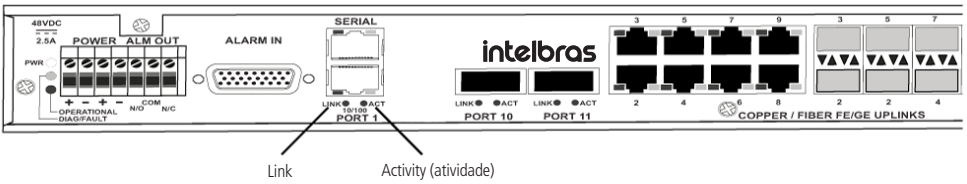
LEDs da OLT 8820 G

LED	Descrição
Power (verde)	Aceso: a tensão da OLT está dentro da faixa de tolerância. Apagado: a tensão da OLT não está operacional.
Diag/Fault (laranja)	Aceso: durante a alimentação inicial ou quando há um evento de alarme na OLT. Apagado: a OLT está operando normalmente.
Operational (verde)	Piscando: durante a iniciação da OLT. Aceso: a OLT está funcionando normalmente.

Descrição dos LEDs frontais da OLT 8820 G

Observação: um evento de alarme será emitido quando qualquer porta uplink estiver vaga ou desconectada, ocasionando o acendimento do LED Diag/Fault

LEDs das portas de gerenciamento

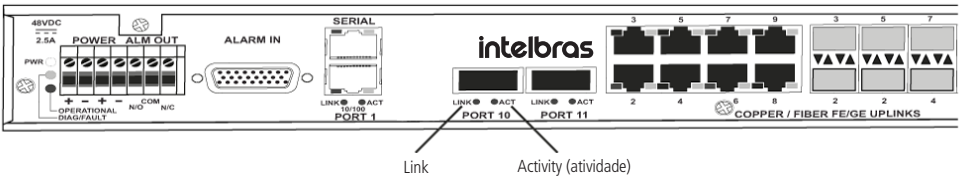


LEDs das portas de gerenciamento

LED	Cor/Comportamento	Descrição
Link	Verde/Acesa	O link está ativo
	Apagada	Sem link
Activity	Amarela/intermitente	Atividade no link
	Apagada	Sem atividade

Tabela com o comportamento dos LEDs de gerenciamento

LEDs das portas 10 GE

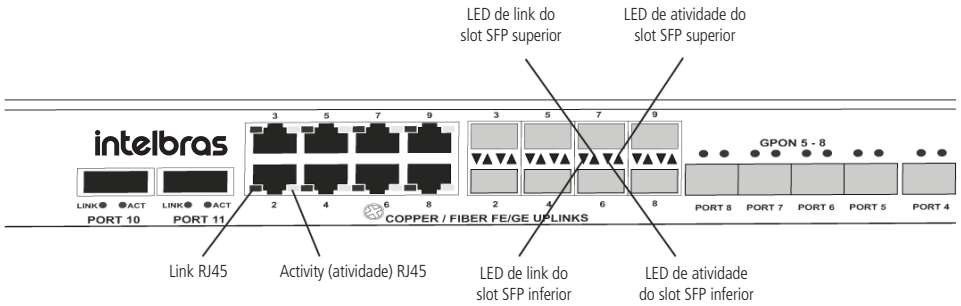


LEDs das portas 10 GE

LED	Cor/Comportamento	Descrição
Link	Verde/Acesa	O link está ativo
	Apagada	Sem link
Activity	Amarela/intermitente	Atividade no link
	Apagada	Sem atividade

Tabela com o comportamento dos LEDs 10 GE

LEDs das portas Gigabit Ethernet

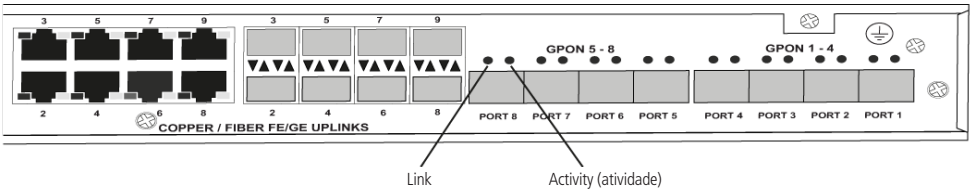


LEDs das portas Gigabit Ethernet

LED	Cor/Comportamento	Descrição
Link	Verde/Acesa	O link está ativo
	Apagada	Sem link
Activity	Amarela/intermitente	Atividade no link
	Apagada	Sem atividade

Tabela com o comportamento dos LEDs Gigabit Ethernet

LEDs das portas GPON



LEDs das portas GPON

LED	Cor/Comportamento	Descrição
Link	Verde/Acesa	O link está ativo
	Apagada	Sem link
Activity	Amarela/intermitente	Atividade no link
	Apagada	Sem atividade

Tabela com o comportamento dos LEDs GPON

6.4. Conexão dos cabos ópticos

Conexões da fibra óptica

Antes de fazer qualquer conexão, certifique-se de que os cabos ópticos e os componentes estejam limpos e sem poeira e detrito. Ao fazer uma conexão de fibra óptica, evite tocar nas extremidades do cabo de fibra óptica na parte externa do conector acoplado. Tocá-lo pode contaminar os conectores.

Gerenciamento de fibra óptica

Quando o gerenciamento das instalações de fibra são adequadamente planejadas, permite a manutenção ou substituição de qualquer subconjunto removível contida na solução sem ter de remover ou alterar a estrutura de suporte dos cabos usado durante a instalação original. A manutenção e o crescimento do sistema a longo prazo devem ser considerados durante a instalação da solução GPON.

Orientações de instalação da fibra óptica

Raio de curvatura de cabos de fibra óptica: um raio de curvatura mínimo de 30 mm é recomendado para garantir o desempenho especificado do sistema. Curvas acentuadas nos cabos de fibra óptica criam atenuação ou perda de sinal óptico indesejável.

Agrupamento de cabos de fibra óptica: conduítes enrolados em espiral flexíveis em diversos tamanhos são recomendados para controlar cabos de fibra óptica. Amarrações não são recomendadas para unir ou envolver cabos de fibra óptica. O conduíte enrolado em espiral pode ser mantido usando amarrações desde que a força de aperto da amarração não comprima o conduíte.

Separar cabos de cobre e cabos de fibra óptica é recomendado, pois a força de amarração usada para reter cabos de cobre é mais pesados do que sd fibras, podendo gerar perdas imprevisíveis de transmissão óptica.

7. Operação, administração e manutenção da OLT 8820 G

7.1. Acesso através da Interface de Linha de Comando (CLI)

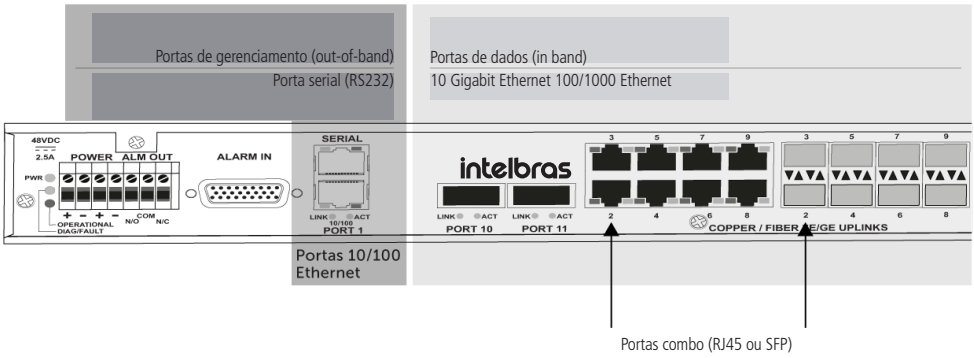
Visão geral de gerenciamento da OLT 8820 G

Você deve configurar uma interface de gerenciamento para acessar a OLT 8820 G, utilizando o terminal de linha de comando (CLI), interface web ou através de gerenciamento remoto.

Esta seção descreve como configurar e gerenciar as interfaces de gerenciamento da OLT 8820 G:

- » Porta Serial RS232 (gerenciamento out-of-band)
- » Porta 10/100 Ethernet (gerenciamento out-of-band)
- » Portas uplink 100/1000 Ethernet (gerenciamento in-band)
- » IP sobre bridge, em portas uplink 100/1000 Ethernet (gerenciamento in-band)

As portas Ethernet 10/100 e 100/1000 podem ser configuradas para gerenciamento através da CLI, adicionando um endereço de IP na porta física ou no uplink, TLS ou nas bridges de agregação de links.



Portas de gerenciamento da OLT 8820 G

Configuração padrão da OLT 8820 G

- » O nome de usuário é intelbras[1] e a senha é intelbras.
- » Por padrão, o profile *ip-interface-record* é automaticamente configurado na interface *1-1-1-0-eth/ip*. Esta interface é configurada com o endereço IP de gerenciamento 192.168.10.1/24 na porta 10/100 Ethernet.

> **Observação:** a interface 10/100BASE-T Ethernet recebe por padrão o endereço IP 192.168.10.1. Ao realizar o comando *set2default* sem a opção de restauração, o endereço IP volta para o padrão de fábrica

[1] Este usuário é referenciado em outros arquivos do sistema, e realizando a alteração, você poderá perder o acesso à OLT através deste usuário.

Gerenciamento out-of-band

Configuração da porta serial RS232 para gerenciamento out-of-band

A OLT 8820 G oferece uma interface serial RS232 para gerenciamento out-of-band. A porta serial da OLT 8820 G possui o profile *rs232-profile* com as seguintes configurações:

- » 9600 bps.
- » 8 bits de dados.
- » Sem paridade.
- » 1 bits de parada.
- » Sem controle de fluxo.

> **Dica:** as configurações da porta serial podem ser alteradas modificando o profile *rs232-profile*

Por padrão, é possível gerenciar a OLT 8820 abrindo uma sessão Telnet, SSH ou HTTP através do endereço IP 192.168.10.1 quando conectado através da porta de gerenciamento 10/100 Ethernet.

Observação: a OLT 8820 G suporta 11 sessões de gerenciamento simultaneamente, 5 sessões telnet, 5 sessões SSH e uma única sessão local através da porta serial

Configuração da porta serial RS232 para gerenciamento

Cuidado: a porta serial suporta as seguintes velocidades: 9600, 19200, 38400 e 57600. Não configure a velocidade da porta para um valor não suportado, podendo causar a perda de acesso a porta serial

Para atualizar o profile *rs232-profile* insira o seguinte comando:

```
iSH> update rs232-profile 1-1-1-0/rs232
rs232-profile       1-1-1-0/rs232
Please provide the following: [q]uit.
rs232PortInSpeed: ----------->       {9600}: 57600
rs232PortOutSpeed: ---------->       {9600}:
rs232PortInFlowType: -------->       {none}:
rs232PortOutFlowType: ------->       {none}:
rs232AsyncPortBits:---------->       {8}:
rs232AsyncPortStopBits:------>       {one}:
rs232AsyncPortParity: ------->       {none}:
rs232AsyncPortAutobaud: ----->       {disabled}:
.........................
Save changes? [s]ave, [c]hange or [q]uit: s
```

Configuração de uma interface IP na porta 10/100 BaseT Ethernet para gerenciamento out-of-band da OLT 8820 G

A OLT 8820 G possui uma única interface 10/100 BaseT full duplex (nomeada *ethernet1*) projetada para o gerenciamento da OLT.

Por padrão essa interface é configurada com o endereço IP 192.168.10.1/24. Conecte um PC (com endereço IP configurado na mesma sub-rede da OLT) na porta Ethernet 10/100 para gerenciar a OLT.

Cuidado: a interface Ethernet deve ser configurada antes de qualquer outras interfaces no sistema, mesmo se você não pretende gerenciar a OLT através da porta Ethernet

Observação: a OLT 8820 G possui os seguintes endereços IP reservados internamente:

Sub-rede	Range de endereços IPs
10.1.1.0/30	10.1.1.0 a 10.1.1.3
127.30.0.1/32	127.30.0.1

Os usuários devem evitar atribuir esses endereços IP para as interfaces, afim de evitar potenciais problemas de conflito de IP

Removendo o endereço IP padrão e configurando um novo endereço IP na interface 10/100 Ethernet

O endereço IP padrão pode ser substituído por um endereço IP designado pelo usuário.

1. Verifique o endereço IP existente;

```
iSH> interface show
1 interface
Interface        Status      Rd/Address              Media/Dest Address    IfName
1/1/1/0/ip       UP          1 192.168.10.1/24       00:01:47:85:b8:99     AutoConfig
```

2. Para alterar o endereço IP da interface 10/100 de gerenciamento, remova a interface e configure um novo endereço de IP.

Se o novo endereço IP de gerenciamento da OLT não estiver na mesma sub-rede que o PC, a conexão com a OLT será perdida. Altere o endereço IP do PC colocando na mesma sub-rede do novo endereço IP de gerenciamento da OLT para que a conexão com a OLT seja restabelecida.

O exemplo a seguir configura um novo endereço de IP para gerenciamento:

```
iSH> interface delete 1/1/1/0/ip
Delete complete

iSH> interface add 1-1-1-0/eth 10.55.1.161/24
Created ip-interface-record 1-1-1-0-eth/ip.
```

Verificação da interface

Use o comando *interface show* para verificar se a interface Ethernet foi configurada corretamente:

```
iSH> interface show
1 interface
Interface          Status   Rd/Address           Media/Dest Address   IfName
1/1/1/0/ip         UP       1 10.55.1.161/24     00:01:47:85:b8:99    1-1-1-0-eth
```

Definição da rota default

O exemplo a seguir cria uma rota default usando o gateway 10.55.1.254 com um custo 1 (um):

```
iSH> route add default 10.55.1.254 1
```

Verificação das rotas configuradas

Use o comando *route show* para verificar se as rotas foram adicionadas:

```
iSH> route show
Destination Routing Table
Dest                       Nexthop            Cost     Owner         Fallback
0.0.0.0/0                  10.55.1.254        1        STATICLOW
10.55.1.0/24               1/1/1/0/ip         1        LOCAL
```

Use o comando *ping* para verificar conectividade ao gateway padrão:

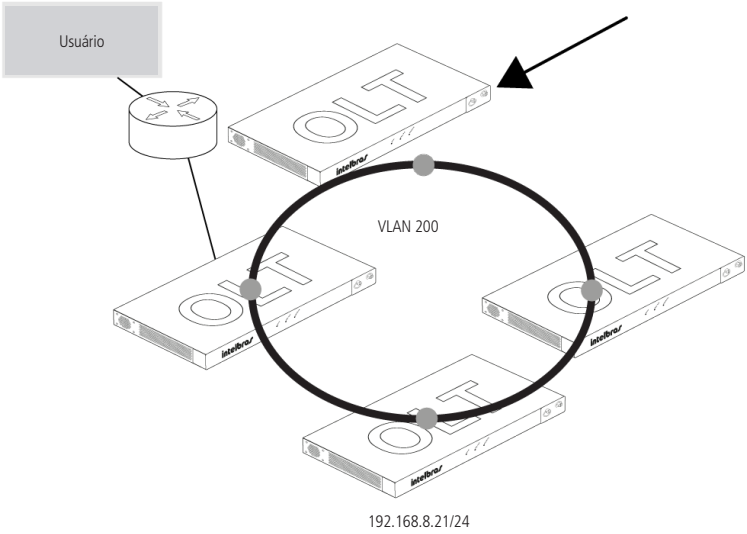
```
iSH> ping 10.55.1.254
PING 10.55.1.254: 64 data bytes
!!!!!
----10.55.1.254 PING Statistics----
5 packets transmitted, 5 packets
received round-trip (ms)    min/avg/max
= 0/1/5
```

Para parar o ping, pressione *CTRL+C*.

Gerenciamento in-band

Configuração IP sobre bridge para gerenciamento in-band da OLT

O IP sobre bridge permite que você insira um endereço IP em uma bridge VLAN para gerenciamento do dispositivo. Essa VLAN pode ser usada para gerenciar múltiplas OLT 8820 G. Cada OLT 8820 G suportar até seis IPs sobre bridge.



IP sobre bridge

Configuração de um endereço IP em uma porta uplink Ethernet para gerenciamento in-band

Configuração de um endereço IP em uma porta uplink Ethernet para gerenciamento in-band da OLT 8820 G.

Configuração de uma interface de gerenciamento in-band na porta uplink Ethernet

O exemplo a seguir configura o endereço IP para gerenciamento da OLT 8820 G em uma porta uplink Ethernet.

1. Configure uma porta uplink Ethernet para gerenciamento in-band;

```
iSH> interface add 1-1-2-0/eth vlan 200 192.168.8.21/24
Created ip-interface-record 1-1-2-0-eth-200/ip.
```

Verifique a interface.

```
iSH> interface show
2 interfaces
Interface        Status    Rd/Address             Media/Dest Address   IfName
1/1/1/0/ip       UP        1 10.55.1.161/24       00:01:47:85:b8:99    1-1-1-0-eth
1/1/2/0/ip       UP        1 192.168.8.21/24      00:01:47:85:b8:9a    1-1-2-0-eth-200
```

Removendo a interface IP de gerenciamento

1. Verifique a interface;

```
iSH> interface show
2 interfaces
Interface        Status    Rd/Address             Media/Dest Address   IfName
1/1/1/0/ip       UP        1 10.55.1.161/24       00:01:47:85:b8:99    1-1-1-0-eth
1/1/2/0/ip       UP        1 192.168.8.21/24      00:01:47:85:b8:9a    1-1-2-0-eth-200
```

2. Remova a interface IP de gerenciamento da OLT 8820 G.

```
iSH> interface delete 1-1-2-0-eth-200 vlan 200
Delete complete
```

Configuração TLS IP sobre bridge

> **Observação:** a interface da porta lógica para IP sobre bridge na OLT 8820 G deve ser obrigatoriamente *1-1-6-0/ipobridge* para a transmissão correta dos pacotes IP

Antes de configurar uma interface IP sobre bridge, crie uma bridge TLS ou uma bridge uplink. Se a bridge não existir, a mensagem de erro a seguir é exibida.

```
iSH> interface add 1-1-6-0/ipobridge vlan 200 192.168.123.21/24
Error: Couldn't determine type of IPOBRIDGE!
        Create an 'uplink' or 'tls' bridge(s) first.
```

Criação de IP sobre bridge em uma bridge TLS

Crie uma interface IP sobre bridge usando o endereço de IP 192.168.8.21/24 com interface de porta lógica 6 com VLAN 200.

1. Crie uma bridge TLS em uma interface uplink:

```
iSH> bridge add 1-1-4-0/eth tls vlan 200
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth/bridge
Bridge-path added successfully
```

2. Verifique a bridge:

```
      Orig
Type  VLAN/SLAN    VLAN/SLAN      Physical         Bridge                St      Table Data
tls                200            1/1/4/0/eth      1-1-4-0-eth/bridge    DWN
1 Bridge Interfaces displayed
```

3. Insira o comando *interface add* interface/type do tipo ipobridge:

```
iSH> interface add 1-1-6-0/ipobridge vlan 200 192.168.8.21/24
Created ip-interface-record ipobridge-200/ip.
```

O comando *interface add* cria uma bridge ipobridge tls com VLAN 200 com um endereço IP e uma bridge tls correspondente em uma porta Ethernet para gerenciamento do dispositivo.

4. Verifique a interface:

```
iSH> interface show
2 interfaces
Interface        Status    Rd/Address              Media/Dest Address     IfName
1/1/1/0/ip       UP        1 172.24.200.64/24      00:01:47:27:14:54      1-1-1-0-eth
1/1/6/0/ip       UP        1 192.168.8.21/24       00:01:47:27:14:54      ipobridge-200
```

5. Verifique a bridge tls em uma porta Ethernet criada pelo comando *interface add:*

```
iSH> bridge show
                 Orig
Type VLAN/SLAN   VLAN/SLAN    Physical             Bridge                 St Table Data
tls              Tagged 200   1/1/4/0/eth          1-1-4-0-eth/bridge     UP D 54:75:d0:1b:a6:4b
ipobtls          Tagged 200   1/1/6/0/ipobridge    ipobridge-200/bridge   UP S 00:01:47:85:b8:99
S 192.168.8.21
2 Bridge Interfaces displayed
```

6. Defina a rota default.

Configuração de IP sobre bridge em uma bridge uplink

Para criar um IP sobre bridge em uma bridge uplink, você deve criar a bridge uplink e em seguida adicionar a interface ipobridge. O comando *ipobridge* interface lê o perfil *bridge-path* que é criado com o comando bridge add, entende que uma bridge uplink é designada e a seguir cria um downlink *ipobridge.*

Criação de um IP sobre bridge para uma bridge uplink

Crie uma interface IP sobre bridge usando o endereço de IP 192.168.8.21/24 e uma interface de porta lógica 6 com VLAN 64.

1. Crie uma bridge uplink em uma interface uplink naVLAN 64;

```
iSH> bridge add 1-1-4-0/eth uplink vlan 64 tagged
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth-64/bridge
Bridge-path added successfully
```

2. Verifique a bridge de uplink:

```
iSH> bridge show
     Orig
Type VLAN/SLAN    VLAN/SLAN      Physical        Bridge                  St Table Data
upl               Tagged 64    1/1/4/0/eth    1-1-4-0-eth-64/bridge   UP S VLAN 64 default
1 Bridge Interfaces displayed
```

3. Adicione a interface ipobridge:

```
iSH> interface add 1-1-6-0/ipobridge vlan 64 192.168.8.21/24
Created ip-interface-record ipobridge-64/ip.
```

O comando *interface add* cria uma bridge ipobridge com VLAN 64 e um endereço IP.

4. Verifique a interface ipobridge:

```
iSH> interface show
2 interfaces
Interface          Status    Rd/Address               Media/Dest Address    IfName
1/1/1/0/ip         UP        1 192.168.254.205/24   00:01:47:27:14:87     1-1-1-0-eth
1/1/6/0/ip         UP        1 192.168.8.21/24      00:01:47:27:14:87     ipobridge-64
```

5. Verifique as bridges criadas por ipobridge:

```
iSH> bridge show
    Orig
Type VLAN/SLAN       VLAN/SLAN      Physical     Bridge                  St Table Data
upl        Tagged 64     1/1/4/0/eth            1-1-4-0-eth-64/bridge   UPS VLAN 64 default
ipobdwn    Tagged 64     1/1/6/0/ipobridge      ipobridge-64/bridge     UP S 00:01:47:b9:ef:24
                                                                         S 192.168.8.21
2 Bridge Interfaces displayed
```

Configuração de um linkagg IP sobre bridge

IP sobre bridge permite que você insira um endereço de IP sobre uma bridge VLAN em bridges TLS. Isso permite que VLANs possam ser usadas para gerenciar múltiplas OLTs 8820 G.

Criação de uma interface IP sobre bridge

Crie uma interface IP sobre bridge usando o endereço de IP 10.11.12.13/24 e uma VLAN 777. O exemplo a seguir exibe a criação de um IP sobre bridge.

> **Observação:** a interface da porta lógica para IP sobre bridge na OLT 8820 G deve ser obrigatoriamente *1-1-6-0/ipobridge* para a transmissão correta dos pacotes IP

1. Verifique o grupo *linkagg;*

```
iSH> linkagg show
LinkAggregations:
slot  unit   ifName      partner: Sys            Pri     grp ID   status    agg mode
1*    1      1-1-1-0     00:00:00:00:00:00       0x0     0x0      ACT       On
             links       slot    port    subport         status
             1-1-2-0     1       2       0               ACT
             1-1-3-0     1       3       0               ACT
```

2. Crie uma bridge TLS em um grupo linkagg que gerenciará o tráfego que passa para o grupo utilizando o comando *bridge add*, e a seguir verifique a bridge criada com o comando *bridge show*:

```
iSH> bridge add 1-1-1-0/linkagg tls vlan 777 tagged
Adding bridge on 1-1-1-0/linkagg
Created bridge-interface-record linkagg-1-1-777/bridge
Bridge-path added successfully
```

```
iSH> bridge show
          Orig
Type      VLAN/SLAN VLAN/SLAN    Physical          Bridge                    St Table Data
tls       Tagged 777             1/1/1/0/linkagg   linkagg-1-1-777/bridge    UP
1 Bridge Interfaces displayed
```

3. Insira o comando *interface add* interface/type com o tipo ipobridge:

```
iSH> interface add 1-1-6-0/ipobridge vlan 777 10.11.12.13/24
Created ip-interface-record ipobridge-777/ip.
```

Este comando cria a nova interface IP e uma nova bridge correspondente. A bridge criada será uma bridge TLS (Transparent LAN Service).

As portas 2 e 3 agora são alcançadas para upstream e o IP 10.11.12.13/24 pode chegar a outros dispositivos upstream na mesma VLAN.

Uma vez que as portas 2 e 3 da OLT 8820 G são membros de um grupo *linkagg*, a bridge TLS na VLAN 777 é automaticamente criada como uma bridge *linkagg.*

```
iSH> bridge show
          Orig
Type      VLAN/SLAN VLAN/SLAN Physical  Bridge                    St Table Data
tls       Tagged 777 1/1/1/0/linkagg    linkagg-1-1-777/bridge    UP
ipobtls   Tagged 777 1/1/6/0/ipobridge  ipobridge-777/bridge      UP S 00:01:47:85:b8:99
                                                                    S 10.11.12.13
2 Bridge Interfaces displayed
```

4. Insira o comando *interface show* para verificar a interface IP e o comando *bridge show* para verificar a bridge:

```
iSH> interface show
2 interfaces
Interface         Status     Rd/Address              Media/Dest Address  IfName
1/1/1/0/ip        UP         1 192.168.254.207/24    00:01:47:27:14:85   1-1-1-0-eth
1/1/6/0/ip        UP         1 10.11.12.13/24        00:01:47:27:14:85   ipobridge-777
```

Removendo IP sobre bridge

Remova a interface IP sobre bridge e a bridge TLS na mesma VLAN quando necessário.

1. Para remover a interface IP sobre bridge:

```
iSH> interface delete 1/1/6/0/ip
Delete complete
```

A interface IP sobre bridge é removido, assim como a interface *ipobridge*.

```
iSH> interface show
1 interface
Interface     Status  Rd/Address           Media/Dest Address                      IfName
1/1/1/0/ip    UP      1 192.168.254.207/24 192.168.254.207/24 00:01:47:27:14:85    1-1-1-0-eth
```

Quando a interface IP é removida, a *ipobridge* também é.

```
iSH> bridge show
                Orig
Type VLAN/SLAN  VLAN/SLAN     Physical           Bridge                  St Table Data
tls             Tagged 777    1/1/1/0/linkagg    linkagg-1-1-777/bridge  UP
1 Bridge Interfaces displayed
```

2. Para remover a bridge TLS *linkagg* na VLAN 777.

```
iSH> bridge delete linkagg-1-1-777/bridge vlan 777
Bridge-path deleted successfully linkagg-1-1-
777/bridge delete complete
```

A interface IP sobre bridge não suporta SNMP.

7.2. Acesso através da interface web

A OLT 8820 G permite configuração de gerenciamento através de uma Interface Web.

Interface web

Para gerenciar a OLT 8820 G usando a Interface Web:

» **Endereço IP padrão**

Para acessar o dispositivo através da Interface Web utilizando o endereço IP padrão do dispositivo, deve-se configurar o endereço de IP no PC para qualquer endereço na sub-rede 192.168.10.0, exceto 192.168.10.1. O endereço IP 192.168.10.1 é usado como o endereço padrão da Interface Web.

» **Interface IP configurada**

Para acessar o dispositivo através da Interface Web através de um endereço IP diferente do endereço IP padrão, conecte-se diretamente ao dispositivo usando a porta console.

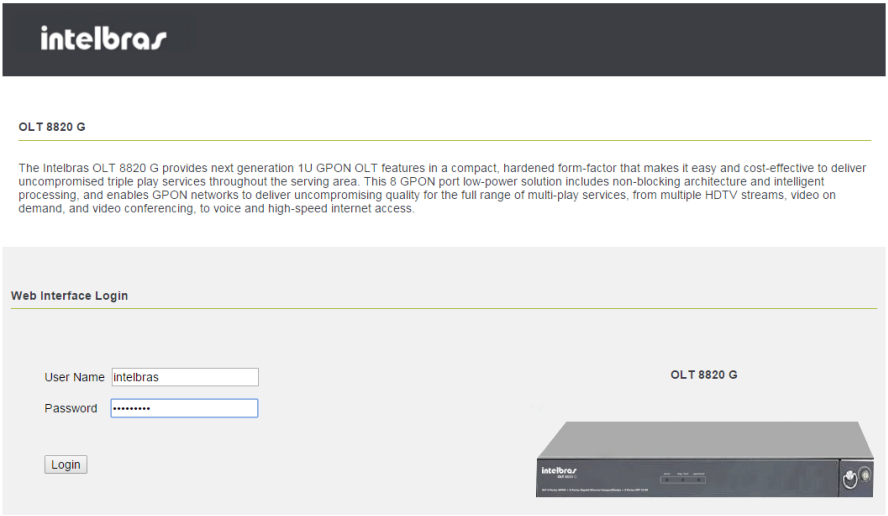
Remova o endereço de IP padrão e adicione o endereço IP desejado. Se o novo endereço de IP não estiver na mesma sub-rede do endereço IP do PC a conexão com a OLT será perdida. Altere o endereço IP do PC para estar na mesma sub-rede do novo endereço IP configurado para a OLT.

```
iSH> delete ip-interface-record AutoConfig/ip
iSH> interface add 1-1-2-0/eth vlan 94 172.24.94.103/24
Created ip-interface-record ethernet2-94/ip
iSH> route add default 172.24.94.254 1
```

A partir de um PC conectado à porta 10/100 da OLT 8820 G, certifique-se de que o endereço de IP do PC esteja na mesma sub-rede do endereço IP da OLT 8820 G. Por padrão, o endereço IP 192.168.10.1 é atribuído à porta Ethernet 10/100 (*1-1-1-0/eth*).

Para acessar a Interface Web, insira o endereço IP da OLT no navegador, logo após será exibida a página de login da OLT 8820 G.

> ☑ **Observação:** a Interface Web somente suporta navegadores Internet Explorer e Mozilla



Tela de login da interface web

Na página de Login, insira o nome de usuário e a senha. O nome de usuário padrão é *intelbras* e a senha padrão é *intelbras.*

Clique no menu desejado para exibir as opções de gerenciamento. Para uma página de ajuda, clique no ícone ⓘ ou no título do produto em qualquer janela.

7.3. Login na porta serial

A OLT 8820 G oferece uma interface serial RS232 out-of-band para gerenciamento. A interface serial possui a seguinte configuração padrão:

- 9600 bps.
- 8 bits de dados.
- Sem paridade.
- 1 bits de parada.
- Sem controle de fluxo.

> **Dica:** as configurações da porta serial podem ser alteradas modificando o profile *rs232-profile*

Por padrão, é possível gerenciar a OLT 8820 abrindo uma sessão Telnet, SSH ou HTTP através do endereço IP 192.168.10.1 quando conectado através da porta de gerenciamento 10/ 100 Ethernet.

> **Observação:** a OLT 8820 G suporta 11 sessões de gerenciamento simultaneamente, 5 sessões telnet, 5 sessões SSH e uma única sessão local através da porta serial

Login e logout na OLT

Para realizar login na OLT (nome de usuário padrão é *intelbras* e a senha padrão é *intelbras*).

```
login:intelbras
password:
iSH>
```

Para fazer logout na OLT, insira o comando *logout*:

```
iSH> logout
```

> **Dica:** a OLT faz o logout automaticamente após um período de inatividade. O tempo de logout padrão é 10 minutos, mas isso pode ser alterado com o comando *timeout*

Habilitar e desabilitar o sistema de log

Por padrão, o login é habilitado na porta serial e desabilitado nas sessões telnet e SSH. Para habilitar ou desabilitar o log para a sessão, use o comando a seguir:

```
iSH> log session off | on
```

O comando *log session* é aplicável somente à sessão atual. Você também pode habilitar ou desabilitar o log para todas as sessões da porta serial usando o comando a seguir:

```
iSH> log serial on | off
```

A configuração deste comando persiste nas reinicializações da OLT.

7.4. Administração da OLT 8820 G

Obs.: *todos os níveis de acesso definidos pelo parâmetro* access level, *agora possuem os mesmos acessos disponíveis na CLI do equipamento, ou seja, não há mais distinção entre os níveis de acesso definidos no parâmetro access level. Por conta disso, recomenda-se que seja setado somente o nível admin na criação de novos usuários.*

Contas de usuários

É possível configurar contas de usuários para o acesso ao terminal de linha de comando (CLI) da OLT 8820 G para a realização de configurações e gerencia do sistema.

Comando user

O comando user possibilita adicionar, modificar, exibir ou remover contas de usuários da interface CLI.

Sintaxe

```
user add <user-name> [password password] [prompt prompt] [admin] [debug]
[voice] [data] [manuf] [dbase] [systems] [tools] [useradmin] [all]
user modify <user-name> [password password] [prompt prompt] [admin]
[voice] [data] [manuf] [dbase] [systems] [tools]
[useradmin] [all]
user delete <user-name>
user show [<user-name>]
```

Comando user:

- **add**
  Adiciona um novo usuário com as configurações especificadas.
- **username**
  Nome da conta de usuário.
- **password password**
  Especifica a senha atribuída a esse usuário. Caso a senha tenha caracteres especiais, deve-se inserir a senha entre aspas.
- **prompt**
  Especifica o prompt do sistema exibido ao usuário.
- **access level**
  Especifica os níveis de acesso atribuídos ao usuário. A opção *all* determina todos os níveis de acesso. Níveis de acesso individuais podem ser especificados adicionando a palavra chave true ou false depois de um nível de acesso. Por exemplo, *manuf false all true* determina todos os níveis de acesso, exceto o nível manuf.
- **Exemplo 1**

```
iSH> user add paulo password 123 prompt "iSH >" admin voice systems dbase
User record saved.
.............................
User name:(paulo) User prompt:(iSH >)
Access Levels: (admin)(voice)(system)(dbase)
```

- **Exemplo 2**

```
iSH> user modify paulo password 123 all false admin true
OK to modify this account? [yes] or [no]: yes
```

```
User record updated.
.................................
User name:(paulo) User prompt:(iSH>)
Access Levels: (admin)
```

» **Exemplo 3**

```
iSH> user show
.................................
User name:(intelbras) User prompt:(iSH>)
Access Levels: (admin)(voice)(data)(manuf)(database)(systems)(tool)(useradmin)
.................................
User name:(paulo) User prompt:(iSH>)
Access Levels: (admin)(voice)(systems)(dbase)
.................................
User name:(joao) User prompt:(test4 >)
Access Levels: (admin)debug(voice)(data)(manuf)(database)(systems)(tool)(useradmin)
```

» **Exemplo 4**

```
iSH> user show paulo
.................................
User name:(paulo) User prompt:(iSH>)
Access Levels: (admin)(voice)(systems)(dbase)
```

» **Exemplo 5**

```
iSH> user delete paulo
OK to delete this account? [yes] or [no]: yes
Account paulo deleted
```

» **Comando adduser**

Cada usuário administrativo do sistema deve ter uma conta de usuário. A conta especifica o nome do usuário e senha, assim como o seu nível de privilégio, determinando seu acesso aos comandos.

Usuários com privilégios *admin* têm acesso a todos os comandos administrativos. Usuários com privilégios user possuem acesso a um conjunto limitado de comandos. O maior nível de acesso é *useradmin*, que possibilita a criação de contas de usuários.

Para adicionar uma conta de usuário, insira o seguinte comando:

```
iSH> adduser
Please provide the following: [q]uit.
User Name: matias
User Prompt[iSH>]:
Please select user access levels.
admin: ---------->  {no}: yes
voice: ---------->  {no}:
data: ---------->  {no}:
manuf: ---------->  {no}:
database: ------>  {no}:
systems: ------->  {no}:
tool: ---------->  {no}:
useradmin: ----->  {no}: yes
.................................
User name:(matias) User prompt:(iSH>)
Access Levels:
(admin)(useradmin)
Save new account? [s]ave, [c]hange or [q]uit: s
User record saved.
TEMPORARY PASSWORD: hmj4OLTFU
```

Imediatamente após a ativação da conta do usuário, deve-se alterar a senha que foi inserida automaticamente pelo sistema, conforme exido no comando anterior *TEMPORARY PASSWORD: hmj4OLTFU.*

Alterando a senha padrão dos usuários

Ao adicionar uma conta de usuários, o sistema atribui automaticamente a senha para cada usuário. A maioria dos usuários desejam alterar sua senha. O comando *changepass* altera a senha da conta do usuário que está atualmente logado no sistema. A seguir temos um exemplo de alteração de senha:

```
iSH> changepass
Current Password: senha_atual
New password: nova_senha
Confirm New Password: nova_senha
Password change successful.
```

Removendo usuários

Para remover uma conta de usuário, insira o comando *deleteuser* e especifique o nome do usuário:

```
iSH> deleteuser joao
OK to delete this account? [yes] or [no]: yes
User record deleted.
```

Removendo a conta do admin

Além de remover contas de usuários comuns, também é possível remover a conta do usuário *admin*. Essa conta é criada automaticamente pelo sistema e fornece acesso total ao CLI.

> **Observação:** não será possível excluir a conta com permissão *admin* (ou *useradmin*) se a conta estiver em utilização

Para remover a conta do usuário com permissão *admin*, insira o comando *deleteuser* e especifique o nome do usuário:

```
iSH> deleteuser intelbras
```

Se desejar, é possível criar novamente uma conta com o nome intelbras após deletá-la:

```
iSH> adduser
Please provide the following: [q]uit.
User Name: intelbras
User Prompt[iSH>]:

Please select user access levels.
admin: ----------> {no}: yes
voice: ----------> {no}: yes
data: -----------> {no}: yes
manuf: ----------> {no}: yes
database: -------> {no}: yes
systems: --------> {no}: yes
tool: -----------> {no}: yes
useradmin: ----->  {no}: yes
.................................
User name:(intelbras) User prompt:(iSH>)
Access Levels:
(admin)(voice)(data)(manuf)(database)(systems)(tools)(useradmin)  Save new account? [s]ave, [c]
hange or [q]uit: s
User record saved.
TEMPORARY PASSWORD: hmj4OLTFU
```

Redefinir senhas

Caso algum usuário esquecer a senha, um usuário com privilégio *admin* poderá redefinir a senha utilizando o comando *resetpass*, como no exemplo a seguir:

```
iSH> resetpass matias
User record updated.
UserName: matias, Password: rgbsm8mm
Password change successful.
```

Navegação no sistema de arquivos da OLT 8820 G

Use os comandos a seguir para acessar o sistema de arquivos da OLT 8820 G:

- **cd:** altera o diretório.
- **dir:** lista os conteúdos do diretório.
- **pwd:** exibe o caminho do diretório de trabalho atual.

Use os comandos *cd, dir* e *pwd* para listar os conteúdos do sistema de arquivos, como no exemplo a seguir:

O cartão de memória flash contém um sistema de arquivos DOS que armazena o código de inicialização do sistema, imagens do software e configuração. Durante a inicialização do sistema, a imagem do software é descomprimida do cartão e carregada na memória do sistema.

Alterar o diretório.

```
iSH> cd /card1
```

Listar o diretório corrente.

```
iSH> dir
Listing Directory .:
drwxrwxrwx 1  0 0 4096      Dec    27    1990     bulkstats/
drwxrwxrwx 1  0 0 4096      Apr    8     03:06    datastor/
drwxrwxrwx 1  0 0 4096      Apr    8     03:06    log/
drwxrwxrwx 1  0 0 4096      Jan    1     1980     odm/
drwxrwxrwx 1  0 0 4096      Mar    19    13:37    onreboot/
drwxrwxrwx 1  0 0 4096      Dec    27    1990     pub/
-rwxrwxrwx 1  0 0 220       Mar    19    13:44    banner.txt
-rwxrwxrwx 1  0 0 1124      Mar    19    13:44    logo.txt
-rwxrwxrwx 1  0 0 11931199  Mar    26    23:31    mx1u19x.bin
-rwxrwxrwx 1  0 0 8495616   Jan    1     1980     mx1u19x_http.tar
-rwxrwxrwx 1  0 0 18612244  Mar    21    12:00    ont142xg-0301219.img
-rwxrwxrwx 1  0 0 3277312   Mar    21    12:00    onu110g-1125543.img
     139559860 bytes available
```

Comandos básicos para administração da OLT 8820 G

Comando list

O comando *list* exibe todos os perfis disponíveis na OLT 8820 G (lista parcial exibida):

```
iSH> list
alarm-config: ifIndex
analog-fxs-cfg-profile: ifIndex
analog-fxs-status-profile: ifIndex
analog-if-cfg-profile: ifIndex
analog-if-non-per-profile: ifIndex
analog-if-status: ifIndex
bridge-interface-record: ifIndex bulk-statistic: index
bulk-statistics-config: index
card-profile: shelf/slot/cardType
community-access-profile: community
```

```
community-profile: community
cpe-mgr-global: index
description: descriptionIndex
device-codecs: index/codecType
dhcp-client-lease-resource: shelf/slot/interfaceNum
dhcp-client-resource: shelf/slot
dhcp-server-group: index
dhcp-server-host: index
```

O comando *list bridge-interface-record* lista todos os perfis de bridge do sistema.

```
iSH> list bridge-interface-record
bridge-interface-record     1-1-2-0-eth-200/bridge
1 entry found.
```

O comando *list system* exibe a lista de perfis do sistema.

```
iSH> list system
system    0
1 entry found.
```

Para visualizar o tipo de dispositivo, insira list *card-profile:*

```
iSH> list card-profile
card-profile        1/1/10300
1 entry found.
```

Comando show

Use o comando *show* para visualizar todas as opções em um perfil. Por exemplo, se você precisa saber quais códigos de países estão disponíveis na OLT 8820 G, use o comando *show system*.

```
iSH> show system
syscontact:------------> {260}
sysname:--------------> {260}
syslocation:----------> {260}
enableauthtraps:------>  enabled     disabled
setserialno:----------> {0 - 2147483647}
zmsexists:------------> true     false
zmsconnectionstatus:--> active     inactive
zmsipaddress:---------> {0 - 0}
configsyncexists:-------> true     false
configsyncoverflow:-----> true     false
configsyncpriority:----> none     low     medium     high
configsyncaction:------> noaction     createlist     createfulllist
configsyncfilename:-----> {68}
configsyncstatus:------->  synccomplete  syncpending  syncerror  syncinitializing
configsyncuser:--------> {36}
configsyncpasswd:------> {36}
numshelves:-----------> {0 - 0}
shelvesarray:---------> {36}
numcards:-------------> {0 - 0}
ipaddress:------------> {0 - 0}
alternateipaddress:---> {0 - 0}
countryregion:--------> argentina australia belgium china costarica finland france germany
hongkong italy japan korea mexico netherlands newzealand singapore spain sweden switzerland uk
us afghanistan albania algeria americansamoa andorra angola anguilla antarctica antiguabarbuda
armenia aruba austria azerbaijan bahamas bahrain bangladesh barbados belarus belize benin bermuda
```

```
bhutan bolivia bosniaherzegovina botswana bouvetisland brazil britishindianoceanterritory
bruneidarussalam bulgaria burkinafaso burundi cambodia cameroon canada capeverde caymanislands
centralafricanrepublic chad chile christmasisland cocosislands colombia comoros congo cookislands
cotedivoire croatia cuba cyprus czechrepublic denmark djibouti dominica dominicanrepublic
easttimor ecuador egypt elsalvador equatorialguinea eritrea estonia ethiopia falklandislands
faroeislands fiji frenchguiana frenchpolynesia frenchsouthernterritories gabon gambia georgia ghana
gibraltar greece greenland grenada guadeloupe guam guatemala guinea guineabissau guyana haiti
heardislandmcdonaldislands holysee honduras hungary iceland india indonesia iran iraq ireland
israel jamaica jordan kazakstan kenya kiribati northkorea kuwait kyrgyzstan lao latvia lebanon
lesotho liberia libyanarabjamahiriya liechtenstein lithuania luxembourg macau macedonia madagascar
malawi malaysia maldives mali malta marshallislands martinique mauritania mauritius mayotte
micronesia moldova monaco mongolia montserrat morocco mozambique myanmar namibia nauru nepal
netherlandsantilles newcaledonia nicaragua niger nigeria niue norfolkisland northernmarianaislands
norway oman pakistan palau palestinianterritory panama papuanewguinea paraguay peru philippines
pitcairn poland portugal puertorico qatar reunion romania russia rwanda sainthelena saintkittsnevis
saintlucia saintpierremiquelon saintvincentthegrenadines samoa sanmarino saotomeprincipe
saudiarabia senegal seychelles sierraleone slovakia slovenia solomonislands somalia southafrica
southgeorgia srilanka sudan suriname svalbardjanmayen swaziland syria taiwan tajikistan tanzania
thailand togo tokelau tonga trinidadtobago tunisia turkey turkmenistan turkscaicosislands
uganda ukraine unitedarabemirates uruguay uzbekistan vanuatu venezuela vietnam virginislandsuk
virginislandsus wallisfutuna westernsahara yemen yugoslavia zambia zimbabwe
primaryclocksource:---> [Shelf {0-255}/Slot {0-1}/Port {0-500}/SubPort/Type] |[Name/Type]
ringsource:-----------> internalringsourcelabel externalringsourcelabel
revertiveclocksource:-> true     false
voicebandwidthcheck:--> true     false
alarm-levels-enabled:-> critical+major+minor+warning
userauthmode:---------> local     radius     radiusthenlocal     radiusthencraft
radiusauthindex:------> {0 - 2147483647}
secure:---------------> enabled disabled
webinterface:---------> enabled disabled
options:--------------> cvlanonly+nol3bridgetable+ipg88bits+disdefpktrules+enablexcardlinkag
g+fiberlan
reservedVlanIdStart:--> {0 - 4090}
reservedVlanIdCount:--> {0 - 2048}
```

Use o comando show para exibição de informações adicionais, como por exemplo *show bridge-interface-record* para visualizar mais detalhes sobre as bridges.

```
iSH> show bridge-interface-record
vpi:------------------------------------>      {0 - 4095}
vci:------------------------------------>      {0 - 65535}
vlanId:---------------------------------->      {0 - 4094}
stripAndInsert:-------------------------->      false     true
customARP:------------------------------->      false     true
filterBroadcast:------------------------->      false     true
learnIp:--------------------------------->      false    true
learnUnicast:---------------------------->      false     true
maxUnicast:------------------------------>      {0 - 2147483647}
learnMulticast:-------------------------->      false     true
forwardToUnicast:------------------------>      false     true
forwardToMulticast:---------------------->      false      true
forwardToDefault:------------------------>      false     true
bridgeIfCustomDHCP:---------------------->      false     true
bridgeIfIngressPacketRuleGroupIndex:---->      {0 - 2147483647}
vlanIdCOS:------------------------------->      {0 - 7}
outgoingCOSOption:----------------------->      disable  all
outgoingCOSValue:------------------------>      {0 - 7}
s-tagTPID:------------------------------->      {33024 - 37376}
```

```
s-tagId:-------------------------------->      {0 - 4094}
s-tagStripAndInsert:--------------------->      false     true
s-tagOutgoingCOSOption:------------------>      s-tagdisable       s-tagall
s-tagIdCOS:------------------------------>      {0 - 7}
s-tagOutgoingCOSValue:-------------------->     {0 - 7}
mcastControlList:------------------------>      {264}
maxVideoStreams:------------------------->      {0 - 210}
isPPPoA:--------------------------------->      false     true
floodUnknown:----------------------------->     false     true
floodMulticast:--------------------------->     false     true
bridgeIfEgressPacketRuleGroupIndex:------>      {0 - 2147483647}
bridgeIfTableBasedFilter:----------------->     none+mac+ip
bridgeIfDhcpLearn:------------------------>     none+mac+ip
mvrVlan:---------------------------------->     {0 - 4094}
vlan-xlate-from:-------------------------->     {0 - 4095}
slan-xlate-from:-------------------------->     {0 - 4095}
bridge-type:------------------------------>      uplink  downlink  intralink tls  rlink  pppoa  wire
mvr  user  downlinkvideo  downlinkdata  downlinkpppoe  downlinkp2p  downlinkvoice  downlinkupstreammcast
ipobtls  ipobuplink  ipobdownlink
```

Comando get

Use o comando *get* para visualizar a configuração atual dos perfis. O comando *get system 0* exibe informações sobre a configuração atual da OLT 8820 G.

```
iSH> get system 0
system    0
syscontact: ------------------>      {}
sysname: --------------------->      {}
syslocation: ----------------->      {}
enableauthtraps: ------------->      {disabled}
setserialno: ----------------->      {0}
zmsexists: ------------------->      {false}
msconnectionstatus: ---------->      {inactive}
zmsipaddress: ---------------->      {0.0.0.0}
configsyncexists: ------------>      {false}
configsyncoverflow: ----------->      {false}
configsyncpriority: ----------->      {high}
configsyncaction: ------------>      {noaction}
configsyncfilename: ----------->      {}
configsyncstatus: ------------>      {syncinitializing}
configsyncuser: --------------->      {}
configsyncpasswd: ------------>      ** private **
numshelves: ------------------>      {1}
shelvesarray: ---------------->      {}
numcards: --------------------->      {1}
ipaddress: -------------------->      {192.168.10.1}
alternateipaddress: ---------->      {0.0.0.0}
countryregion: --------------->      {us}
primaryclocksource: ---------->      {0/0/0/0/0}
ringsource: ------------------>      {internalringsourcelabel}
revertiveclocksource: -------->      {true}
voicebandwidthcheck: --------->      {false}
alarm-levels-enabled: -------->      {critical+major+minor+warning}
```

```
userauthmode: --------------->      {local}
radiusauthindex: ------------>      {0}
secure: ---------------------->      {disabled}
webinterface: ---------------->      {enabled}
options: ---------------------->      {NONE(0)}
reservedVlanIdStart: -------->      {0}
reservedVlanIdCount: -------->      {0}
```

Comando update

Para atualizar o perfil *system 0* e todos os outros perfis, use o comando *update*. O comando *update system 0* modificará através de interações campo por campo do perfil.

> ⚠ **Cuidado:** você deve ter muito cuidado ao alterar os perfis, modifique apenas campos conhecidos e necessários

Por exemplo:

```
iSH> update system 0
system   0
Please provide the following: [q]uit.
syscontact: ------------>      {}:
sysname: ---------------->      {}:
syslocation: ------------>      {}:
enableauthtraps: ------->      {disabled}:
setserialno: ------------>      {0}:
zmsexists: ------------->      {true}: false
...
...
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Comando interface show

O comando *interface show* exibe as interfaces IP "numbered" ou "unnumbered (flutuantes)" disponíveis atualmente na OLT 8820 G.

```
iSH> interface show
1 interface
Interface         Status   Rd/Address          Media/Dest Address    IfName
1/1/1/0/ip        UP       1 10.55.1.161/24    00:01:47:85:b8:99     1-1-1-0-eth
```

Coluna	Descrição
Interface	Exibe a interface física da interface IP
Status	Exibe se a interface está ativa ou inativa
Rd/Address	Endereço IP atribuído a este gateway
Media/Dest Address	Media/Dest Address é o endereço MAC de um dispositivo
IfName	Nome da interface

Coluna interface show

Comando bridge show

O comando *bridge show* exibe as bridge interfaces na OLT 8820 G. Uma bridge é uma combinação de bridges interfaces trabalhando juntas.

```
iSH> bridge show
          Orig
Type      VLAN/SLAN VLAN/SLAN     Physical      Bridge                    St Table Data
upl       Tagged 200              1/1/2/0/eth   1-1-2-0-eth-200/bridge    UP S VLAN 200 default
1 Bridge Interfaces displayed
```

Use o comando *bridge show* com um VLAN ID para visualizar todas as bridges na VLAN determinada.

```
iSH> bridge show vlan 200
          Orig
Type      VLAN/SLAN VLAN/SLAN      Physical       Bridge                    St Table Data
upl       Tagged 200               1/1/2/0/eth    1-1-2-0-eth-200/bridge    UP S VLAN 200 default
1 Bridge Interfaces displayed
```

7.5. Comandos: bridge stats

Você pode usar o comando bridge stats para visualizar os pacotes transmitidos ou recebidos em uma bridge interface. Ao adicionar o nome de uma bridge você pode ver as estatísticas da referida bridge.

As estatísticas de entrada e saída de pacotes das bridge são habilitadas por padrão.

```
iSH> bridge stats
Interface                Received Packets          Transmitted Packets Storm Detect Packets        Byte Counters
Name                  UCast  MCast  BCast  UCast  MCast  Bcast  Error  Ucast  Mcast  Bcast  Alarm Received Transmitted
1-1-4-0-eth-64/bridge   -      -     682     0      0      0      0      0      0      0      0       -        -
1-1-10-0-eth/bridge     -      -      -      0      0      0     682     0      0      0      0       -        -
1-1-2-0-eth-0-502/bridge -     -     682     0      2      0      0      0      0      0      0       -        -
```

SNMP

Criar nomes de comunidade SNMP e listas de acesso

O perfil *community-profile* especifica o nome da comunidade e um nível de acesso para que o gerenciador SNMP acesse o sistema da OLT. Ele também pode opcionalmente especificar um *community-access-profile*, que é usado para verificar o endereço IP de origem do Gerenciador SNMP. O sistema suporta até 50 listas de acesso diferentes.

Os seguintes níveis de acesso de comunidade são suportados:

- **noaccess:** a comunidade não possui acesso.
- **read:** a comunidade somente possui aesso de leitura ao sistema, com exceção das informações contidas em *community-profile* e *community-access-profile*.
- **readandwrite:** a comunidade tem acesso de leitura/escrita ao sistema, com exceção das informações contidas em *community-profile* e *community-access-profile*.
- **admin:** a comunidade possui acesso de leitura/escritura em todo o sistema, incluindo informações contidas em *community-profile* e *community-access-profile*.

Criar um perfil de comunidade

O exemplo a seguir define uma comunidade *public* com privilégios somente de leitura:

```
iSH> new community-profile 1
Please provide the following: [q]uit.
community-name: ----->     {}: public
permissions: ------------>     {read}:
access-table-index: ---->     {0}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Criar listas de acesso à comunidade SNMP

O exemplo a seguir define um nome de comunidade *private* com privilégios de leitura/escritura e também cria uma lista de acesso para verificar que os gerenciadores SNMP estão acessando a OLT através dos endereços IP conhecidos 192.168.9.10 e 192.168.11.12:

1. Primeiramente, crie uma lista de acesso para o primeiro endereço IP:

```
iSH> new community-access-profile 2
Please provide the following: [q]uit.
access-table-index: ---->     {0}: 1
```

```
ip-address: ------------>     {0.0.0.0}: 192.168.9.10
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

2. A seguir, crie uma lista de acesso para o segundo endereço IP com o mesmo *access-table-index (1):*

```
iSH> new community-access-profile 3
Please provide the following: [q]uit.
access-table-index: ---->     {0}: 1
ip-address: ------------>     {0.0.0.0}: 192.168.11.12
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Por fim, crie um *community-profile* que especifique o nome da comunidade e use o mesmo *access-table-index* (1) conforme definido nos dois *community-access-profiles* que você acabou de criar:

```
iSH> new community-profile 4
Please provide the following: [q]uit.
community-name: ----->     {}: private
permissions: ------------>     {read}: readandwrite
access-table-index: ---->     {0}: 1
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Configuração de traps SNMP

O perfil *trap-destination* define um receptor de traps na qual a OLT 8820 G enviará traps SNMP. Para configurar um receptor de trap, você deve saber as seguintes informações:

- » O endereço IP da estação de trabalho do gerenciador SNMP
- » O nome da comunidade que o receptor de trap está configurado

Observe que os parâmetros *resendseqno* e *ackedseqno* são definidos pela OLT. Os outros parâmetros no perfil *trap-destination* podem ser deixados em seus valores padrão. O exemplo a seguir configura um receptor de trap com o endereço de IP 192.168.3.21:

```
iSH> new trap-destination 32
Please provide the following: [q]uit.
trapdestination: --------->     {0.0.0.0}: 192.168.3.21
communityname: ------------>     {}: public
resendseqno: ------------->     {0}:
ackedseqno: --------------->     {0}:
traplevel: ---------------->     {low}:
traptype: ----------------->     {(null)}: 0
trapadminstatus: ---------->     {enabled}:
gatewaytrapserveraddr:---->     {36}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

7.6. Administração das portas

Visão geral do comando port

O comando port possui diversas funções administrativas e é usado para:

- » Alterar o status administrativo de uma porta física ou de uma interface virtual na OLT 8820 G com os comandos *port up, port down, port bounce,* ou *port testing.*
- » Verificar o status administrativo de uma porta física ou de uma interface virtual na OLT 8820 G com o comando *port show.*

» Visualizar o status operacional, a velocidade e o modo duplex das portas Ethernet com o comando *port status.*
» Associar uma string de texto com uma interface física, incluindo grupos de ligação, com o conjunto de comandos *port description.*
» Exibir ou limpar diversas informações de estatísticas nas portas Ethernet com o comando *port stats.*
» Definir o nível de criticidade dos alarmes nas portas Ethernet com o comando *port config alarm.*

Visualizar o status administrativo e operacional das portas com o comando port status e port show

Comando port status e port show

1. Use o comando *port status* para visualizar status operacional, velocidade e modo duplex de uma porta Ethernet;

> **Observação:** o comando *port status* somente é válido para portas Ethernet

```
iSH> port status 1-1-2-0/eth
Operational status     : Up
Rate in Mbps           : 1000
Duplex                 : Full
```

2. Use o comando *port show* para visualizar o status administrativo de uma porta ou interface;

```
iSH> port show 1-1-2-0/eth
Interface 1-1-2-0/eth
  Physical location:        1/1/2/0/eth
  Administrative status: up
  Port type specific information:
    Link state mirroring not configured.
```

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:        1/1/1/0/gponolt
  Administrative status: up
```

Alterar o status administrativo das portas com os comandos port testing, up, down ou bounce

Comando port testing

1. Use o comando *port testing* para definir o status administrativo como teste em uma porta Ethernet;

```
iSH> port testing 1-1-2-0/eth
1-1-2-0/eth set to admin state TESTING
```

2. Verifique o status;

```
iSH> port show 1-1-2-0/eth
Interface 1-1-2-0/eth
  Physical location:        1/1/2/0/eth
  Administrative status: testing
  Port type specific information:
    Link state mirroring not configured.
```

3. Use o comando *port testing* para definir o status administrativo como teste em uma porta GPON da OLT;

```
iSH> port testing 1-1-1-0/gponolt
1-1-1-0/gponolt set to admin state TESTING
```

4. Verifique o status.

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
   Physical location:
                        1/1/1/0/gponolt
Administrative status: testing
```

Comando port up

1. Use o comando *port up* para definir o status administrativo como ativo em uma porta Ethernet;

```
iSH> port up 1-1-2-0/eth
1-1-2-0/eth set to admin state UP
```

2. Verifique o status;

```
iSH> port show 1-1-2-0/eth
Interface 1-1-2-0/eth
  Physical location:        1/1/2/0/eth
  Administrative status: up
  Port type specific information:
    Link state mirroring not configured.
```

3. Use o comando *port up* para definir o status administrativo como ativo em uma porta GPON da OLT;

```
iSH> port up 1-1-1-0/gponolt
1-1-1-0/gponolt set to admin state UP
```

4. Verifique o status.

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:         1/1/1/0/gponolt
  Administrative status: up
```

Comando port down

1. Use o comando *port down* para definir o status administrativo como inativo em uma porta Ethernet;

```
iSH> port down 1-1-2-0/eth
1-1-2-0/eth set to admin state DOWN
```

2. Verifique o status;

```
iSH> port show 1-1-2-0/eth
Interface 1-1-2-0/eth
  Physical location:        1/1/2/0/eth
  Administrative status: down
  Port type specific information:
    Link state mirroring not configured.
```

3. Use o comando *port down* para definir o status administrativo como inativo em uma porta GPON da OLT;

```
iSH> port down 1-1-1-0/gponolt
1-1-1-0/gponolt set to admin state DOWN
```

4. Verifique o status.

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:        1/1/1/0/gponolt
  Administrative status: down
```

Comando port bouce

1. Use o comando *port bounce* para realizar uma operação de down (inativo) e em seguida uma operação de up (ativo) em uma porta Ethernet;

```
iSH> port bounce 1-1-2-0/eth
1-1-2-0/eth set to admin state DOWN 1-1-2-
0/eth set to admin state UP
```

2. Verifique o status;

```
iSH> port show 1-1-2-0/eth
Interface 1-1-2-0/eth
Physical location: 1/1/2/0/eth
Administrative status:    up
Port type specific information:
  Link state mirroring not configured.
```

3. Use o comando *port bounce* para realizar uma operação de down (inativo) e em seguida uma operação de up (ativo) em uma GPON da OLT;

```
iSH> port bounce 1-1-1-0/gponolt
/gponolt set to admin state DOWN
1-1-1-0/gponolt set to admin state UP
```

4. Verifique o status.

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:        1/1/1/0/gponolt
  Administrative status: up
```

Descrições das portas

Regras para configurar descrições das portas

A OLT 8820 G possui um campo de descrição de porta, que oferece um mapeamento entre uma porta física ou bridge e um usuário (assinante). Esse mapeamento aprimora o gerenciamento da OLT 8820 G sem exigir documentos adicionais para oferecer o mapeamento. As informações de descrição de portas podem ser inseridas para portas ou bridges. As informações de descrição de portas também inclui opção de busca.

As regras para inserir uma descrição de porta são:

- » Descrições de portas não necessitam ser únicas.
- » O campo de descrição de porta é um campo de texto com até 54 caracteres.
- » Qualquer caractere pode ser usado, incluindo espaços, $,@,-,.,etc. Os únicos caracteres não suportados são as aspas duplas, ", que é um delimitador para identificar o início e o término da linha de texto, o circunflexo "^" e a interrogação "?".
- » Descrições de portas são associadas com portas físicas e não interfaces lógicas. Para unir tecnologias, as descrições de portas são suportadas tanto na porta física, como no grupo de agregação, para o caso de você desejar usar uma palavra-chave como um nome de companhia para interfaces de grupo.
- » Mesmo que as descrições de porta possam ser buscadas, você não pode realizar comandos usando a descrição de porta. Por exemplo, não é possível usar um comando como "bridge modify DescriçãoPorta …".

Adicionar, modificar, listar e apagar uma descrição de porta

O comando port description add associa uma descrição de texto a uma interface física (incluindo grupos de agregação):

```
port description add <physical interface> <text string>
```

> **Observação:** descrições de portas não necessitam ser únicas. Se um cliente tem muitas conexões, elas podem ter a mesma descrição de porta. Você também pode usar o campo descrição de porta como meio de identificar um grupo de interfaces

Adicionar uma descrição para uma porta

1. Para adicionar uma descrição de porta, insira:

```
iSH> port description add 1-1-1-0/gponolt "Subscriber A"
```

Neste caso, a descrição de porta possui espaços, portanto as aspas são necessárias.

2. Para verificar a descrição da porta, insira:

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:        1/1/1/0/gponolt
  Description:     Subscriber A
  Administrative status: up
```

3. Para adicionar uma descrição de porta sem espaços, insira:

```
iSH> port description add 1-1-8-0/gponolt Carringtons
```

4. Para verificar a descrição da porta, insira:

```
iSH> port show 1-1-8-0/gponolt
Interface 1-1-8-0/gponolt
  Physical location:        1/1/8/0/gponolt
```

```
  Description:     Carringtons
  Administrative status: up
```

Modificar uma descrição de porta

O comando port description modify permite que você modifique uma descrição de porta existente.

```
port description modify <physical interface> <text string>
```

1. Inserir uma descrição de porta:

```
iSH> port description add 1-1-1-0/gponolt "Cafe Roma"
```

2. Verificar a descrição da porta:

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:                1/1/1/0/gponolt
  Description:                      Cafe Roma
  Administrative status:    up
```

3. Modificar a descrição da porta:

```
iSH> port description modify 1-1-1-0/gponolt "Cafe Barrone"
```

4. Verificar a modificação da descrição da porta:

```
iSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
  Physical location:        1/1/1/0/gponolt
  Description:              Cafe Barrone
  Administrative status:    up
```

Listar a descrição de porta

O comando *port description list* listará as descrições de uma porta desejada.

```
 Interface Description
-------------------------------------------------------------------------------
1-1-2-0/eth  -
1-1-2-0/gponolt  -
1-1-2-1/gpononu US Insurance Consortium, Inc.
1-1-2-2/gpononu -
1-1-2-3/gpononu -
1-1-2-4/gpononu -
1-1-2-5/gpononu -
1-1-2-6/gpononu -
1-1-2-7/gpononu -
1-1-2-8/gpononu -
1-1-2-9/gpononu -
1-1-2-10/gpononu -
1-1-2-11/gpononu -
1-1-2-12/gpononu -
<SPACE> for next page, <CR> for next line, A for all, Q to quit
```

Remover descrição de porta

O comando *port description* delete remove a descrição de porta de uma interface física.

```
port description delete <physical interface>
```

1. Para visualizar a descrição de porta em uma porta física, insira:

```
iSH> port show 1-1-2-0/gponolt
Interface 1-1-2-0/gponolt
  Physical location:                1/1/2/0/gponolt
  Description:                      US Insurance Consortium, Inc.
  Administrative status:    up
```

2. Para apagar a descrição de porta, insira:

```
iSH> port description delete 1-1-2-0/gponolt
```

3. Para visualizar a remoção da descrição, insira:

```
iSH> port show 1-1-2-0/gponolt
Interface 1-1-2-0/gponolt
  Physical location:        1/1/2/0/gponolt
  Administrative status: up
```

Buscar descrições de porta

O comando *port description find* oferece uma busca textual que permite procurar uma sequência de texto nos campos de descrição de porta. A tela exibe a descrição e o local físico. Se diversas descrições de portas tiverem a mesma sequência de texto, todas serão exibidas.

```
port description find <text string>
```

```
iSH> port description find Carringtons
Results for Carringtons
Description:            Carringtons
Interface:              1-1-8-0/gponolt

iSH> port description find "US Insurance Consortium, Inc."
Results for US Insurance Consortium, Inc.
Description:             US Insurance Consortium, Inc.
Interface:               1-1-2-0/gponolt
```

> **Observação:** observe que, para os itens de busca que não têm espaços, as aspas não são necessárias

Espelhamento de portas

A OLT 8820 G oferece o recurso de espelhamento de portas como ferramenta de diagnóstico usada para resolver problemas com transmissão/recepção de pacotes em portas uplink.

As regras para espelhamento de portas são:

- A OLT 8820 G suportar uma porta espelho por vez.
- Somente é possível configurar espelhamento de portas em portas ethernet da OLT 8820 G.
- Todas as portas espelhadas devem estar na mesma OLT 8820 G.
- Qualquer porta Ethernet pode ser espelhada para outra porta Ethernet na mesma OLT 8820 G, exceto a porta 10/100 Ethernet de gerenciamento.
- Quando uma porta é um membro de um grupo de agregação de link, o grupo de agregação de link ou uma porta no grupo de agregação de link pode ser espelhada.

> **Observação:** se mais de uma porta precisar ser espelhada, você deve inserir as portas em um grupo de agregação de link. As portas devem permanecer no grupo de agregação de link para o espelhamento continuar

Sintaxe do comando port mirror

A sintaxe do comando *port mirror* é:

```
port mirror <from-interface> <to-interface> <vlan
<vlanId>> <in|out|both|off>
```

Variável	Definição
from-interface	Interface para espelhar
to-interface	Interface para onde os pacotes são enviados
vlanID	Tag da VLAN externa
In	Espelhar os pacotes de entrada
Out	Espelhar os pacotes de saída
Both	Espelhar os pacotes de entrada e saída
off	Desabilitar o espelhamento de portas da interface

Variáveis para o comando port mirror

Criar uma porta espelhada na porta ethernet de uplink

» **Caso 1:** configurar uma porta uplink 100/1000 ethernet para espelhar os pacotes de entradas para uma outra porta 100/1000 ethernet

1. Neste caso, ambas as portas são 100/1000 Ethernet;

```
iSH> port mirror 1-1-2-0/eth 1-1-3-0/eth vlan 200 in
```

Este exemplo habilita o espelhamento dos pacotes de entrada da porta *1-1-2-0/eth* e envia os pacotes para a porta 1-1-3-0/eth na VLAN 200.

2. Para desabilitar o espelhamento, insira o comando *off.*

```
iSH> port mirror 1-1-2-0/eth 1-1-3-0/eth vlan 200 off
```

» **Caso 2:** configurar um grupo de agregação para espelhar os pacotes de entradas e saídas para uma porta 100/1000 ethernet

1. Verifique as portas no grupo de agregação de link;

```
iSH> linkagg show
LinkAggregations:
slot  unit   ifName      partner: Sys            Pri     grp ID   status    agg mode
1*    1      1-1-1-0     00:00:00:00:00:00       0x0     0x0      ACT       On
             links       slot    port    subport         status
             1-1-2-0     1       2       0               ACT
             1-1-3-0     1       3       0               ACT
```

2. Neste caso, 1-1-1-0/linkagg é o grupo de agregação e 1-1-4-0/eth é a porta 100/1000 ethernet que receberá os pacotes;

```
iSH> port mirror 1-1-1-0/linkagg 1-1-4-0/eth vlan 700 both
```

Este exemplo habilita o espelhamento dos pacotes de entrada e saída das portas 1-1-2-0/eth e 1-1-3-0/eth que pertencem ao grupo de agregação e os enviam para a porta 1-1-4-0/eth na VLAN 700.

3. Para desabilitar o espelhamento, insira off no final do comando.

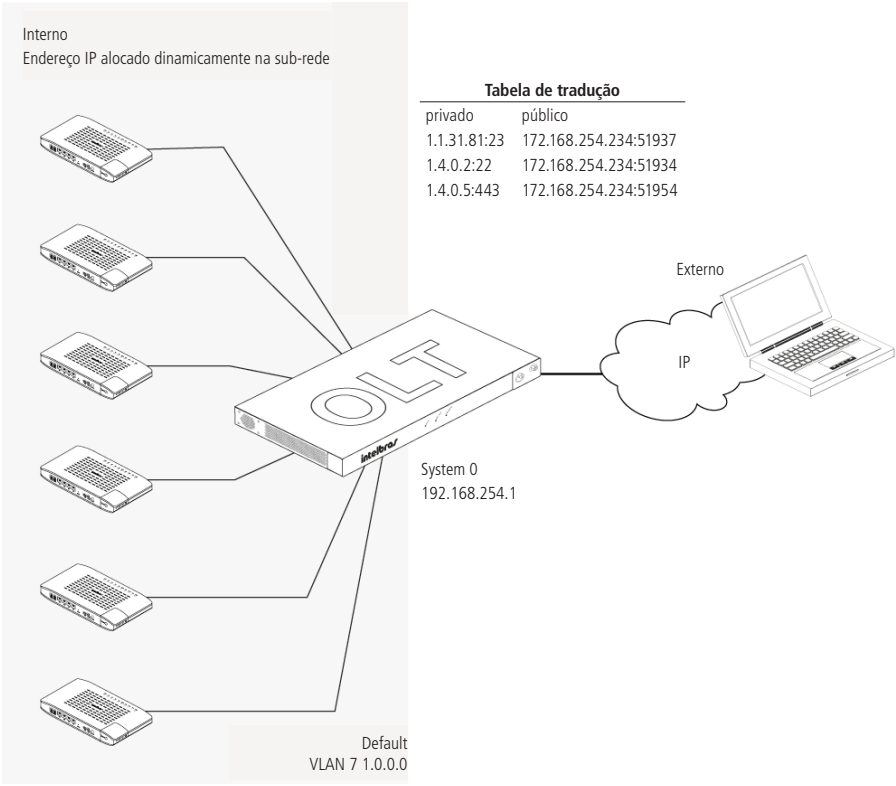
```
iSH> port mirror 1-1-1-0/linkagg 1-1-4-0/eth vlan 700 off
```

7.7. CPE Manager (Gerenciador de CPE)

O Gerenciador de CPE da OLT 8820 G oferece meios para gerenciar as CPEs (Customer Premises Equipment) dos usuários (assiantes) sem exigir endereços IPs roteáveis para acessá-las. O Gerenciador de CPE é especificamente projetado para a OLT Intelbras e pode ser usado com qualquer CPE (ONT) que suporta a recepção de um endereço IP via DHCP em uma VLAN.

Em muitos provedores de serviços (ISPs), a crescente utilização das ONTs (CPEs) criam um desafio operacional, pois o número de dispositivos que requerem endereços IP causam um grande uso de espaço desses endereços, tornando difícil a atribuição de endereços roteáveis para esses dispositivos.

A solução para este problema é o Gerenciador de CPE, que adiciona capacidade de proxy para a OLT, permitindo em seu gerenciamento a criação de uma interface IP, afim de fornecer acesso IP para todas as ONTs (CPEs) conectadas a OLT. Esta interface IP é criada em uma porta upstream e é roteável na rede de gerenciamento do provedor, fornecendo endereços IPs e tradução de portas de protocolo durante o encaminhamento de pacotes para as ONTs configuradas para este gerenciamento. Desta forma, o endereço IP da OLT pode ser usado para o gerenciamento das ONTs sem ter necessidade de consumir o espaço de endereços IPs ou ter que adicionar rotas para alcançar as ONTs que estão nos clientes.



Aplicação do CPE Manager

Acessando o endereço privado da ONT (CPE)

Para acessar uma ONT configurada pelo gerenciador de CPE, acesse a OLT através de seu endereço IP, no entanto, em vez de usar as portas de protocolo conhecidos, (por exemplo, porta 80 utilizado pelo protocolo http) deve-se utilizar as portas públicas da ONT mais um deslocamento específico de porta para o protocolo desejado. Os protocolos suportados são Echo, FTP (data), FTP (control), SSH, Telnet, HTTP, SNMP e HTTPS.

Para selecionar as portas, utilize o comando *cpe-mgr add*. Este comando possui várias opções dependendo da seleção dos parâmetros *compact* e *security:*

» **compact [full | partial | none]**

A seleção do modo *compact* define quantas portas podem ser acessadas usando a conexão NAT-PAT; quanto mais portas são acessadas por dispositivo, menos dispositivos poderão ser acessados.

» **security [enabled | disabled | default]**

A seleção do modo *security* define se as portas usarão SSH, por exemplo HTTP ou HTTPS, Telnet ou SSH.

Uma lista de compensações para portas públicas baseadas nos modos compact e security é apresentada na tabela.

O padrão para o modo compact é a opção full (mapeamento de três portas). Para o modo security, o padrão é a opção default, isto é, utiliza as configurações de segurança determinadas no profile system 0.

Compensação para porta pública	Tipo	Nome	Modos Compact e Security				
			Full		Partial		None
			Secure habilitado	Secure desabilitado	Secure habilitado	Secure desabilitado	N/A (todas as portas)
7	TCP, UDP	ECHO	+0	+0	+0	+0	+0
20	TCP	FTP - dados	—	—	—	—	+1
21	TCP	FTP - controle	—	—	—	—	+2
22	TCP, UDP	SSH	+1	—	+1	—	+3
23	TCP, UDP	Telnet	—	+1	—	+1	+4
80	TCP	HTTP	—	+2	—	+3	+5
81	TCP	HTTP	—	—	—	—	+6
161	TCP, UDP para partial e nenhum UDP para modo compact full	SNMP	+2	+2	+2	+2	+7
162	UDP	Traps SNMP (somente upstream)	+0	+0	+3	+3	+1
443	TCP	HTTPS	+2	—	+3	—	+8

Compensações para portas públicas

A rede definida por padrão é a *1.0.0.0/8* (classe A), utilizando a VLAN 7.

O endereço IP fornecido para a ONT (CPEs), seguem as orientações gerais:

<Class A network>.<Slot>.<Port number: higher order byte>.<Port number: lower order byte>

Observe que o formato GPON tem a porta/subporta codificados no endereço de IP, o que permite 12 bits para uma subporta e 4 bits para o número de porta:

*<class A>.<slot>.<subport upper 8 bits>.<subport lower 4 bits * 16 + port>*

Configurando o CPE Manager (Gerenciador de CPE)

Configurando a OLT 8820 G com gerenciador de CPE:

1. Adicione o endereço IP pública da OLT para o Gerenciador de CPE;
   `cpe-mgr add public 10.55.1.237`
2. Para ativar o CPE-MGR em uma ONT, deve-se sempre utilizar a gem port 5xx, onde xx é a posição da ONT na porta PON (varia de 1 a 64);
3. Adicione uma ONT Intelbras. Para a realização do comando, a ONT já deve possuir um GTP configurado;
   `cpe-mgr add local 1-1-3-501/gponport gtp 1`
4. Se o GTP não existir, deve-se criá-lo inserindo o comando new gpon-traffic-profile + <gpon-traffic-profile index>;

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile  1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ----->          {0}: 512000
traffic-class: --------------->         {ubr}:
compensated: ----------------->         {false}:
shared: ---------------------->         {false}:
dba-enabled: ----------------->         {false}:
dba-fixed-us-ubr-bw: --------->         {0}:
dba-fixed-us-cbr-bw: --------->         {0}:
dba-assured-us-bw: ---------->          {0}:
dba-max-us-bw: -------------->          {0}:
dba-extra-us-bw-type: ------>           {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
```

```
iSH> cpe-mgr add local 1-1-3-501/gponport gtp 1
GEM port 1-1-3-501/gponport created
  Configured Gerenciador de CPE's local network:
    Class A network: 1.0.0.0
    Local IP: 1.0.0.1
    VLAN ID: 7
  Created CPE Management interface: 1-1-3-501-gponport-7/ip
```

Alterando a VLAN da rede local

Normalmente as configurações padrão da OLT são aceitáveis. Entretanto, é possível alterar a rede padrão (classe A) ou a VLAN ID, você pode usar o comando a seguir. Observe que ao alterar a VLAN, será necessário alterar as configurações de VLAN de todas as ONTs (CPEs). A VLAN 7 é a VLAN de gerenciamento padrão para as ONTs Intelbras.

1. Para alterar o VLAN ID da rede privada local do Gerenciador de CPE, utilize a sintaxe a seguir (este novo VLAN ID será utilizado para o gerenciamento interno das ONTs através do gerenciador de CPE):

```
cpe-mgr add local vlan <vlan id>
```

Para alterar manualmente o VLAN ID para o padrão, utilize o seguinte comando:

```
iSH> cpe-mgr add local vlan 7
```

> **Observação:** a Intelbras não recomenda alterar a VLAN padrão, pois as ONTs Intelbras utilizam a VLAN 7 como a VLAN de gerenciamento padrão

> **Observação:** somente é possível modificar a VLAN padrão de gerenciamento quando não houver nenhuma ONT (CPE) configurada na rede no momento

Alterando a rede local (classe A) utilizada pelo gerenciador de CPE

Novamente a Intelbras recomenda a utilização das configurações padrões. Entretanto, caso necessite alterar a rede padrão (é permitido somente endereços de rede classe A) utilize o comando a seguir. Caso desejar alterar as configurações de rede local após a conexão e configuração das ONTs (CPEs), será necessário remover os dispositivos antes de realizar as alterações:

1. Para alterar o endereço de rede local privado do Gerenciador de CPE, utilize a sintaxe a seguir (este novo endereço de rede será utilizado para o gerenciamento interno das ONTs através do gerenciador de CPE). Somente é permitido endereços de rede classe A:

```
cpe-mgr add local network <endereço de rede classe A>
```

2. Para alterar manualmente o endereço de rede para o padrão, utilize o seguinte comando:

```
iSH> cpe-mgr add local network 1.0.0.0
```

> **Observação:** somente é possível modificar o endereço de rede padrão de gerenciamento quando não houver nenhuma ONT (CPE) configurada na rede no momento

Por padrão, é utilizado a rede 1.0.0.0/8 (classe A). Em outras palavras, uma rede de categoria A possui máscara de rede de 8 bits, que significa que somente o primeiro byte (octeto) do endereço IP é comum entre os todos os nós da rede. Se você executar o seguinte comando: *cpe-mgr add local network 2.0.0.0*, a rede classe A será alterada e todos os IPs locais começarão com 2.

Visualizando as portas utilizadas pelo gerenciador de CPE

O comando *cpe-mgr show* oferece um mapeamento entre a interface e o endereço IP local juntamente com as portas configuradas.

```
iSH> cpe-mgr show
     Gerenciador de CPE public side interface:
          IP        10.55.1.237
     Gerenciador de CPE local management network:
          IP 1.0.0.1/8 (default) (active)
          VlanID:   7 (default)
     Managed CPE Interface Configuration:
```

Interafce	Local IP	ECHO	FTP	SSH	Telnt	HTTP	SNMP	HTTPS
1-1-1-501/gponport	1.1.31.84	51936	-	-	51937	51938	51938	-
1-1-3-501/gponport	1.1.31.83	51921	-	-	51922	51923	51923	-
1-1-2-701/gponport	1.1.43.211	51933	-	-	-	-	51935	-
1-1-3-701/gponport	1.1.43.201	51939	-	-	51943	51944	51946	-
1-1-4-701/gponport	1.1.43.243	51948	-	-	51949	51951	51951	-
1-1-5-701/gponport	1.1.43.223	51952	-	-	-	51955	51954	-

Modo compact full com security desabilitado.

```
iSH> cpe-mgr show local 1-1-3-501/gponport
Public IP address: 10.55.1.237
Public Access Port:
         Protocol  Port
         ECHO              51936
         SNMP Traps        51936
         Telnet            51937
         HTTP              51938
         SNMP              51938
Local   IP   Address:  1.1.31.83
```

Modo compact full com security habilitado.

```
iSH> cpe-mgr show local 1-1-2-701/gponport
Public IP address: 10.55.1.237
Public Access  Port:
         Protocol  Port
         ECHO              51939
         SNMP Traps        51939
         SSH               51940
         HTTPS             51941
         SNMP              51941
         Local IP Address: 1.1.43.211
```

Modo compact none. Observe que, como todas as portas estão disponíveis, o modo security não é aplicável neste caso.

```
iSH> cpe-mgr show local 1-1-3-701/gponport
Public IP address: 0.55.1.237
Public Access Port:
         Protocol  Port
         ECHO              51942
         SNMP Traps        51943
         FTP               51943/51944
         SSH               51945
         Telnet            51946
         HTTP(80)          51947
         HTTP(81)          51948
         SNMP              51949
         HTTPS             51950
         Local IP Address: 1.1.43.201
```

Modo compact partial com security desabilitado.

```
iSH> cpe-mgr show local 1-1-4-702/gponport
Public IP address: 10.55.1.237
Public Access Port:
```

```
        Protocol  Port
        ECHO              51951
        Telnet            51952
        SNMP              51953
        HTTP              51954
        SNMP Traps        51954
        Local IP Address: 1.1.43.243
```

Modo compact partial com security habilitado.

```
iSH> cpe-mgr show local    1-1-5-701/gponport
Public IP address: 10.55.1.237
Public Access Port:
        Protocol  Port
        ECHO              51955
        SSH               51956
        SNMP              51957
        HTTPS             51958
        SNMP Traps        51958
        Local IP Address: 1.1.43.223
```

Resolução de problemas do gerenciador de CPE

Para verificar ou solucionar problemas do Gerenciador de CPE, você deve entender o que faz os dois comandos utilizado pelo Gerenciador de CPE. O primeiro comando é *cpe-mgr add public*.

» Define *natenabled* para "yes" no profile *ip-interface-record* para o endereço público configurado, em nosso exemplo, o endereço 10.55.1.237.

Ao utilizar as configurações padrões e a rede local ainda não tenha sido criada, o segundo comando é *cpe-mgr add local*:

» Cria um registro flutuante no profile *ip-interface-record* com o endereço IP 1.0.0.1 (apenas é criado se os padrões estão sendo usados e se o registro ainda não existir).

» Cria um registro no profile *ip-unnumbered-record* para o registro criado no profile ip-interface-record (apenas é criado se os padrões estão sendo usados e se o registro ainda não existir).

» Cria um profile *dhcp-server-subnet* para a rede 1.0.0.0 (apenas é criado se os padrões estão sendo usados e se o registro ainda não existir).

» Cria um registro de host no profile *ip-interface-record* para a CPE na interface. Designa um endereço IP local com base na descrição da interface (não roteável, mas pode ser alcançado a partir da rede local ou por Telnet para a OLT e em seguida um Telnet da OLT para a ONT).

» Cria um perfil *pat-bind* do tipo *cpemgr* ou *cpemgrsecure*.

> **Observação:** o perfil *ip-interface-record* criado não é um registro de "host" normal e não pode ser visto usando o comando *host show*

O perfil pat-bind do primeiro dispositivo do exemplo, contém o endereço IP local (1.1.31.83) e a porta pública (51921):

```
iSH> list pat-bind
pat-bind 2
1 entry found.

iSH> get pat-bind 2
pat-bind 2
public-ipaddr: --->         {10.55.1.237}
public-port: ----->         {51921}
local-ipaddr: ---->         {1.1.31.83}
local-port: ------>         {3}
portType: -------->         {cpemgr}
```

```
iSH> cpe-mgr show local 1-1-3-501/gponport
```

```
Public IP address: 10.55.1.237
Public Access Port:
         Protocol  Port
                   ECHO                51921
                   SNMP Traps          51921
                   Telnet              51922
                   HTTP                51923
                   SNMP                51923
                   Local IP Address: 1.1.31.83
```

O endereço local oferecido é baseado na interface na seguinte forma:

```
<local class A network>.<slot>.<port HI byte>.<port LO byte>
```

A partir da interface de nosso exemplo, 1-1-3-501/gponport, o endereço IP local (conforme exibido acima no perfil *pat-bind 2*) é 1.1.31.83. Se precisar verificar esse número, realize o comando get no perfil *pat-bind* ou use o comando *cpe-mgr show local.*

Informações adicionais sobre o gerenciador de CPE

O primeiro dispositivo será acessível pelo endereço IP público da OLT 8820 G e pela porta base da ONT (CPE). A porta base da ONT (CPE) para o primeiro dispositivo é 51921. Para alcançar uma das portas conhecidas, você deve fornecer a compensação para a porta pública.

A porta conhecida (7) é para echo, e tem uma compensação de zero.

1º dispositivo	ECHO	+0	51921
	FTP (dados)	+1	
	FTP (controle)	+2	
	SSH	+3	
	Telnet	+4	
	HTTP	+5	
	HTTP	+6	
	SNMP	+7	
	HTTPS	+8	
2º dispositivo	ECHO	+0	51930
	FTP (dados)	+1	
	FTP (controle)	+2	
	SSH	+3	
	Telnet	+4	
	HTTP	+5	
	HTTP	+6	
	SNMP	+7	
	HTTPS	+8	
3º dispositivo	ECHO	+0	51939
	FTP (dados)	+1	
	FTP (controle)	+2	
	SSH	+3	
	Telnet	+4	
	HTTP	+5	
	HTTP	+6	
	SNMP	+7	
	HTTPS	+8	

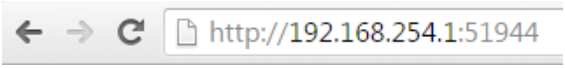
Observação: os exemplos usam o modo compact definido em none. Ao utilizar diferentes variações do modo *compact* e do modo *security* exige diferentes compensações

Para realizar uma conexão telnet ao primeiro CPE através da porta conhecida, 23, é necessário usar a porta base da CPE mais a compensação de porta pública, que é igual a 4; Você usaria o endereço da OLT 8820 G (10.55.1.237), na porta 51925 (51921 + 4) para uma conexão via Telnet a ONT. A partir de um prompt Unix ou DOS, o comando seria o seguinte:

```
telnet 10.55.1.237 51925
```

Para acessar o segundo dispositivo, você precisa iniciar com a porta base da CPE para tal dispositivo. Cada dispositivo consome nove portas públicas, portanto o primeiro dispositivo tem uma variação de porta de 51921 - 51929, o segundo dispositivo tem uma variação de porta de 51930 - 51938, o terceiro dispositivo de 51939 - 51947 e assim por diante.

Para acessar a porta HTTP do terceiro dispositivo por um navegador é necessário iniciar pelo primeiro endereço de porta pública 51921 + 18 (ponto de início 51921 mais duas vezes nove para alcançar o inicio das portas do terceiro dispositivo, então utilizar a compensação de 5 para chegar à porta 80 (HTTP) do terceiro dispositivo, ou seja 51944.



Inserindo o endereço de acesso da ONT

Conforme as CPEs são removidas ou adicionadas, lacunas serão formados na lista de dispositivos, portanto a ordem eventualmente torna-se arbitrária, mas é usada na discussão para elucidar como o mecanismo funciona.

A porta base da CPE e as informações dos dispositivos adicionados são exibidos através do comando *cpe-mgr show.*

Acessando as ONTs (CPEs) via interface web

Criação dos links de acesso as ONTs (CPEs) via interface web

A partir do interface de linha de comando da OLT 8820 G:

1. Crie uma interface de gerenciamento para a OLT 8820 G;
2. Crie um endereço IP público de gerenciamento utilizando o endereço IP de gerenciamento da OLT 8820 G;

```
iSH> cpe-mgr add public 192.168.10.1
CPE Manager using 192.168.10.1 for public interface.
```

3. Crie um endereço IP local de gerenciamento para a interface. Certifique-se de que o perfil de tráfego GPON específico existe;

```
iSH> cpe-mgr add local 1-1-3-501/gponport gtp 1
GEM port 1-1-3-501/gponport created
Configured Gerenciador de CPE's local network:
Class A network: 1.0.0.0
Local IP:          1.0.0.1
VLAN ID: 7
Created CPE Management interface: 1-1-3-501-gponport-7/ip
```

4. Visualize o registro *pat-bind* que foi automaticamente criado;

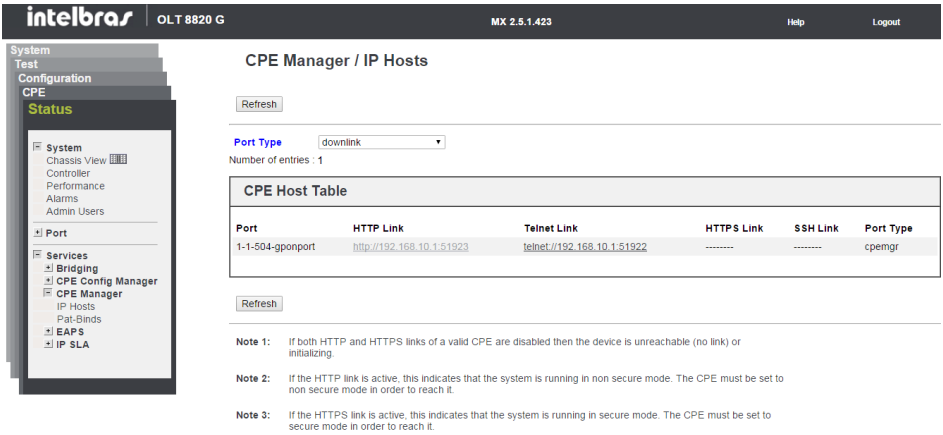
```
iSH> get pat-bind 2
pat-bind 2
public-ipaddr: ----->       {192.168.10.1}
public-port: ------->       {51921}
local-ipaddr: ------>       {1.1.31.83}
local-port: -------->       {3}
portType: ---------->       {cpemgr}
```

5. Verifique se a interface IP *cpe-mgr* está ativa (up);

```
iSH> interface show
2 interfaces
Interface      Status  Rd/Address          Media/Dest Address                IfName
1/1/1/0/ip     UP      1 192.168.10.1/24 00:01:47:24:08:ae 1-1-1-0-eth     1-1-1-0-eth
1/1/3/501/ip   UP      1 [1.0.0.1]        1.1.31.83                         1-1-3-501-gponport-7
```

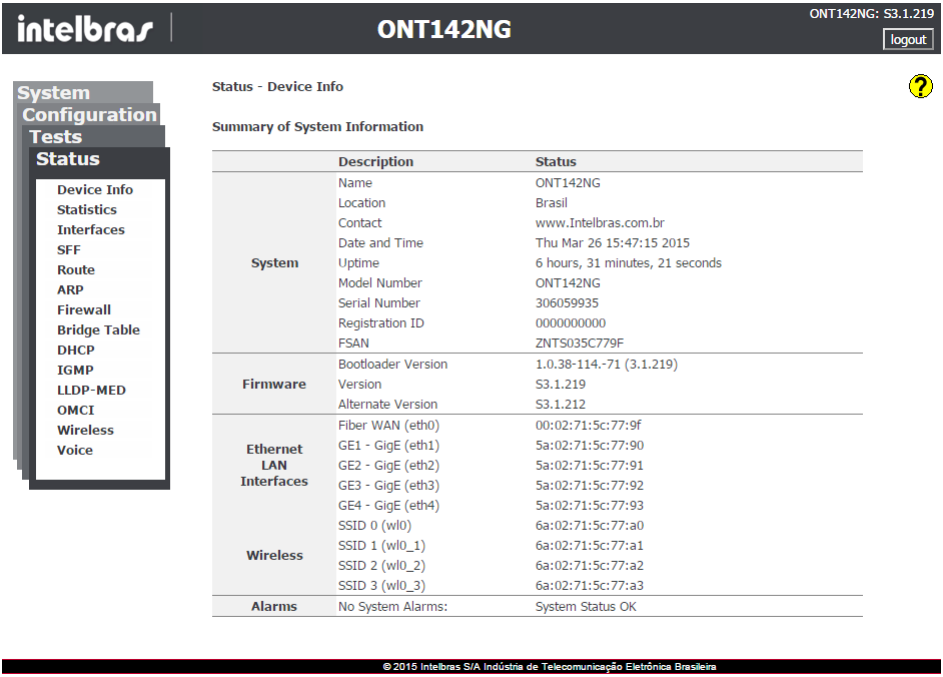
6. A partir de um navegador, acesse a interface web de gerenciamento da OLT 8820 G, *http://192.168.10.1;*

7. Através da interface web da OLT, visualize o link de acesso da ONT (CPE) clicando em *Status>Service>CPE Manager> IP Hosts;*



Links de acesso a interface web das ONTs (CPEs)

8. Clique no link da ONT desejada para acessar a respectiva interface web.



Página da interface web para ONT Intelbras

Definições da OLT 8820 G

Embora a OLT 8820 G não possua cartões (módulos), as configurações do dispositivo são armazenadas em um perfil chamado *card-profile*. O tipo de interface para a OLT 8820 G sempre segue a convenção de que shelf é 1, slot é 1 e a subporta é 0. Atualize o perfil *card-profile* para modificar as configurações da OLT. A tabela a seguir exibe o número e o nome da imagem do software da OLT 8820 G.

Cartão	Tipo	Nome da imagem do software
OLT 8820 G	10500	mx1u19x.bin

Tipo do dispositivo para a OLT 8820 G

1. Use o comando slots para exibir o status da OLT 8820 G;

```
iSH> slots
Cards
1: MXK 19x/MXK 198 - 8 GPON OLT, 8 FE/GE (RUNNING)
```

2. Insira o comando *get card-profile 1/1/tipo* para visualizar os parâmetros do perfil *card-profile*;

```
iSH> get card-profile 1/1/10500
card-profile        1/1/10500
sw-file-name: ----------------->        {mx1u19x.bin}
admin-status: ---------------->        {operational}
upgrade-sw-file-name: -------->        {}
upgrade-vers: ---------------->        {}
admin-status-enable: -------->        {enable}
sw-upgrade-admin: ------------>        {reloadcurrrev}
sw-enable: ------------------->        {true}
sw-upgrade-enable: ---------->        {false}
card-group-id: --------------->        {1}
hold-active: ----------------->        {false}
weight: ---------------------->        {nopreference}
card-line-type: -------------->        {unknowntype}
card-atm-configuration: ------>        {notapplicable}
card-line-voltage: ---------->        {not-used}
maxvpi-maxvci: --------------->        {notapplicable}
card-init-string: ------------>        {}
wetting-current: ------------>        {disabled}
pwe-timing-mode: ------------>        {none}
```

7.8. Gerenciamento seguro da OLT 8820 G

Tipos seguros de gerenciamento (SSH, SFTP e HTTPS)

Habilitar segurança no gerenciamento da OLT 8820 G

O perfil *system 0* oferece um parâmetro *secure* que permite somente comunicação segura para atividades de gerenciamento. Quando a segurança está habilitada, a OLT 8820 G usa os seguintes protocolos:

- Secure File Transfer Protocol (SFTP)
- Secure shell (SSH)
- HTTPS (HTTP secure)

A tabela a seguir descreve quais protocolos são permitidos quando o parâmetro *secure* está habilitado (*enabled*) e quais protocolos são permitidos quando o parâmetro *secure* está desabilitado (*disabled*).

Desabilitado	Habilitado
TFTP, FTP	SFTP
Telnet, SSH	SSH
HTTP	HTTPS

Protocolos para o parâmetro secure

Habilitar o gerenciamento seguro na OLT 8820 G

1. Para habilitar o recurso de gerenciamento seguro, insira o comando *update system 0* e altere o parâmetro *secure* de disabled para enabled, e salve o arquivo:

> **Observação:** após habilitar o parâmetro secure, HTTPS e alterações na interface web têm efeito somente após a próxima reinicialização. SSH e SFTP não exigem reinicialização

```
iSH> update system 0
system   0
Please provide the following: [q]uit.
syscontact: ------------->  {}:
sysname: ---------------->  {}:
syslocation: ------------>  {}:
enableauthtraps: -------->  {disabled}:
setserialno: ------------>  {0}:
zmsexists: -------------->  {false}:
zmsconnectionstatus: ---->  {inactive}:
zmsipaddress: ----------->  {0.0.0.0}:
configsyncexists: -------->  {false}:
configsyncoverflow: ------->  {false}:
configsyncpriority: ------>  {high}:
configsyncaction: -------->  {noaction}:
configsyncfilename: ------->  {}:
configsyncstatus: -------->  {syncinitializing}:
configsyncuser: ---------->  {}:
configsyncpasswd: -------->  {** private **}:   ** read-only
** numshelves: ---------->  {1}:
shelvesarray: ------------>  {}:
numcards: --------------->  {1}:
ipaddress: -------------->  {192.168.10.1}:
alternateipaddress: ----->  {0.0.0.0}:
countryregion: ---------->  {us}:
primaryclocksource: ----->  {0/0/0/0/0}:
ringsource: ------------->  {internalringsourcelabel}:
revertiveclocksource: --->  {true}:
voicebandwidthcheck: ---->  {false}:
alarm-levels-enabled: --->  {critical+major+minor+warning}:
userauthmode: ------------>  {local}:
radiusauthindex: -------->  {0}:
secure: ----------------->  {disabled}: enabled
webinterface: ------------>  {enabled}:
options: ---------------->  {NONE(0)}:
reservedVlanIdStart: ---->  {0}:
reservedVlanIdCount: ---->  {0}:
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Conjuntos de criptografia

A OLT 8820 G suporta as seguintes criptografias para SSH.

Criptografia	Tamanho da chave
aes256-cbc	32 bytes (256 bits)
rijndael256-cbc	32 bytes (256 bits)
aes192-cbc	24 bytes (192 bits)
rijndael192-cbc	24 bytes (192 bits)
aes128-cbc	16 bytes (128 bits)
rinjdael128-cbc	16 bytes (128 bits)
blowfish-cbc	16 bytes (128 bits)
3des-cbc	24 bytes (192 bits)
arcfour	16 bytes (128 bits)

Criptografias da OLT 8820 G

Clientes SSH testados para OLT 8820 G

Secure Shell (SSH) é uma interface de comando e um protocolo utilizado para acesso seguro a um computador remoto. Os comandos inseridos utilizando SSH são criptografados e mantidos seguros de duas maneiras. Ambas as extremidades da conexão cliente/servidor são autenticadas usando um certificado digital e as senhas são protegidas por criptografia. Você pode conectar-se a uma OLT 8820 G usando um cliente SSH da sua escolha para criptografar a sessão. Os clientes SSH testados são:

- OpenSSH
  - cygwin
  - Linux
  - Solaris
- Putty
- Teraterm
- SecureCRT
- Absolute Telnet

Assinaturas digitais e criptografia de chave pública

Observação: por motivos de segurança, as chaves do host não são acessíveis via SNMP e não podem ser salvas/restauradas com o comando dump

Chaves DSA e RSA

A OLT 8820 G cria automaticamente um Digital Signature Algorithm (DSA), um padrão para assinaturas digitais, e suporta RSA, um algoritmo para criptografia de chave pública. As chaves de host DSA e RSA para o servidor são persistentemente armazenadas no perfil *encryption-key*. Para gerenciar as chaves do host, use o comando *encryption-key*.

RSA envolve uma chave pública e uma chave privada. A chave pública pode ser conhecida para todos e é usada para criptografar mensagens. Mensagens criptografas com a chave pública podem ser descriptografadas somente usando a chave privada.

Quando o sistema é iniciado pela primeira vez, ele tentará carregar as chaves DSA e RSA existentes. Se elas não existirem, o sistema cria uma chave DSA de 512 bits.

O comando *encryption-key* pode ser usado para visualizar as chaves atuais, criar uma nova chave, gerar chaves que podem ter sido comprometidas e remover as chaves.

1. Para criar uma nova chave, insira:

```
iSH> encryption-key add rsa 1024
Generating key, please wait ... done.
iSH>
```

Observação: a gereção de chaves é uma tarefa computacionalmente intensiva. Quanto maior for a chave, maior o tempo levará para ela ser gerada. Aguarde até que o sistema exiba que a geração da chave foi concluída antes de continuar

2. Para visualizar a nova chave, insira:

> **Observação:** o comando *encryption-key show* exibe as chaves que foram geradas e estão disponíveis para uso. O comando não exibe necessariamente apenas a chave criptográfica em uso

```
iSH> encryption-key show
Index     Type     Length
-------------------------
1         dsa      512
2         rsa      1024
```

3. Para gerar uma chave que pode ter sido comprometida, insira:

```
iSH> encryption-key renew dsa
Generating key, please wait ... done.
```

4. Para apagar uma chave de criptografia, insira:

```
iSH> encryption-key delete dsa
```

Comandos encryption-key

» **encryption-key add**

Adiciona uma chave criptográfica ao perfil encryption-key.

Sintaxe: encryption-key add [rsa|dsa] [512|768|1024|2048]

Opções: rsa|dsa

Nome e tipo da chave criptográfica.

512|768|1024|2048

O número de bytes definido para a chave.

» **encryption-key delete**

Remove uma chave criptográfica do perfil encryption-key.

Sintaxe: encryption-key delete [rsa|dsa]

Opções: rsa|dsa

Nome e tipo da chave criptográfica.

» **encryption-key renew**

Substitui uma uma chave criptográfica comprometida.

Sintaxe: encryption-key renew [rsa|dsa]

Opções: rsa|dsa

Nome e tipo da chave criptográfica.

» **encryption-key show**

Exibe as chaves criptográficas existentes.

Sintaxe: encryption-key show

Segurança de acesso a portas

A OLT 8820 G oferece segurança às portas UDP/TCP que são utilizadas no gerenciamento da OLT. Utilize o perfil *port-access* para definir as portas UDP/TCP, endereço IP ou a sub-rede do endereço IP que serão permitidos para acessar a porta.

O recurso de segurança de acesso a portas é um mecanismo lista branca. Se um endereço IP de um host não é especificado no perfil *port-access*, os usuários do referido host não poderão acessar a porta.

As portas usadas para gerenciamento são:

» telnet, porta 23.
» SSH, porta 22.
» HTTP, porta 80.
» HTTPS, porta 443.
» SNMP, porta 161.

Se você escolher restringir acesso à porta SNMP, deve haver uma regra para permitir a OLT 8820 G ter acesso a seu próprio SNMP.

Por padrão, perfis *port-access* não existem e todas as portas estão abertas. Após um perfil *port-access* ser configurado para uma porta, todos os outros endereços IP ou sub-redes são bloqueados. Essa restrição ocorre somente após a criação do primeiro perfil *port-access.*

> **Observação:** a segurança de acesso a portas não é independente da configuração de gerenciamento seguro (SFTP e SSH) do perfil *system 0.* Se o modo de gerenciamento seguro é habilitado de forma a oferecer SSH e SFTP e restringir acesso via telnet, porém você forneceu acesso telnet com o perfil port-access para um dispositivo (ou vários dispositivos), o dispositivo não será acessado

Criar entradas no perfil port-access

Para criar uma entrada no perfil *port-access*:

1. Crie uma nova entrada inserindo *new port-access n*, onde n é um número de identificação de entrada disponível;
2. No parâmetro *portNumber,* insira o número da porta;
3. No parâmetro *srcAddr* insira o endereço IP ou o primeiro endereço IP da sub-rede;
4. No parâmetro *netMask*, insira 255.255.255.255 para uma máscara de rede de um único endereço IP ou uma máscara de rede para uma sub-rede.

Até 100 entradas no perfil *port-access* podem ser criadas.

Criar uma entrada para um endereço IP no perfil port-access

Para criar uma entrada para um endereço IP específico:

Crie um novo perfil *port-access* e especifique o número da porta, o endereço IP do host e a máscara de rede 255.255.255.255 (esta máscara de rede significa que apenas um único endereço IP de host especificado será permitido).

Este exemplo cria a entrada 1 no perfil *port-access* para porta HTTP 80 permitindo apenas o host com endereço IP 172.16.42.1 tenha acesso via HTTP na OLT 8820 G.

> **Observação:** para criar proteção contra acesso a portas para HTTP e HTTPS, você precisará criar entradas no perfil *port-access* para a porta 80 e a porta 443

```
iSH> new port-access 1
port-access  1
Please provide the following: [q]uit.
portNumber: --->  {0}: 80
srcAddr: ------>  {0.0.0.0}: 172.16.42.1
netMask: ------>  {0.0.0.0}: 255.255.255.255
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Criar uma entrada para uma sub-rede no perfil port-access

Para criar uma entrada para uma sub-rede:

Crie um novo perfil *port-access* e especifique o número da porta, o endereço IP da sub-rede e a máscara de rede da sub-rede desejada, para permitir acesso de todos os host que pertençam a sub-rede especificada.

Este exemplo cria a entrada 2 no perfil *port-access* para porta Telnet 23 permitindo que os hosts da rede 172.16.41.xxx tenham acesso via Telnet na OLT 8820 G.

> **Observação:** normalmente, somente a porta 23 é usada para acesso telnet

```
iSH> new port-access 2
port-access  2
Please provide the following: [q]uit.
portNumber: --->  {0}: 23
srcAddr: ------>  {0.0.0.0}: 172.16.42.0
netMask: ------>  {0.0.0.0}: 255.255.255.0
```

```
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Exibindo as entradas no perfil port-access

Para exibir as entradas configuradas no perfil *port-access*, use o comando *list:*

```
iSH> list port-access
port-access 1
1 entry found.
```

Modificando as entradas no perfil port-access

Para modificar uma entrada configurada no perfil *port-access*, use o comando *update*. O exemplo a seguir altera o endereço IP de origem da rede para 172.16.40.0:

```
iSH> update port-access 2
portNumber: ----->     {23}
srcAddr: -------->     {172.16.41.0} 172.16.40.0
netMask: -------->     {255.255.255.0}
1 entry found.
.................
Save new record? [s]ave, [c]hange or [q]uit: s
Updated record saved.
```

Criando uma entrada no perfil port-access para a OLT 8820 G manter acesso ao SNMP

Crie uma nova entrada no perfil *port-access* e especifique o número de porta SNMP, o endereço IP 127.0.0.0 e a máscara de sub-rede 255.0.0.0.

```
iSH> new port-access 10
Please provide the following: [q]uit.
portNumber: ------------>     {0}: 161
srcAddr: --------------->     {0.0.0.0}: 127.0.0.0
netMask: --------------->     {0.0.0.0}: 255.0.0.0
.................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Suporte a autenticação Radius

A OLT 8820 G suporta autenticação de acesso local e/ou via Radius (Remote Authentication Dial In User Service). É possível configurar as seguintes combinações de autenticação: autenticação local, autenticação Radius ou autenticação Radius e local. Os usuários Radius são configurados com o atributo Service-Type como Administrative-User ou NAS-Prompt-User. Radius é usado somente para autenticação de login.

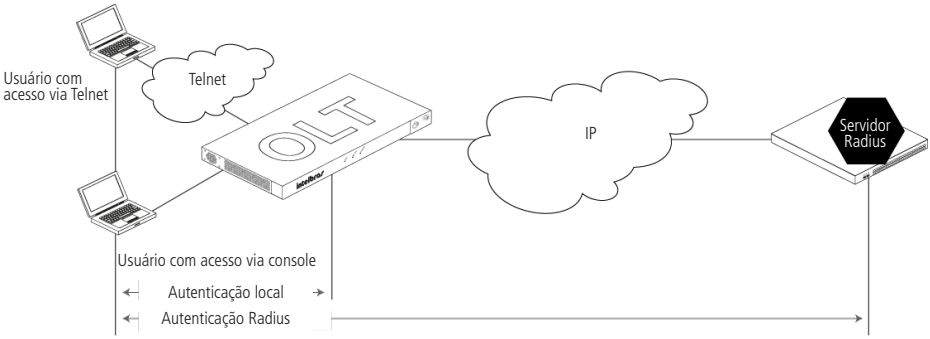
A tabela a seguir exibe o mapeamento de service-type das permissões da OLT 8820 G.

Atributo Service-Type	Permissões da OLT 8820 G
Administrative-User	admin, debug, voice, data, manuf, database, systems, tools, useradmin
NAS-Prompt-User	admin, voice, data, manuf, database, systems, tools, useradmin

Mapeamento de service-type para permissões na OLT 8820 G

Ao estabelecer uma conexão na OLT 8820 G com autenticação Radius, a OLT passa as informações Radius com segurança para o servidor Radius. O servidor Radius então autentica o usuário permitindo ou negando acesso a OLT. Se o acesso é negado e a opção de autenticação local também está configurada, a OLT autentica o acesso com base nos usuários e senhas configurados localmente em sua base de dados. Para logins e falhas de logins, uma mensagem no console é gerada com o ID de usuário e o endereço IP do dispositivo do qual o login foi originado. Logins com falha são registrados como mensagens de log (alerta) no arquivo de log da OLT 8820 G.

Por padrão, o acesso via Radius utiliza a porta 1812 (UDP) para autenticação. Esse parâmetro pode ser alterado no perfil radius-client. A imagem a seguir ilustra a autenticação Radius na OLT 8820 G.



Autenticação Radius na OLT 8820 G

Observação: siga as orientações do servidor Radius para instruções de configuração Radius. Por exemplo, ao usar a OLT 8820 G com o servidor FreeRadius:

- » Crie somente uma entrada no arquivo *clients.conf* para cada sub-rede ou OLT 8820 G individual. Para OLTs individuais, o endereço IP neste arquivo deve corresponder ao endereço IP da interface de saída usada pela OLT para conectar-se ao servidor Radius.
- » A OLT 8820 G usa o valor armazenado no arquivo *system.sysname Radius* para o atributo NAS-Identifier.
- » A shared-secret do perfil *radius-client* da OLT deve corresponder exatamente ao shared-secret da entrada configurada para o cliente Radius.

Configuração do suporte a Radius

A OLT 8820 G pode ser configurado para autenticação local, autenticação Radius ou Radius e autenticação local. Múltiplos perfis radius-client podem ser definidos usando números de índice e subíndice. Esse esquema de índice pode ser usado para criar números de índice para grupos ou servidores Radius. Quando um número de índice é especificado no perfil do sistema, a OLT 8820 G tenta autenticação de cada servidor Radius no grupo na ordem sequencial dos números do subíndice.
Para configurar o suporte Radius:

Observação: antes de iniciar este procedimento, certifique-se de que a OLT 8820 G possui conectividade IP com o servidor Radius

1. Crie um perfil radius-client na OLT 8820 G com o número de índice desejado e as configurações Radius para nome do servidor, shared-secret, número de novas tentativas e outros parâmetros. O primeiro número no índice é usado para um grupo de perfis radius-client, então múltiplos perfis podem ser atribuídos na OLT. O segundo número no índice especifica a ordem em que os perfis radius-client são apresentados. Esse exemplo especifica o *radius-client 1/1* com o nome de servidor *radius1* e *shared-secret de secret*. Um resolvedor DNS deve ser configurado no sistema para resolver o nome do servidor e o endereço IP. Se um resolvedor DNS não estiver disponível, especifique o endereço IP do servidor Radius. O índice 1/1 especifica que esse perfil é o primeiro perfil no grupo 1;

```
iSH> new radius-client 1/1
Please provide the following: [q]uit.
server-name: --->  {}: radius1.test.com [O resolvedor DNS deve ser configurado no sistema.]
udp-port: ------>  {1812}:
shared-secret: ->  {** password **}: secret
retry-count: --->  {5}:
retry-interval: >  {1}:
.................
Save new record? [s]ave, [c]hange or [q]uit: s
Record created.
```

2. Crie outro perfil radius-client na OLT 8820 G com as configurações Radius desejadas para nome do servidor, shared-secret, número de tentativas e outros parâmetros. Esse exemplo especifica o *radius-client 1/2* com o endereço IP do servidor *172.24.36.148* e *shared-secret de secret*. O índice 1/2 especifica que esse perfil é o segundo perfil do grupo1;

```
iSH> new radius-client 1/2
Please provide the following:[q]uit.
server-name: ----->     { }:172.24.36.248
udp-port: ------->      {1812}:
shared-secret: -->      {** password **}: secret
retry-count: ---->      {5}:
retry-interval: ->      {1}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
Record created.
```

3. Crie perfis radius-client adicionais para cada servidor Radius adicional a ser atribuído a esta OLT 8820 G;
4. No perfil system da OLT 8820 G, defina o método de autenticação de usuário desejado e especifique o índice do perfil radius a ser usado. Esse exemplo especifica o *radiusauthindex* de índice 1. Esse índice é configurado com dois perfis radius-client (1/1, 1/2). A OLT 8820 G primeiramente tenta a autenticação usando o servidor especificado no radius-client 1/1. Se essa autenticação falhar, a OLT tenta a autenticação usando o servidor radius-client 1/2. Se essa autenticação também falhar, a OLT tenta autenticação com base na configuração do modo de autenticação no perfil system. Esse exemplo usa *radiusthenlocal*.

> ⚠ **Cuidado:** se o modo de autenticação de usuário for configurado apenas para radius, a autenticação local é desabilitada. Desta forma, caso haja algum problema com o servidor Radius (perda de conectividade ou mesmo uma alteração de configuração do servidor Radius) o acesso ao gerenciamento da OLT pode ser perdido. Aconselhamos que ao configurar acesso a OLT através de autenticação Radius, seja configurado o modo de autenticação de usuário como *radiusthenlocal*

Após concluir a configuração Radius, a OLT 8820 G exibe mensagens da atividade de login e logout do Radius no console.

```
iSH> update system 0
system    0
Please provide the following: [q]uit.
syscontact: ------------------>       {:
sysname: ---------------------->       {}:
syslocation: ------------------>       {}:
enableauthtraps: -------------->       {disabled}:
setserialno: ------------------>       {0}:
zmsexists: -------------------->       {false}:
zmsconnectionstatus: ---------->       {inactive}:
zmsipaddress: ----------------->       {0.0.0.0}:
configsyncexists: ------------->       {false}:
configsyncoverflow: ------------>       {false}:
configsyncpriority: ------------>       {high}:
configsyncaction: ------------->       {noaction}:
configsyncfilename: ------------>       {}:
configsyncstatus: ------------->       {syncinitializing}:
configsyncuser: ---------------->       {}:
configsyncpasswd: ------------->       {** private **}:   ** read-only
** numshelves: ---------------->       {1}:
shelvesarray: ----------------->       {}:
numcards: --------------------->       {1}:
ipaddress: -------------------->       {192.168.10.1}:
alternateipaddress: ----------->       {0.0.0.0}:
```

```
countryregion: ---------------->       {us}:
ryclocksource: ---------------->       {0/0/0/0/0}:
ringsource: ------------------->       {internalringsourcelabel}:
revertiveclocksource: -------->       {true}:
voicebandwidthcheck: --------->       {false}:
alarm-levels-enabled: -------->       {critical+major+minor+warning}:
userauthmode: ----------------->       {local}: radiusthenlocal
radiusauthindex: ------------->       {0}: 1
secure: ---------------------->       {disabled}:
webinterface: ----------------->       {enabled}:
options: ---------------------->       {NONE(0)}:
reservedVlanIdStart: --------->       {0}:
reservedVlanIdCount: --------->       {0}:
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Para usuários logados através de autenticação Radius, o prompt do sistema aparece como *username@systemname*. Por exemplo, o prompt do sistema para o usuário_A configurado na OLT 8820 G que possui o system name como 8820G será exibido como "usuário_A@8820G". O system name (nome do sistema) é configurado usando o parâmetro sysname no perfil *system 0*.

7.9. Alarmes da OLT 8820 G

Gerenciador de alarmes

O gerenciador de alarmes da OLT 8820 G inclui a capacidade de visualizar os alarmes ativos no sistema (usando o comando *alarm show*) e de armazenar alarmes ativos no dispositivo.

O comando de alarme usa a sintaxe a seguir:

alarm show [summary]

Por exemplo, o comando a seguir exibe o número de alarmes ativos atualmente, o número total de alarmes, o número de alarmes apagados e cada alarme ativo com sua gravidade:

```
iSH> alarm show

************       Central Alarm Manager       ************
ActiveAlarmCurrentCount                         :1
AlarmTotalCount                                 :5
ClearAlarmTotalCount                            :4
OverflowAlarmTableCount                         :0
ResourceId               AlarmType                                        AlarmSeverity
-------------------------------------------------------------------------------------
1-1-1-0/gpononu      linkDown                                                 critical
```

A opção summary exibe o número de alarmes ativos no momento, o número total de alarmes e o número de alarmes apagados no sistema:

```
iSH> alarm show summary
************       Central Alarm Manager       ************
ActiveAlarmCurrentCount     1
AlarmTotalCount             5
ClearAlarmTotalCount        4
OverflowAlarmTableCount     0
```

O comando *alarm clear* elimina um alarme temporário que o sistema não pôde eliminar.

> ⚠ **Cuidado:** alarmes apagados com o comando *alarm clear* não serão exibidos novamente se a condição persistir. O alarme será exibido novamente somente se a condição persistir, parar, e voltar a ocorrer.

```
iSH> alarm clear
Num  ResourceId            AlarmType       AlarmSeverity
---------------------   -------------    ----------------
 1    1-1-1-0/gpononu      linkDown           critical

Caution: use this option with discretion.
   Alarm will not be redisplayed if condition reoccurs. Alarm will redisplay only
   if condition reoccurs, goes away, and then reoccurs.
Enter alarm number from list, or 'q' to quit: 1

   Alarm successfully deleted
Enter alarm number from list, or 'q' to quit: q
```

O comando *alarm clear* elimina alarmes apenas um de cada vez pelo número de alarme exibido na coluna *Num.*

```
iSH> alarm show
************       Central Alarm Manager       ************
         AlarmCurrentCount                     0
         AlarmTotalCount                       5
         ClearAlarmTotalCount                  5
         OverflowAlarmTableCount               0
There are currently no alarms in the system
```

Supressão de alarme

O recurso de supressão de alarme permite que a notificação e saída de alarme/LED sejam desabilitadas com base no nível de gravidade dos alarmes existentes e para os alarmes futuros. Quando um nível de alarme é desabilitado, todos os alarmes existentes deste tipo são apagados do sistema, alarmes futuros deste mesmo tipo não acionam os LEDs ou relés de alarme e também não são exibidos na saída de alarmes.

A tabela a seguir lista as opções de supressão de alarme e os comportamentos resultantes. Por padrão, alarmes para todos os níveis de gravidade são habilitados.

Configuração de níveis de alarme habilitados	Comportamento de alarme
critical+major+minor+warning	Habilita todos os níveis de alarme. Configuração padrão
critical+major+minor	Desabilita todos os alarmes warning
critical+major	Desabilita todos os alarmes minor e warning
critical+major+warning	Desabilita todos os alarmes minor
critical+minor+warning	Desabilita todos os alarmes major
critical+minor	Desabilita todos os alarmes major e warning
critical+warning	Desabilita todos os alarmes major e minor
critical	Desabilita todos os alarmes major, minor e warning
major	Desabilita todos os alarmes critical, minor e warning
major+minor+warning	Desabilita todos os alarmes critical
major+minor	Desabilita todos os alarmes critical e warning
major+warning	Desabilita todos os alarmes critical e minor
minor	Desabilita todos os alarmes critical, major e warning
minor+warning	Desabilita todos os alarmes critical e major
(no levels)	Desabilita todos os níveis de alarme

Opções de supressão de alarme

Este exemplo desabilita notificação de alarme/LED e saída para todos os alarmes atuais e futuros com os níveis de gravidade minor e warning.

```
iSH> update system 0
system    0
Please provide the following: [q]uit.
syscontact: --------------> {}:
```

```
sysname: ----------------> {}:
syslocation: -------------> {}:
enableauthtraps: ---------> {disabled}:
setserialno: -------------> {0}:
zmsexists: ---------------> {false}:
zymsconnectionstatus: ----> {inactive}:
zmsipaddress: ------------> {0.0.0.0}:
configsyncexists: --------> {false}:
configsyncoverflow: ------> {false}:
configsyncpriority: ------> {high}:
configsyncaction: --------> {noaction}:
configsyncfilename: ------> {}:
configsyncstatus: --------> syncinitializing}:
configsyncuser: ----------> {}:
configsyncpasswd: --------> {** private **}:   ** read-only **
numshelves: --------------> {1}:
shelvesarray: ------------> {}:
numcards: ----------------> {1}:
ipaddress: ---------------> {192.168.10.1}:
alternateipaddress: ------> {0.0.0.0}:
countryregion: -----------> {us}:
primaryclocksource: ------> {0/0/0/0/0}:
ringsource: --------------> {internalringsourcelabel}:
revertiveclocksource: ----> {true}:
voicebandwidthcheck: -----> {false}:
alarm-levels-enabled: ----> {critical+major+minor+warning}: critical+major
userauthmode: ------------> {local}:
radiusauthindex: ---------> {0}:
secure: ------------------> {disabled}:
webinterface: ------------> {enabled}:
options: -----------------> {NONE(0)}:
reservedVlanIdStart: -----> {0}:
reservedVlanIdCount: -----> {0}:
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Alarmes padrão Ethernet

Insira o comando *port show alarm interface/type* para visualizar o nível de gravidade de alarme nas portas Ethernet. O padrão para portas de uplink Ethernet é critical.

```
iSH> port show alarm 1-1-2-0/eth
Interface    Alarm severity     Status trap
1-1-2-0/eth  CRITICAL           ENABLED
```

Gravidade do alarme configurável para portas Ethernet

A gravidade de alarme para portas Ethernet pode ser configurada conforme os níveis a seguir:

critical, major, minor ou warning.

Alteração do nível de gravidade de alarme para uma porta Ethernet

Use o comando *port config alarm interfaceName/type severity <severity level>* para definir o nível de gravidade em uma porta Ethernet.

1. Visualize a configuração de alarme atual em uma porta Ethernet;

```
iSH> port show alarm 1-1-4-0/eth
Interface       Alarm severity          Status trap
1-1-4-0/eth     CRITICAL                ENABLED
```

2. Para configurar um alarme diferente em uma porta Ethernet;

```
iSH> port config alarm 1-1-4-0/eth severity major
Alarm severity level set for 1-1-4-0/eth is major
```

3. Verifique a nova configuração do alarme.

```
iSH> port show alarm 1-1-4-0/eth
Interface       Alarm severity          Status trap
1-1-4-0/eth     MAJOR                   ENABLED
```

Alteração do nível de gravidade de alarme para múltiplas portas Ethernet

Use o comando *port config alarm interfaceName/type severity <severity level>* para definir o nível de gravidade em múltiplas portas Ethernet.

1. Visualize os níveis de alarme para todas as portas de uplink Ethernet;

```
iSH> port show alarm 1-1-*-*/eth
Interface       Alarm severity          Status trap
1-1-9-0/eth     CRITICAL                ENABLED
1-1-8-0/eth     CRITICAL                ENABLED
1-1-7-0/eth     CRITICAL                ENABLED
1-1-6-0/eth     CRITICAL                ENABLED
1-1-5-0/eth     CRITICAL                ENABLED
1-1-4-0/eth     MAJOR                   ENABLED
1-1-3-0/eth     CRITICAL                ENABLED
1-1-2-0/eth     CRITICAL                ENABLED
1-1-1-0/eth     CRITICAL                ENABLED
```

2. Altere a configuração de alarme de todas as portas;

```
iSH> port config alarm 1-1-*-*/eth severity critical
Alarm severity level set for 1-1-8-0/eth is critical
Alarm severity level set for 1-1-7-0/eth is critical
Alarm severity level set for 1-1-6-0/eth is critical
Alarm severity level set for 1-1-5-0/eth is critical
Alarm severity level set for 1-1-4-0/eth is critical
Alarm severity level set for 1-1-3-0/eth is critical
Alarm severity level set for 1-1-2-0/eth is critical
Alarm severity level set for 1-1-1-0/eth is critical
```

3. Verifique o nível de gravidade do alarme.

```
iSH> port show alarm 1-1-*-*/eth
Interface       Alarm severity          Status trap
1-1-9-0/eth     CRITICAL                ENABLED
1-1-8-0/eth     CRITICAL                ENABLED
1-1-7-0/eth     CRITICAL                ENABLED
1-1-6-0/eth     CRITICAL                ENABLED
1-1-5-0/eth     CRITICAL                ENABLED
1-1-4-0/eth     CRITICAL                ENABLED
1-1-3-0/eth     CRITICAL                ENABLED
1-1-2-0/eth     CRITICAL                ENABLED
1-1-1-0/eth     CRITICAL                ENABLED
```

7.10. Restaurando padrão de fábrica

Restauração via interface de linha de comando

Acessar a interface de linha de comando da OLT e seguir o procedimento:

1. Executar o comando *set2default* e responder às perguntas confirmando que deseja realizar a restauração.
   Continue? (yes or no) [no]: ***yes***
   Ok to reset to default (system will reboot) ? [yes] or [no]: ***yes***
   Do you want to exit from this request? (yes or no) [yes] ***no***
   Are you sure? (yes or no) [no] ***yes***

```
iSH>
iSH> set2default
No restore file (/card1/onreboot/restore) found.
Setting to default will result in an empty database.
Continue? (yes or no) [no]: yes


************************************************************
ALL CONFIGURATION DATA on this MXK SYSTEM will be LOST IF YOU
PROCEED WITH THIS STEP!
************************************************************

Ok to reset to default (system will reboot) ? [yes] or [no]: yes

Do you want to exit from this request? (yes or no) [yes] no

Are you sure? (yes or no) [no] yes
Saving default console baud rate settings 9600 baud in NVRAM.
Please adjust the console baud rate accordingly.
```

7.11. Upgrade de firmware da OLT

Para atualização do firmware da OLT é necessária a utilização de um servidor TFTP para transferência dos arquivos necessários à atualização.

Upgrade via interface de linha de comando

Acessar a interface de linha de comando da OLT e seguir o procedimento:

1. Importar a imagem do firmware e o software WEB-GUI para a OLT.
   » iSH>image download ip-server-tftp mx1u19x-versão.bin /card1/mx1u19x.bin

   Exemplo:

```
zSH> image download 10.10.10.12 mx1u19x-2.5.1.423.bin /card1/mx1u19x.bin
Image download to: /card1/mx1u19x.bin
Bytes copied:  11931199
Image download successful
```

   » iSH>file download ip-server-tftp Intelbras-mx1u19x_http-versão.tar /card1/mx1u19x_http.tar

   Exemplo:

```
zSH> file download 10.10.10.12  Intelbras-mx1u19x_http-2.5.1.423.tar /card1/mx1u19x_http.tar
Bytes copied:   8495616
File download successful
```

2. Reiniciar a OLT.

```
zSH>
zSH> reboot
Rebooting...
```

Obs.: » *A OLT possui dois arquivos para sua atualização (mx1u19x-versão.bin e Intelbras-mx1u19x_http-versão.tar).*

» *O arquivo* mx1u19x-versão.bin *é a imagem/firmware da OLT que DEVE ser colocado na raiz do sistema "/card1" e DEVE possuir o nome mx1u19x.bin.*

» *O arquivo* Intelbras-mx1u19x_http-versão.tar *é o software da WEB-GUI que DEVE ser colocado na raiz do sistema "/card1" e DEVE possuir o nome mx1u19x_http.tar.*

» *O comando* image download *DEVE ser utilizado para copiar o firmware atualizado do servidor TFTP para dentro do sistema da OLT.*

» *O comando* file download *DEVE ser utilizado para copiar qualquer arquivo, exceto o firmware, do servidor TFTP para dentro do sistema da OLT.*

Upgrade em caso de crash ou perda de usuário e/ou senha

1. Conectar-se através da porta serial na OLT que, por sua vez, possui a seguinte configuração.
   - » 9600 bps.
   - » 8 bits de dados.
   - » Sem paridade.
   - » 1 bit de parada.
   - » Sem controle de fluxo.
2. Desligar e ligar a OLT.

```
iSH>
Starting mx1U19xROM.
MX 2.2.1.211  Created on: Sep 13 2011, 21:23:57
No CPLD on mx1U
Preparing to load full image...
```

3. Assim que a mensagem acima aparecer, digite "*zhone*" e pressione "*enter*" seguidamente, até interromper o boot.

```
iSH>
Starting mx1U19xROM.
MX 2.2.1.211  Created on: Sep 13 2011, 21:23:57
No CPLD on mx1U
Preparing to load full image...


Boot process interrupted.
```

4. Adicionar um IP temporário na porta 1 (na mesma sub-rede que o servidor TFTP).

```
zSH> ipconfig 10.10.10.14 255.255.255.0
zSH>
zSH>
```

5. Importar a imagem do firmware e o software WEB-GUI para a OLT.

   iSH> image download ip-server-tftp mx1u19x-versão.bin /card1/mx1u19x.bin

   Exemplo:

```
zSH> image download 10.10.10.12 mx1u19x-2.5.1.423.bin /card1/mx1u19x.bin
Image download to: /card1/mx1u19x.bin
Bytes copied:  11931199
Image download successful
```

   iSH> file download ip-server-tftp Intelbras-mx1u19x_http-versão.tar /card1/mx1u19x_http.tar

   Exemplo:

```
zSH> file download 10.10.10.12  Intelbras-mx1u19x_http-2.5.1.423.tar /card1/mx1u19x_http.tar
Bytes copied:   8495616
File download successful
```

Obs.: » *A OLT possui dois arquivos para sua atualização (mx1u19x-versão.bin e Intelbras-mx1u19x_http-versão.tar).*

- » *O arquivo* mx1u19x-versão.bin *é a imagem/firmware da OLT que DEVE ser colocado na raiz do sistema "/card1" e DEVE possuir o nome mx1u19x.bin.*
- » *O arquivo* Intelbras-mx1u19x_http-versão.tar *é o software da WEB-GUI que DEVE ser colocado na raiz do sistema* /card1 *e DEVE possuir o nome* mx1u19x_http.tar.
- » *O comando* image download *DEVE ser utilizado para copiar o firmware atualizado do servidor TFTP para dentro do sistema da OLT.*
- » *O comando* file download *DEVE ser utilizado para copiar qualquer arquivo, exceto o firmware, do servidor TFTP para dentro do sistema da OLT.*

6. Reiniciar a OLT.

```
zSH>
zSH> reboot
Rebooting...
```

8. GPON na OLT 8820 G

Embora este guia seja principalmente voltado à configuração da OLT 8820 G, também é importante entender a tecnologia subjacente.

> **Observação:** todos os comandos que começam com *gpononu* ou *gponolt* podem ser substituídos por *onu* ou *olt* respectivamente. Por exemplo: > gpononu set é o mesmo que > *onu set* ; > *gponolt show bw* é o mesmo que > *olt show bw*

8.1. Terminologia GPON

Componentes GPON de uma ODN (optical deployment networks)

Redes ópticas são compreendidas por diversos componentes entre os dispositivos associados.

- **OLT**

  Optical Line Terminator. Este dispositivo é considerado como o terminal da ODN (observe que cada porta GPON é considerado como uma OLT).

- **Fibra óptica**

  A fibra óptica é o cabo físico.

- **Splitter ópticos (somente GPON)**

  Splitters ópticos dividem um único sinal óptico em diversos sinais ópticos.

- **Acopladores**

  Acopladores são meios conectorizados para cabos emendados e possui perda de sinal.

- **ONT ou ONU**

  Optical Network Terminator (ONT) e Optical Network Unit (ONU) são termos consideravelmente semelhantes definidos nas normas ITU-T G.984 GPON. Ambos oferecem uma terminação para a ODN e conversão a alguma mídia elétrica. Entretanto, ONTs normalmente têm diversos serviços e interfaces para os assinantes, como Ethernet LAN, FXS e WiFi. ONUs teriam um uplink de interface GPON (como na ONT), mas na direção downstream elas oferecem portas de acesso de cobre de última milha, como VDSL2 ou Fast Ethernet, que conectam-se a equipamentos nas instalações do cliente, como um modem VDSL2 ou Switch ou roteador.

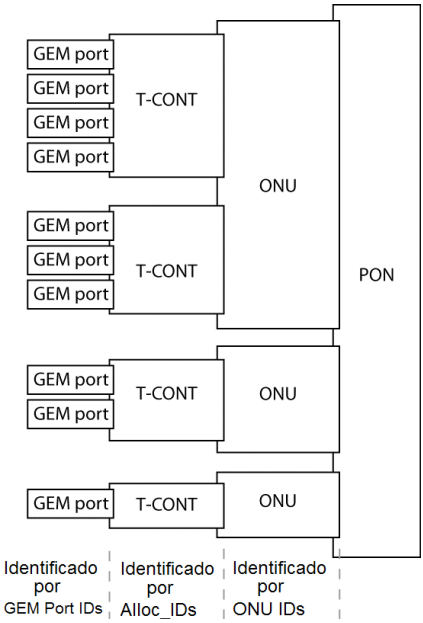
- **Atenuadores**

  Atenuação é o termo para a perda de energia óptica na ODN. Alguns dispositivos podem receber uma energia óptica muito forte, devido a característica do receptor. Essa situação normalmente ocorre em configurações em laboratório. Um atenuador pode ajustar essa potência óptica.

Todos os componentes de fibra mencionados acima são importantes no planejamento e na instalação de redes GPON.

Relação entre T-conts e GEM Ports

A imagem a seguir exibe a relação entre T-conts e GEM Ports.



Relação entre T-conts e GEM Ports

» **T-Conts**

Transmission Containers (T-conts) é como a ONU representa um grupo de conexões lógica que aparecem como uma entidade única de comportamente de tráfego, com a finalidade de atribuir largura de banda no lado upstream da ONU.

Cada ONU possui um ou mais T-conts. A OLT descobre o número de T-conts suportados pela ONU e atribui Alloc IDs para as T-conts da ONU. Alloc ID é o identificador de um T-cont.

Cada T-cont contém uma ou mais GEM Ports. O Alloc ID é atribuído a um T-cont durante a criação da GEM Port.

A alocação de largura de banda em um T-cont é definida no perfil de tráfego GPON (GTP). Múltiplas GEM Ports podem compartilhar um T-cont habilitando o recurso compartilhado no perfil de tráfego GPON associado.

» **GEM Ports**

GEM (GPON Encapsulation Method) Ports são como as ONUs separam os serviços do lado upstream da ONU para as portas downstream. Cada uma dessas GEM Ports precisa ser única na ODN na porta OLT (porta GPON).

GEM Port ID é o identificador de uma GEM Port. Há duas formas de atribuição dos GEM Port ID durante o provisionamento OMCI: forma dinâmica ou arbitrária.

As GEM Ports são dinamicamente criadas durante a realização dos comandos *bridge add* ou *interface add*, da mesma forma, elas podem ser excluídas com os comandos *bridge delete* ou *interface delete*.

A modelagem de tráfego de uma GEM Port é definida em um perfil de gerenciamento de tráfego CPE (CPE traffic management).

8.2. Comando bridge add utilizando USP (Unified Service Provisioning)

O comando *bridge add* define o tipo de transporte e porta OLT e possui a seguinte sintaxe: shelf-slot-port-subport/transport type.

Como a OLT 8820 G não possui módulos expansores de portas GPON, os campos shelf e slot sempre são fixos em 1, o campo port é a porta física da OLT e o campo subport é a interface de identificação e está associado ao campo transport type (tipo de transporte).

Baseado no método de provisionamento USP, segue a sintaxe do comando bridge add (assumindo que o parâmetro GTP já esteja configurado).

- O comando *bridge add* define o tipo de transporte e porta da OLT e possui a seguinte sintaxe: *shelfID-slotID-OLTportID-ONUportID/gpononu*. Perceba que o campo GemportID pode ser omitido, desta forma a OLT atribuirá automaticamente um valor de GemPort dentro do range 257 a 3828 para a bridge interface.
- Opcionalmente pode-se atribuir um valor de GemPort através do comando bridge add, para este caso, deve-se inserir a opção *gem GEMportID* utilizando a seguinte sintaxe: *shelfID-slotID-OLTportID-ONUportID/gpononu gem GEMportID*. Com este formato, qualquer GEMportID dentro do range 257 a 3828 pode ser associado com qualquer ONU, exceto a GemPort 5xx, onde esta faixa é destinada ao uso da função de gerenciador de CPE e os dois últimos dígitos desta faixa devem ser igual a posição da ONU na porta PON (xx pode variar de 1 a 64). Por exemplo, GEMportID 501 pertence a ONU que está na posição 1 da referida porta PON e GEMportID 564 pertence a ONU que está na posição 64 da referida porta PON.

```
iSH> bridge add 1-1-2-20/gpononu downlink vlan 201 tagged eth 1
Adding bridge on 1-1-2-20/gpononu
Created bridge-interface-record 1-1-2-257-gponport-201/bridge
CPE Connection 1-1-2-257/gponport/1/1/0/0 has been created

iSH> bridge add 1-1-2-24/gpononu gem 734 downlink vlan 101 tagged eth 1
Adding bridge on 1-1-2-24/gpononu
Created bridge-interface-record 1-1-2-734-gponport-101/bridge
CPE Connection 1-1-2-734/gponport/1/1/0/0 has been created
```

8.3. Comando bridge add com utilização de range de porta OLT, subporta OLT e Portas UNI

O comando *bridge add* pode ser realizado de forma massiva, os campos OLTportID, ONUportID, Ethernet UNI port ID e WLAN UNI port ID aceitam ranges de valores, desde que o campo desejado esteja entre colchetes "[ ]" e os valores atribuídos sejam separados por virgula "," (para valores não sequenciais) ou por hífen "-" (para valores sequenciais). Para Ethernet UNI port e WLAN UNI port, a palavra curinga "all" pode ser usada também.

A seguir alguns exemplos utilizando o comando *bridge add* especificando portas não sequenciais, portas sequenciais e a palavra curinga. O comando *bridge add* deve ser utilizado com a seguinte sintaxe: *shelfID-slotID-OLTportID-ONUportID/gpononu*.

- **Especificando um range para o campo OLTportID**

  Este exemplo especifica o shelfID 1, slotID 1, as portas PON 1,2,3 e 4 (OLTportIDs), a ONU da posição 4 com GEMportID 604.

```
iSH> bridge add 1-1-[1-4]-4/gpononu gem 604 gtp 1 downlink vlan 504 tagged eth 1
To Abort the operation enter Ctrl-C
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-604-gponport-504/bridge
Adding bridge on 1-1-2-4/gpononu
Created bridge-interface-record 1-1-2-604-gponport-504/bridge
Adding bridge on 1-1-3-4/gpononu
Created bridge-interface-record 1-1-3-604-gponport-504/bridge
Adding bridge on 1-1-4-4/gpononu
Created bridge-interface-record 1-1-4-604-gponport-504/bridge
```

» **Especificando um range para o campo SubportID**

Este exemplo especifica o shelfID 1, slotID 1, Porta PON 1 (OLTportID) e as ONUs da posição 20 a 23 (ONUportIDs).

```
iSH> bridge add 1-1-2-[20-23]/gpononu downlink vlan 101 tagged eth 1

To Abort the operation enter Ctrl-C

Adding bridge on 1-1-2-20/gpononu
Created bridge-interface-record 1-1-2-257-gponport-101/bridge
CPE Connection 1-1-2-257/gponport/1/1/0/0 has been created
Adding bridge on 1-1-2-21/gpononu
Created bridge-interface-record 1-1-2-258-gponport-101/bridge
CPE Connection 1-1-2-258/gponport/1/1/0/0 has been created
Adding bridge on 1-1-2-22/gpononu
Created bridge-interface-record 1-1-2-259-gponport-101/bridge
CPE Connection 1-1-2-259/gponport/1/1/0/0 has been created
Adding bridge on 1-1-2-23/gpononu
Created bridge-interface-record 1-1-2-260-gponport-101/bridge

CPE Connection 1-1-2-260/gponport/1/1/0/0 has been created
```

» **Especificando um range de portas ethernet da ONU (UNI Ports)**

Este exemplo especifica o shelfID 1, slotID 1, a porta PON 1 (OLTportID), a ONU da posição 63 com GEMportID 306 e as portas ethernet da ONU 1 e 2 (UNI Ports).

```
iSH> bridge add 1-1-1-63/gpononu gem 306 downlink vlan 3811 tagged eth [1,2]
Adding bridge on 1-1-1-63/gpononu
Created bridge-interface-record 1-1-1-306-gponport-3811/bridge
CPE Connection 1-1-1-306/gponport/1/1/0/0 has been created
CPE Connection 1-1-1-306/gponport/1/2/0/0 has been created
```

» **Especificando todas as portas ethernet e WLAN (UNI Ports).**

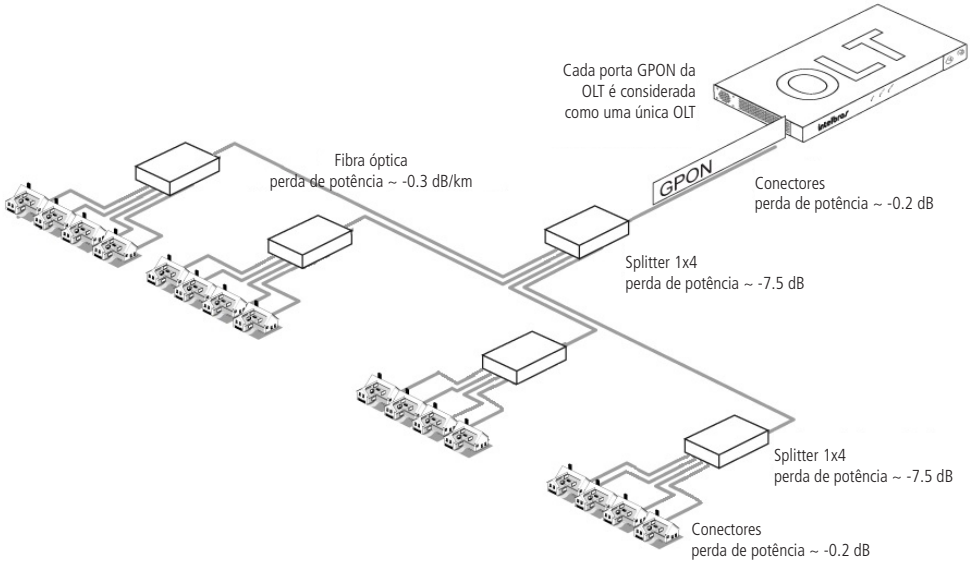
Este exemplo especifica o shelfID 1, slotID 1, a porta PON 1 (OLTportID), a ONU da posição 63 com GEMportID 363 e todas as portas ethernet e SSIDs da ONU.

```
iSH> bridge add 1-1-1-63/gpononu gem 306 downlink vlan 3811 tagged eth all wlan all rg-brouted
Adding bridge on 1-1-1-63/gpononu
Created bridge-interface-record 1-1-1-306-gponport-3811/bridge
CPE Connection 1-1-1-306/gponport/1/1/0/0 has been created
CPE Connection 1-1-1-306/gponport/1/2/0/0 has been created
CPE Connection 1-1-1-306/gponport/1/3/0/0 has been created
CPE Connection 1-1-1-306/gponport/1/4/0/0 has been created
CPE Connection 1-1-1-306/gponport/18/1/0/0 has been created
CPE Connection 1-1-1-306/gponport/18/2/0/0 has been created
CPE Connection 1-1-1-306/gponport/18/3/0/0 has been created
CPE Connection 1-1-1-306/gponport/18/4/0/0 has been created
```

8.4. Planejamento de redes GPON

Ao implementar redes GPON, você deve pensar em termos ópticos em vez de termos elétricos ou baseados em cabos de cobre. Com soluções à base de cobre, você pensa na distância e na tecnologia de transporte (a distância dos assinantes com o CO é uma questão importante quando tratamos de conexões ADSL ou VDSL). Em redes baseadas em fibras óptica, especialmente GPON, você tem de pensar em termos de orçamentos de potência e suas perdas em conexões opticas.

A perda nos enlaces é a quantidade de atenuação de sinal óptico a medida em que se aumenta a distância entre a OLT e os assinantes (ONU). Cada componente, incluindo o próprio cabo de fibra óptica, degrada o sinal. Atenuação é o termo usado para descrever a quantidade de degradação do sinal óptico.



Atenuações em uma rede GPON

O planejamento de uma rede GPON deve incluir um mapa de orçamento de perda de potência onde são exibidos a perda de cada componente, até mesmo o comprimento de cada fibra, que afeta a atenuação do sinal óptico. Como as fibras utilizadas no GPON são conectaos a diversos splitters (divisores ópticos) e cada splitter possui uma perda específica, este orçamento de perda de potência é um requisito importante no planejamento de uma rede GPON. A tabela a seguir exibe os valores típicos utilizados para calcular a perda de potência óptica.

Observação: a perda de potência óptica pode variar de acordo com o fabricante, consulte o fornecedor de cada componente óptico para maiores detalhes

Componente	Perda óptica
Fibra óptica	- 0,3 dB por quilômetro
Splitters	A perda óptica de cada splitter depende do número de divisões existentes: » 1/2 (2 divisões): -4 dB » 1/4 (4 divisões): -7,5 dB » 1/8 (8 divisões): -11 dB » 1/16 (16 divisões): -14 dB » 1/32 (32 divisões): -18 dB » 1/64 (64 divisões): -21,5 dB
Emendas	-0,1 dB
Conectores	-0,2 dB

Componentes de redes GPON e suas perdas ópticas

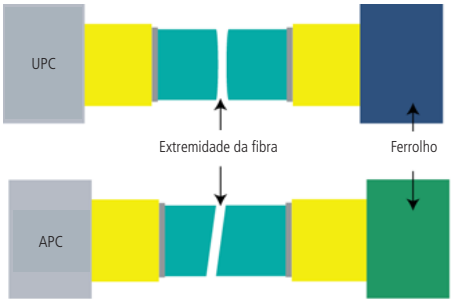
8.5. Teste de instalação

O mapa teórico do orçamento de perda de potência é muito importante ao instalar a fibra. Devem ser feitos testes antes e após a adição de cada componente da rede óptica. Ao corresponder os valores de atenuação de sinal real com a atenuação teórica elaborada através do mapa de orçamento de portência é possível identicar alguns problemas como:

» Macro curvatura no cabo (raio de curvatura muito pequeno).

» Perda de retorno é a perda causada por reflexão do sinal nas conectorizações existentes entre a extremidade final da fibra e um conector, ou em uma emenda.

» "Casamento" incorreto entre conectores UPC e APC podem causar perdas de retorno. Conectores UPC (Ultra Physical Contact) possuem a extremidade final da fibra levemente esférica. Conectores APC (Angled Physical Contact) possuem um ângulo padronizado na extremidade final da fibra. (Mas você deve estar ciente que os conectores APC antigos podem não estar no padrão, possuindo ângulos diferentes na extremidade da fibra.



Extremidade dos conectores UPC e APC

Há ferramentas de teste no mercado que podem ser usadas para testar os componentes conforme são adicionados.

Os valores reais descobertos durante os testes de instalação também devem ser anotados e arquivados pois podem ajudar na resolução de problemas que podem surgir futuramente na rede GPON (ODN).

9. Configuração de BRIDGING

A OLT 8820 G fornece várias plataformas de acesso integrado de alto desempenho e alta densidade, oferecendo flexibilidade aos prestadores de serviços, o que possibilita atender as necessidades do mercado.

Serviços de bridging geralmente são configurados com o comando *bridge add*. O comando *bridge add* cria uma interface lógica especificando os parâmetros para a interface de bridge (tipo de bridge, ID de VLAN, tagging, opções de COS e outros parâmetros). Essa interface lógica é sobreposta em uma interface física como a interface Ethernet ou GPON.

9.1. Visão geral

O encaminhamento da informação pode ocorrer na forma de pacotes (IP) ou quadros (bridging).

» Quadros (frames) são entregues com base em um endereço MAC (briding ou camada 2 do modelo de referencia OSI).

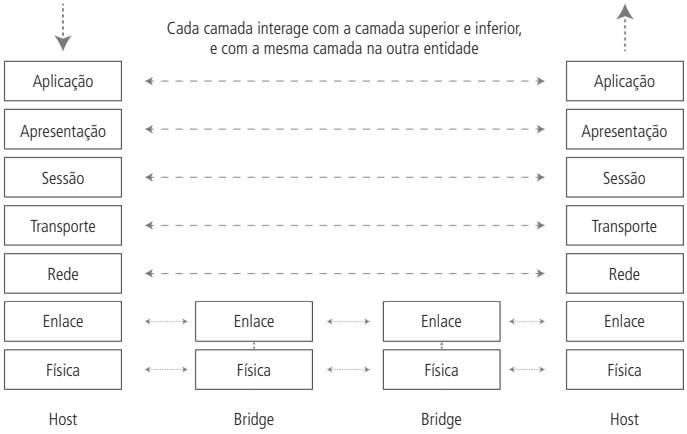
» Pacotes são entregues com base em um endereço IP (routing ou camada 3 do modelo de referencia OSI).

As camadas mencionadas acima são parte do modelo de referência OSI (Open Systems Interconnection). Embora nem todos os protocolos sigam o modelo OSI, o modelo OSI é útil para entender as variações da funcionalidade da rede.

Camada	Nome	Função	
7	Aplicação	Processos de rede e interações de aplicação	Camadas de Host
6	Apresentação	Mapeamento entre a camada de aplicação e camadas inferiores - apresentação de dados e criptografia	
5	Sessão	Gerencia conexões entre a aplicação local e a remota	
4	Transporte	Gerencia conexões fim a fim, confiabilidade, rastreia segmentos e retransmissão (controle de erros)	
3	Rede	Funções de roteamento. Transferência de dados de origem para o destino. O protocolo da camada 3 mais conhecido é o Internet Protocol (IP)	Camadas de Mídia
2	Enlace	Transferência de dados entre entidades de rede	
1	Físico	Relação entre o meio de transporte (cobre, fibra, sem fio) e os dispositivos	

Modelo de Referência OSI (Open Systems Interconnection)

Se uma aplicação em um host solicitar informações de outra aplicação de rede em outro host (por exemplo, clicando em um link para outra página em um navegador), as solicitações progridem para baixo entre as camadas até serem transmitidas em uma mídia física (cabo, fibra óptica, sinal sem fio) até que a mensagem seja coletada em outro terminal progredindo para cima entre as camadas, conforme é exibido na imagem a seguir. A resposta segue o mesmo processo.



Informações de rede solicitada pelas aplicações

As bridges direcionam os quadros com base nas informações do endereço do quadro e nas informações aprendidas do processamento e do direcionamento de outros quadros. O processamento e o direcionamento de quadros é o aprendizado, encaminhamento ou a filtragem feita pelo dispositivo. A quantidade de processamento e informações lidas do quadro é mantida a um nível mínimo para aprimorar a velocidade de transferência do dispositivo.

9.2. Terminologia e conceitos

Porta física

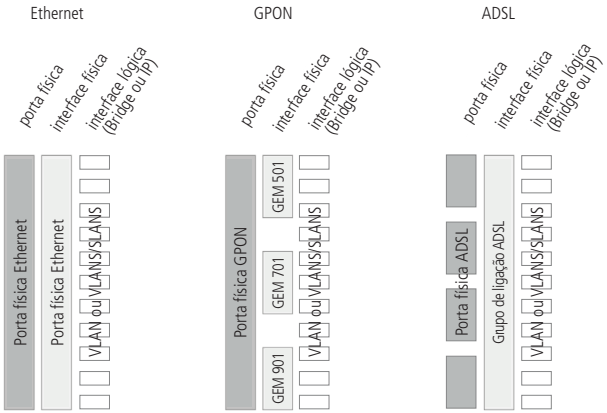
A porta física é a conexão física em um dispositivo, essencialmente a porta física atua na camada 1. Exemplos de portas físicas incluem:

- Meio físico Ethernet (Fast Ethernet ou Gigabit Ethernet)
- Par de fios individuais para FXS ou xDSL
- Porta OLT GPON
- Porta ONU GPON

A porta física não é necessariamente o conector físico. Um conector Champ pode ter 50 pares individuais de cabos. A porta física, neste caso, é o par individual de cabos. A porta física em GPON seria a conexão de fibra óptica, entretanto, essa conexão pode ser e normalmente será compartilhada com diversos dispositivos dos assinantes.

Interface física

Uma interface física pode ser constituída por todas as portas físicas, um subconjunto de portas físicas ou um grupo de portas físicas dependendo dos recursos da tecnologia de transporte, conforme exibido na imagem a seguir.



A porta física, a interface física e a interface lógica variam por tecnologia de transporte e recursos de ligação

O mapeamento de portas físicas para interfaces físicas pode ser:

- » Inteiramente por uma porta física. Por exempplo Ethernet, a interface física é inteiramente a porta física.
- » Um subconjunto de uma porta física. Por exemplo GPON, as GEM Ports são usadas para separar uma porta física única em diversas portas virtuais.
- » Um grupo de portas físicas. Um combinado de múltiplas portas físicas em uma única interface lógica.

Interfaces lógicas são associadas com interfaces físicas.

Interface lógica

Há dois tipos de interfaces lógicas - interfaces bridge e interfaces IP. Essas interfaces podem ser associadas com todo o tráfego ou parte do tráfego em uma interface física. Quando a interface lógica é fragmentada em conexões, essas conexões são identificadas por um VLAN ID (Virtual Local Area Network Identifier) ou uma conexão virtual GPON (GEM Ports) para tecnologias de conexão como GPON.

Bridges e bridges interfaces

Uma bridge é um grupo de bridge interfaces que compartilham um atributo comum para formar uma comunidade de interesse. O atributo que define a comunidade de interesse é o VLAN ID ou uma combinação de SLAN ID e VLAN ID.

Quadros recebidos em uma interface pertencendo a uma bridge somente podem ser enviados a outras interfaces no sistema pertencente à mesma bridge. Muitas bridges podem existir no sistema ao mesmo tempo, cada uma definida pelo VLAN ID ou SLAN ID / VLAN ID.

Bridges conectam segmentos de rede. As extremidades da bridge são as bridge interfaces, conforme definido no perfil *bridge-interface-record*.

Diferentemente de um repetidor, que possui duas interfaces e recebe dados em uma interface e transfere para a outra (normalmente para fortalecer o sinal) ou de um hub que possui mais de duas interfaces e quando recebe dados em uma dessas interfaces, esse dado é encaminhado para todas as outras interfaces, as bridges são mais complexas. Bridges analisam os quadros de dados recebidos para determinar para onde encaminhar cada quadro. Determina-se no dispositivo através de uma configuração de bridge onde os dados chegam (entrada) e para onde os dados serão enviados (saída). A OLT Intelbras usa principalmente dois tipos de bridges - bridges Transparent LAN Services (TLS) (que são chamadas de simétricas porque todas as bridge interface têm o mesmo comportamento) e bridges assimétricas, que podem ser divididas em três tipos de bridge interface diferentes, cada um com seu próprio comportamento.

Quadros que entram em uma bridge interface não são encaminhados de volta para a mesma bridge interface.

VLANs e SLANs, untagged, tagged e stagged

VLANs e SLANs são normalmente utilizadas para separar o tráfego em tipos de serviços, como por exemplo, serviços Triple Play (voz, vídeo e dados). Serviços de voz e vídeo são fornecidos por servidores em redes privadas. As mensagens dos servidores de voz e vídeo são semelhantes e têm a mesma prioridade, somente o conteúdo é diferente. Os serviços de dados vêm de um gateway da Internet pública e o conteúdo não é tão semelhante como o de voz e vídeo.

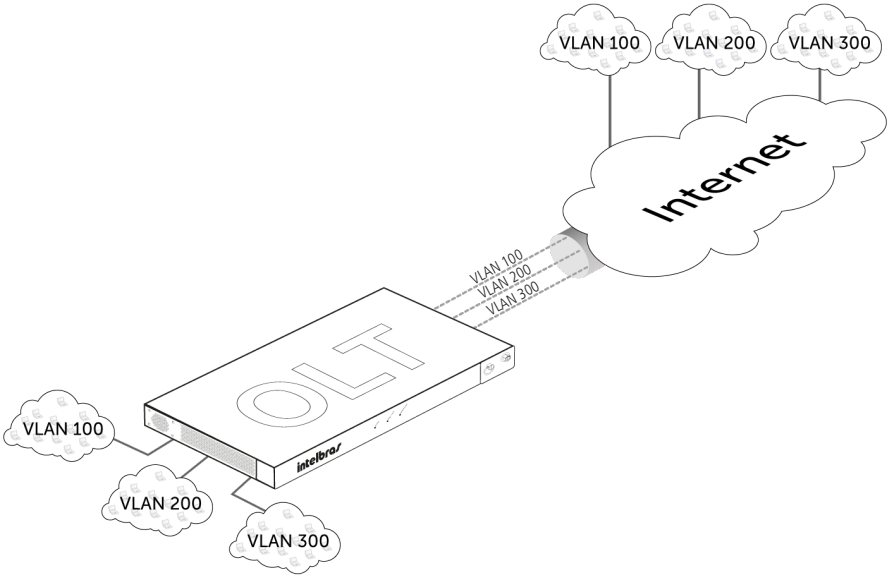
VLANs separam o tráfego de todos os serviços, portanto o tráfego conhecido é separado do tráfego desconhecido. Essa separação também oferece meios para manusear o tráfego de maneira diferente através do uso de marcações de QoS (Quality of Service) afim de priorizar tráfego de vídeo e voz.

A separação do tráfego permite outros mecanismos, como:

» Fornecer segurança porta a porta dos usuários que compartilham uma VLAN tal como Destination MAC Swapping.
» Inserir informações de identificação para servidores DHCP.
» Inserir tags para fins de idenificação como quando a OLT 8820 G é um agente intermediário PPPoE.

Outro exemplo de VLANs e SLANs é a separação de tráfego para grupos de hosts/usuários.

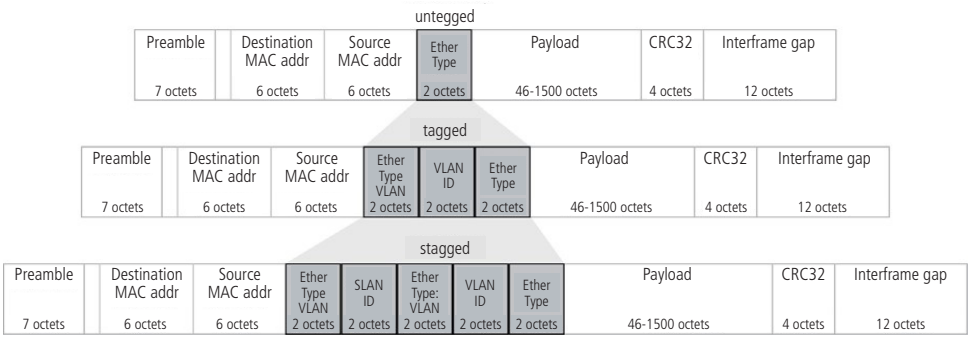
VLANs (e SLANs) também podem ser usados para identificar a origem de quadros conforme exibido na imagem a seguir.



VLANs definem a qual bridge um quadro recebido pertence

O IEEE 802.1 QinQ expandiu o espaço de VLAN no quadro de Ethernet para suportar a identificação de quadros já marcados (tagged). Essa segunda tag, uma SLAN, cria um quadro Ethernet com dupla marcação (double-tagged).

Um quadro que não possui VLAN ID é mencionado como *untagged*. Um quadro que possui um único VLAN ID (mas não um SLAN ID) é mencionado como tagged. Um quadro que possui tanto um VLAN ID como um SLAN ID (dupla marcação) é mencionado como stagged conforme exibido na imagem a seguir.



Quadros Ethernet: não marcados (untagged), com única marcação (tagged) e com dupla marcação (stagged)

Observação: os octetos de VLAN ID e SLAN ID incluem informações CoS

A Interface de Linha de Comando da OLT usa um mecanismo bastante flexível para definir as bridge interfaces. Ao adicionar uma bridge interface, você pode configurá-la para aceitar e enviar quadros não marcados (untagged), quadros marcados (tagged) e quadros com marcação dupla (stagged). Nenhum outro quadro será aceito. Se uma bridge interface estiver esperando um quadro com marcação única, usando o comando *bridge add* com a palavra-chave tagged, quadros não marcados (untagged) ou quadros com dupla marcação (stagged) não serão tratados por essa bridge interface. Se um quadro com dupla marcação (stagged) é esperado pela bridge interface, quadros não marcados (untagged) ou quadros com marcação única (tagged) não serão tratados por essa bridge interface. Esses quadros podem ser tratados por outras bridge interfaces dependendo da configuração.

Apenas uma única bridge interface untagged pode existir em uma porta ou subporta, pois os quadros não possuem um VLAN ID. Bridges untagged são criadas usando o comando *bridge add* com a palavra-chave *untagged.*

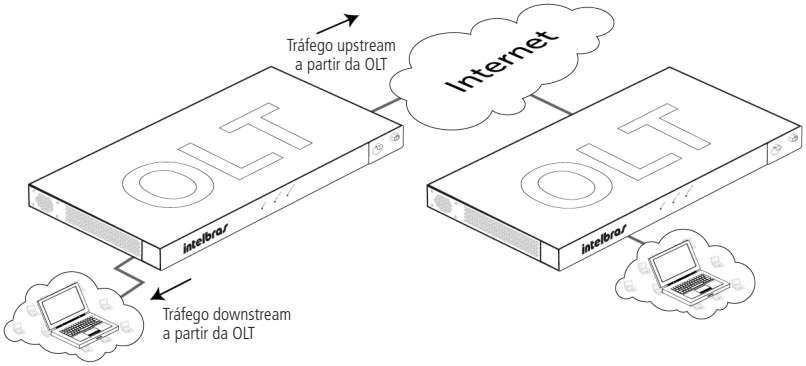
No caso de bridge do tipo, gpononu, ao utilizar o comando *bridge add* deve-se especificar a bridge interface em tagged ou stagged. Se você não designar uma opção de marcação, por padrão a bridge interface é atribuída como untagged. Todas as bridges interface criadas entre a OLT e ONU devem ser tagged ou stagged:

- **downlink**
  insira tagged
- **uplink, intralink**
  insira tagged
- **TLS**
  insira tagged
- **Wire**
  insira tagged.

Em todos os casos, deve ser designado uma VLAN e/ou uma SLAN.

Upstream e downstream

Upstream e downstream são termos situacionais e são usados de maneira centrada na OLT 8820 G. Normalmente o termo upstream significa que as interfaces físicas da OLT são voltadas (indo de encontro) ao núcleo da rede e o termo downstream significa que as interfaces físicas do dispositivo são voltadas (indo de encontro) aos usuários finais (assinantes), conforme exibido na imagem a seguir.



Sentido de tráfego upstream e downstream

Este modelo assume uma hierarquia, mas negligencia a noção de que em algum momento a transmissão de dados deve mudar de upstream para downstream (como vai de uma aplicação para outra, de um host para outro, de um usuário para outro). Em outras palavras, não há como definir o sentido do tráfego claramente em todo o modelo conceitual. Portanto, os termos upstream e downstream são usados com o entendimento geral que upstream é em direção ao núcleo da rede e downstream é em direção ao usuário final (assinante).

Os termos upstream e downstream são associados aos tipos de bridge interface uplink e downlink. Uplinks e downlinks possuem comportamentos específicos e distintos que definem as bridges.

Os termos upstream e downstream também são usados para discutir interfaces TLS. Interfaces TLS têm o mesmo comportamento para interfaces upstream e downstream, o que pode ser vantajoso para determinadas situações de acesso.

Broadcast, multicast e unicast

O objetivo de uma bridge é a transmissão de quadros. Em geral, quadros são recebidos em uma interface e a seguir são transmitidos em uma ou mais interfaces. Há três modos gerais de transmitir quadros:

Unicast

Quadros unicast são enviados para um endereço específico.

Multicast

Quadros multicast são enviados para um número limitado de entidades.

Broadcast

Quadors broadcasts são enviados a todas as entidades disponíveis, normalmente para todos os dispositivos em uma sub-rede.

O modo de aprendizado de uma bridge interface ocorre quando a interface aprende o endereço MAC de origem de um quadro recebido, desta forma o endereço MAC (assim como a VLAN e a bridge interface em que o endereço MAC foi recebido) é colocado no banco de dados de encaminhamento. Quando o endereço MAC de destino de um quadro recebido for igual ao endereço MAC aprendido pela bridge, este quadro será encaminhado para a bridge interface apropriada.

Cada tipo de bridge possui um comportamento distinto na forma de aprendizado dos endereços MAC de origem e de encaminhamento do quadro recebido para o destino correto. Os diferentes comportamentos de aprendizado e encaminhamento são discutidos nas seções a seguir - bridges simétricas e bridges assimétricas.

9.3. Tipos de bridge

A OLT 8820 G possui dois tipos de bridges (bridges simétrica e assimétrica). Bridges Simétricas possui o mesmo comportamento de bridging entre as bridge interfaces, já as Bridges Assimétricas possuem diferentes comportamentos de bridging entre as bridge interface. Bridge TLS é um exemplo de bridge simétrica e bridge de downlink e uplink são exemplos de bridge assimétrica.

O comportamento diferente destes tipos de bridge são úteis para a configuração da rede.

Bridges Simétricas utilizam as seguintes bridge interface (TLS e Wire):

» Bridge interface TLS possuem o mesmo comportamento independentemente de quais portas estão em bridge. Uma bridge interface TLS é criada com o comando *bridge add* e a palavra-chave *tls*. A bridge TLS funciona somente em conjunto com outras bridges TLS. As bridges interfaces wire são uma bridge TLS reservada, possui o mesmo comportamento independentemente de quais portas estão em bridge.

» As bridges interfaces wire é criada com o comando *bridge add* e a palavra-chave *wire*. Uma bridge wire funciona somente em conjunto com outra bridge wire e sua configuração permite que somente duas interfaces sejam configuradas por VLAN e esta VLAN deve ser única no sistema, ou seja, uma vez utilizado uma VLAN em uma bridge wire, esta VLAN não poderá ser utilizada na configuração de nenhum outro tipo de bridge.

> **Observação:** quando um VLAN ID é utilizado entre duas bridge wire, este VLAN ID não poderá ser utilizado em qualquer outro lugar no sistema da OLT

Bridges Assimétricas utilizam as seguintes bridge interface (uplink,downlink e intralink):

» **Uplink**

Bridge de uplink normalmente são utilizados para tráfego de upstream em direção ao núcleo da rede. Uma bridge interface uplink é criada com o comando *bridge add* e a palavra-chave *uplink*.

Uma bridge interface uplink funciona somente em conjunto com outras bridge interfaces assimétricas. Um bridge-path padrão é criado automaticamente.

» **Downlink**

Bridge de Downlink normalmente são utilizados para tráfego de downstream em direção aos assinantes (usuários finais da rede). Uma bridge interface downlink é criada com o comando *bridge add* e a palavra-chave *downlink*.

Uma bridge Interface downlink funciona somente em conjunto com outras bridge interfaces assimétricas.

» **Intralink**

Bridge intralink normalmente são utilizados na interconexão de OLTs.

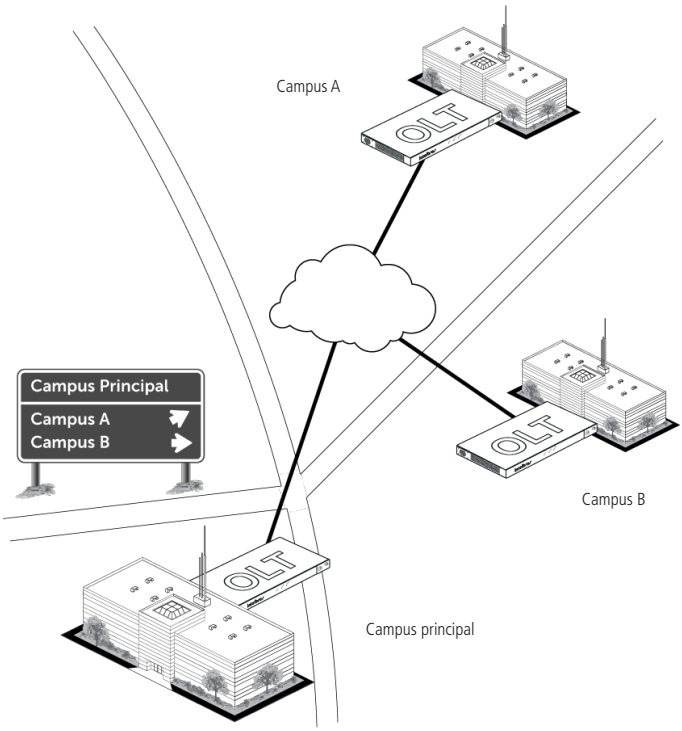
Uma bridge interface intralink é criada com o comando *bridge add* e a palavra-chave *intralink*. Um bridge-path padrão é criado automaticamente.

As bridges intralink funcionam somente em conjunto com outras bridge interfaces assimétricas.

Transparent LAN Services

Bridges TLS (Transparent LAN Services) são utilizadas quando se deseja que o tráfego flua livremente entre uma comunidade de usuários.

Por exemplo, um câmpus escolar pode utilizar bridges TLS para ampliar a sua rede LAN para diversos outros câmpus. Os câmpus remotos aparecerão como estando no mesmo segmento de LAN embora estejam geograficamente separados.



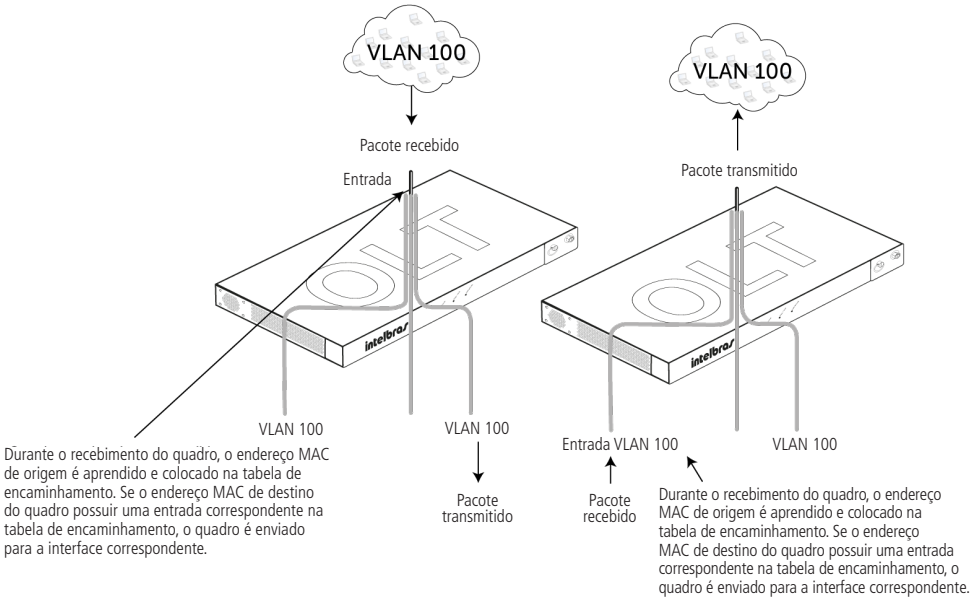
Bridges TLS unindo segmentos remotos como se fossem uma LAN

Outra situação onde bridges TLS são uma boa solução é para aplicações de voz. O banco de dados de encaminhamento da OLT não retém as informações para sempre. Como todas as bridges, se não há atividade na bridge de voz, o endereço MAC do dispositivo de acesso VoIP acabará sendo removido da tabela de encaminhamento da bridge. No sentido upstream está o servidor VoIP que tentará enviar quadros para o dispositivo voip final. Se nenhum endereço MAC está na tabela de encaminhamento, os diferentes tipos de bridges se comportarão de maneiras diferentes. A bridge TLS inundará todas as bridges interfaces pertencentes a VLAN de voz. Bridge de downlink (bridge assimétrica) irão descartas os quadros, não permitindo que a chamada seja completada.

Uma bridge interface TLS é utilizada somente em conjunto com outras bridge interfaces TLS, não podendo ser utilizadas com bridges assimétricas.

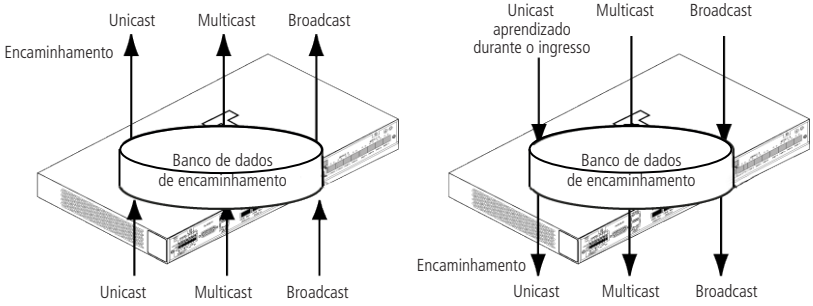
Todas as interfaces em uma bridge TLS são tratadas da mesma maneira conforme exibido na imagem a seguir. Não há designação de um uplink ou um downlink. Ao descrever as interfaces de uma bridge TLS, é útil pensar em termos de entrada ou saída em uma interface.

As bridges TLS aprendem endereços MAC de quadros unicast e encaminham os quadros para destinos aprendidos. Broadcasts e unicasts desconhecidos fluem para todas as interfaces, com exceção da interface de entrada.



Em uma bridge TLS, todas as interfaces aprendem e encaminham da mesma forma

Quadros que entram em uma bridge interface TLS têm seus endereços MAC de origem aprendidos e associados com a interface de modo que os quadros que chegam em outras bridges TLS de mesma VLAN possam ser enviados para a interface correta conforme exibido na imagem a seguir.



Broadcasts e multicasts (exceto IGMP) são inundados para todas as interfaces exceto para a interface que foi recebida.

Endereço MAC de origem são aprendidos durante o ingresso dos quadros.

Quadros Unicast são encaminhados para a interface que possuem o endereço MAC conhecido, ou então são encaminhados para todas as outras interfaces (exceto para a interface de onde recebeu), caso o endereço MAC correspondente não esteja no banco de dados de encaminhamento.

Aprendizado e encaminhamento de quadros em bridges TLS

Configuração da bridge TLS

Para as bridges TLS é indiferente se a interface está voltada para o core da rede ou para o assinante (conforme ocorre com as bridges assimétricas) é necessário apenas que o bridge-path esteja associado com um VLAN ID.

Os parâmetros configuráveis de um bridge-path que são relevantes para as bridges TLS é o aging time, que por padrão é *3600* e o controle de flap que por padrão é definido como default. O controle de flap pode ser configurado como Default, Disabled ou Fast.

O controle de flap fast indica que se um endereço MAC que entra no sistema a partir de uma origem e em seguida é visto a partir de outra origem, a entrada do endereço MAC obtido através da primeira origem é excluída da tabela de encaminhamento e substituída pela segunda origem, sem atraso ou restrição. Se este comportamento não for desejado, o Flap Mode pode ser configurado como disabled ou default.

O aging time padrão é *3600* segundos, este é o tempo que um endereço MAC é mantido na tabela MAC antes de ser removido. Esse período pode ser configurado em uma bridge TLS.

O MCAST e o IGMP Query Interval não são relevantes para bridges TLS.

Configuração de uma bridge TLS

Configurar a interface ethernet (porta eth 2) em uma bridge TLS com VLAN ID 100:

1. Para cada conexão à bridge TLS, utilizar a palavra chave tls:

```
iSH> bridge add 1-1-2-0/eth tls vlan 100 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth/bridge Bridge-path added successfully
```

Bridges TLS podem ser consideradas como uma comunidade, uma vez que compartilha o tráfego como ocorre com o tráfego em uma LAN física.

2. Para criar um perfil de tráfego GPON;

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------->     {0}: 512
traffic-class: ----------------->     {ubr}:
compensated: ------------------->     {false}:
shared: ------------------------>     {false}:
dba-enabled: ------------------->     {false}:
dba-fixed-us-ubr-bw: ------------>     {0}:
dba-fixed-us-cbr-bw: ------------>     {0}:
dba-assured-us-bw: ------------->     {0}:
dba-max-us-bw: ----------------->     {0}:
dba-extra-us-bw-type: ---------->     {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Especifique o ID do GTP (GPON Traffic Profile) ao criar uma GEM Port com o comando *bridge add*. Para bridges TLS utilize a palavra chave *tls:*

```
iSH> bridge add 1-1-4-5/gpononu gem 501 gtp 1 tls vlan 100 tagged
Adding bridge on 1-1-4-5/gpononu
Created bridge-interface-record 1-1-4-501-gponport-100/bridge
Bridge-path added successfully
```

As interfaces configuradas na bridge TLS com VLAN 100 funcionarão como se estivessem na mesma LAN.

4. Verifique as bridges;

```
iSH> bridge show
       Orig
Type   VLAN/SLAN    VLAN/SLAN   Physical          Bridge                          St Table Data
tls    Tagged       100         1/1/2/0/eth       1-1-2-0-eth-100/bridge          DWN
tls    Tagged       100         1/1/4/5/gpononu   1-1-4-501-gponport-100/bridge   DWN
2 Bridge Interfaces displayed
```

5. Verifique o bridge-path.

```
iSH> bridge-path show
VLAN/SLAN Bridge                                  Address
100 N/A                                           VLAN, Age: 3600, MCAST Age: 250, IGMP Query
Interval: 0, IGMP DSCP: 0, Flap Mode: Fast
```

Observação: quando você não especifica *untagged, tagged ou stagged* à bridge interface utilizará a opção padrão. A opção padrão para bridges TLS é untagged

Bridges assimétricas

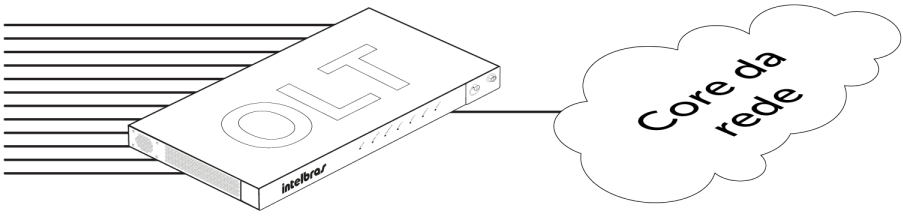
Bridges assimétricas são feitas de um uplink e no mínimo um downlink ou intralink.

Uma única bridge assimétrica pode usar todos os três tipos de bridge interface assimétrica (uplink, downlink e intralink). Entretanto, uma bridge assimétrica poder ter apenas uma única bridge interface uplink. A OLT 8820 G pode ter diversos intralinks e downlinks por bridge.

Normalmente há um uplink e diversos downlinks como teria em um concentrador de linha que divide um link upstream de alta capacidade em diversos links downstream de menor capacidade.

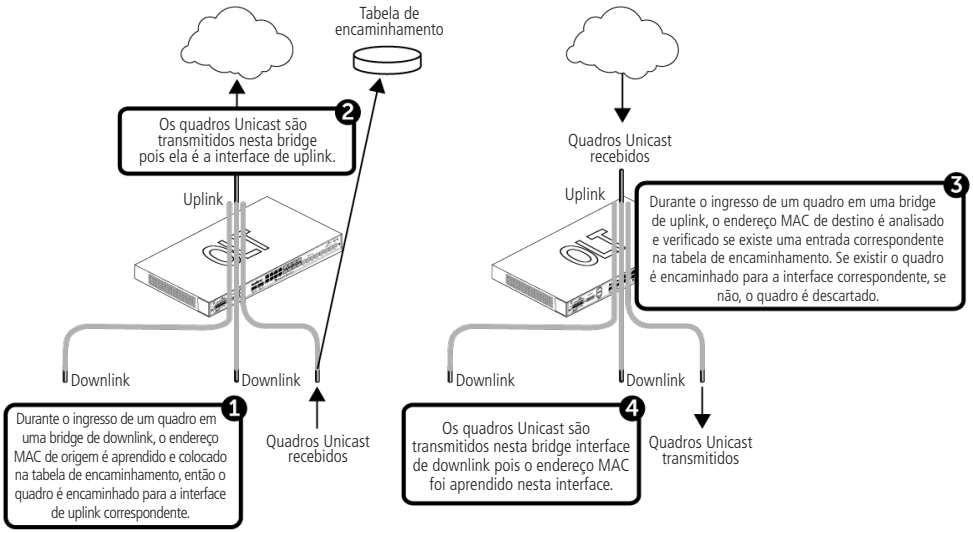
Bridge interfaces intralink são utilizadas para conexões entre OLTs e possui comportamento de aprendizado diferente comparado as bridges uplinks ou downlinks.

Ao configurar o acesso à Internet para diversos assinantes, você deve configurar a OLT 8820 G como um concentrador de linha. Com o modelo de concentrador de linha, você pode criar uma bridge assimétrica com um link upstream de alta capacidade configurado como sendo o uplink e pode ter diversos downlinks configurados para os assinantes (clientes finais).



Modelo do concentrador de linha

Quando um quadro é recebido em uma bridge interface downlink, o endereço MAC de origem é aprendido e inserido na tabela de encaminhamento juntamente com a bridge interface e a VLAN em que o quadro foi recebido. Todos os quadros recebidos em downlinks, independentemente de serem unicast, multicast ou broadcast, são encaminhados ao uplink conforme exibido na imagem a seguir.



Encaminhamento unicast e comportamento de aprendizado para uplinks e downlinks

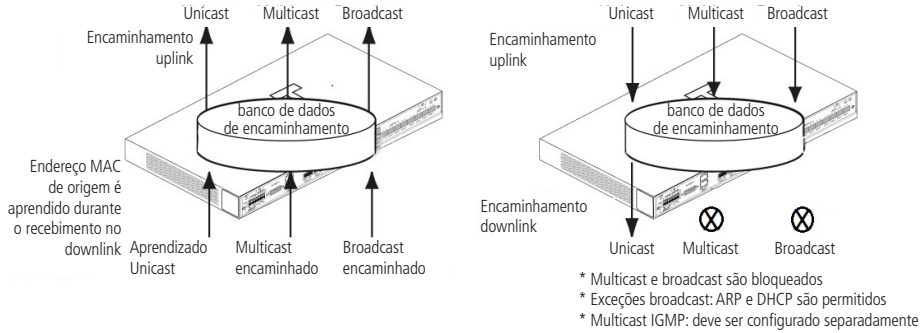
Quando quadros entram em um uplink, o comportamento de uma bridge assimétrica é mais complexo.

Quando um quadro unicast (um quadro que deve ir para um endereço) é recebido na bridge interface uplink e o endereço MAC de destino corresponde a um endereço MAC aprendido, o quadro é encaminhado para a interface de destino correspondente. Quadros unicast desconhecidos recebidos no uplink são descartados. (Exceto no caso de haver um intralink, unicasts desconhecidos são enviados no intralink).

Quadros broadcast têm um código especial na parte do endereço MAC que o identifica como um quadro broadcast. Esses quadros normalmente são duplicados e enviados a todos os dispositivos.

Multicast é usado quando os mesmos dados são exigidos por um grupo de clientes ao mesmo tempo. Diferentemente de broadcast, que envia para todos os dispositivos, multicast oferece conteúdo a um número limitado de dispositivos simultaneamente. Um uso comum de multicats seria para serviços de vídeo. Receber, duplicar e transmitir quadros para vídeo de alta qualidade a um grande número de dispositivos é uma atividade intensiva em termos de tempo de processamento e capacidade. Em multicast, o número de receptores é orientado pelos clientes multicast solicitando o recebimento do tráfego multicast.

Em uma bridge assimétrica, a regra geral é a de que o endereço MAC de origem dos quadros recebidos nos downlinks seja aprendido e encaminhado para o uplink. Quadros unicast recebidos no uplink são encaminhados para o downlink se o endereço MAC de destino corresponder com alguma entrada existente na tabela de encaminhamento. Esta tabela de encaminhamento é populada com os endereços MAC de origem dos quadros recebidos na bridge de downlink. Caso não houver nenhuma correspondência entre o endereço MAC de destino com o endereço MAC de origem contido na tabela de encaminhamento o quadro será descartado. Multicasts e broadcasts recebidos no uplink não são encaminhados com as exceções do DHCP (Dynamic Host Configuration Protocol) e ARP (Address Resolution Protocol) observadas na seção a seguir.



Encaminhamento unicast e comportamento de aprendizado para uma bridge assimétrica

Custom ARP

Quadros de broadcast recebidos na bridge interface de uplink são bloqueados. ARP e DHCP são quadros de broadcast que usam o código de broadcast especial na parte do endereço do quadro de Ethernet, mas que são considerados como exceções.

O ARP busca um endereço IP em um banco de dados que mantém endereços IPs aprendidos. Assim, o ARP é uma mistura de camada 2 (Logical Link com endereços MAC) e camada 3 (Network IP com endereços de IP). Se o quadro for uma mensagem ARP, a OLT compara e filtra o endereço IP solicitado com a tabela de encaminhamento atual.

A configuração customARP pode ser encontrada no profile *bridge-interface-record* que é criado a partir do comando *bridge add*. O comando *update bridge-interface-record* pode ser usado para modificar a configuração customARP.

O modo como os quadros ARP são tratados depende do parâmetro *customARP* no profile *bridge-interface-record*, que normalmente é definido como padrão e não precisa ser alterado.

- » Quando o parâmetro *customARP* é definido em *false*, o pacote ARP é enviado da bridge interface independentemente de uma correspondência ser encontrada para o endereço IP solicitado.
- » Quando o parâmetro *customARP* é definido em *true* e há uma correspondência, o broadcast ARP é encaminhado para a interface que possui o host apropriado. A seguir, o host responderá ao ARP com uma resposta padrão.
- » Quando o parâmetro *customARP* é definido em *true* e não há uma correspondência, o ARP é filtrado e a OLT inunda em broadcast todas as outras bridges interfaces.

Por padrão, o *customARP* é definido em *true* para uplinks e em *false* para downlinks e intralinks.

O parâmetro *customARP* também é definido em *false* para bridges interfaces TLS. Para bridges TLS os pacotes de broadcast são transmitidos. Não há filtragem de broadcast.

Configurar uma bridge uplink

Para uma bridge de uplink, você deve especificar um uplink para enviar quadros recebidos nos downlinks.

Você também deve designar um VLAN ID para corresponder a qualquer VLAN ID configurado nos downlinks.

Configurar uma bridge uplink

1. Adicione uma bridge interface à interface de uplink;

```
iSH> bridge add 1-1-3-0/eth uplink vlan 500 tagged
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-500/bridge
Bridge-path added successfully
```

2. Para criar um perfil de tráfego GPON (GTP);

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------>       {0}: 512000
traffic-class: ---------------->       {ubr}:
compensated: ----------------->       {false}:
```

```
shared: ---------------------->       {false}:
dba-enabled: ------------------>      {false}:
dba-fixed-us-ubr-bw: ---------->      {0}:
dba-fixed-us-cbr-bw: ---------->      {0}:
dba-assured-us-bw: ------------>      {0}:
dba-max-us-bw: ---------------->      {0}:
dba-extra-us-bw-type: -------->       {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Adicione a bridge interface de downlink;

```
iSH> bridge add 1-1-1-3/gpononu gem 501 gtp 1 downlink vlan 500 tagged
Adding bridge on 1-1-1-3/gpononu
Created bridge-interface-record 1-1-3-501-gponport/bridge
```

4. Verifique as bridges.

```
iSH> bridge show
      Orig
Type  VLAN/SLAN  VLAN/SLAN Physical          Bridge                          St Table Data
dwn   Tagged     500       1/1/1/3/gpononu   1-1-1-501-gponport-500/bridge   DWN
upl   Tagged     500       1/1/3/0/eth       1-1-3-0-eth-500/bridge          DWN S VLAN 500 default
2 Bridge Interfaces displayed
```

Bridge add e bridge-path padrões

A OLT cria automaticamente um bridge-path com valores padrão ao inserir o comando *bridge add* na criação de bridges uplink, TLS e intralink.

Bridge-path padrão para bridges uplink:

```
iSH> bridge-path show
VLAN/SLAN   Bridge                      Address
      500 1-1-3-0-eth-500/bridge      Default, Age: 3600, MCAST Age: 250,
IGMP Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

Bridge-path padrão para bridges intralink:

```
iSH> bridge-path show
VLAN/SLAN   Bridge                          Address
          444 1-1-4-0-eth-444/bridge      Intralink
```

Bridge-path padrão para bridges bridges TLS:

```
iSH> bridge-path show
VLAN/SLAN   Bridge               Address
          100 N/A                VLAN, Age: 3600, MCAST Age: 250, IGMP Query
Interval: 0, IGMP DSCP: 0, Flap Mode: Fast
```

Há argumentos opcionais para a bridge que deve ser configurada através da CLI utilizando o comando *bridge-path* modify. Estes argumentos são:

- age (unicast).
- multicast aging period (mcast).
- IGMP query interval (igmpsnooping).
- flap control (flap).
- IGMP timer.
- flags.

Quando o comando *bridge-path modify* é usado em uma bridge existente, o bridge-path previamente existente é sobrescrito e, exceto especificado de outro modo, todos os valores de parâmetros opcionais previamente existentes serão revertidos para o padrão.

Em outras palavras, se o bridge-path existente inclui uma designação para controle de flap e você deseja adicionar o temporizador IGMP, você deve inserir o valor de controle de flap e o valor do temporizador IGMP. Caso contrário, o valor de controle de flap será revertido para o padrão.

Por exemplo, para definir parâmetros como *mcast* e i*gmp* para bridging de vídeo, insira o comando *bridge-path modify* com os valores adequados.

O exemplo a seguir exibe uma bridge adicionada e o bridge-path automaticamente criado.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 999 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-999/bridge
Bridge-path added successfully

iSH> bridge show
      Orig
Type  VLAN/SLAN  VLAN/SLAN       Physical     Bridge                    St Table Data
upl               Tagged 999     1/1/2/0/eth  1-1-2-0-eth-999/bridge    DWN S VLAN 999 default
1 Bridge Interfaces displayed

iSH> bridge-path show
VLAN/SLAN     Bridge                          Address
         999 1-1-2-0-eth-999/bridge          Default, Age: 3600, MCAST Age: 250, IGMP Query
Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

O exemplo a seguir exibe o comando *bridge-path modify* usado para modificar os parâmetros de bridge-path padrão ou adicionar funcionalidade de IGMP. Neste caso, o IGMP snooping é habilitado e o multicast aging period e IGMP query são definidos.

```
iSH> bridge-path modify 1-1-2-0-eth-999/bridge vlan 999 default igmpsnooping enable mcast 120
igmptimer 60
Bridge-path 1-1-2-0-eth-999/bridge/3/999/0/0/0/0/0/0/0 has been modified

iSH> bridge-path show
VLAN/SLAN     Bridge                Address
      999 1-1-2-0-eth-999/bridge    Default, Age: 3600, MCAST Age: 120,
IGMP Query Interval: 60, IGMP Proxy, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

Bridge intralink

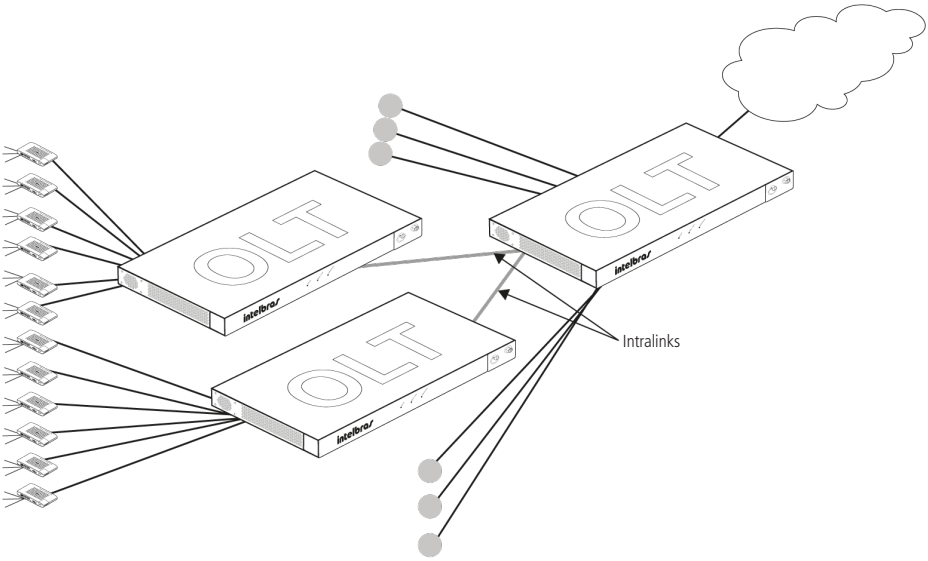
Bridges intralinks são utilizadas basicamente para a interconexão de OLTs. A bridge intralink envia todos os quadros que não podem ser encaminhados a um destino.

Um caso comum para uma bridge assimétrica consiste no aprendizado dos quadros recebidos pela bridge interface de downlink e o encaminhamento dos quadros pela bridge interface de uplink proveniente de uma outra OLT. Se um quadro é recebido em um downlink, o endereço MAC é aprendido. Quando o quadro é recebido em um uplink e o endereço MAC é conhecido, o quadro é encaminhado para a devida bridge interface de downlink. Quando o endereço MAC não é conhecido ele é descartado.

No caso de ter diversas OLTs interconectadas, é possível que a tabela de encaminhamento da OLT principal ou nas OLTs mais próximas do core da rede cresçam de uma forma incontrolável, pois estariam aprendendo os endereços MAC de todos os dispositivos downstream.

Bridge interfaces intralink, em vez de aprender os endereços conectados à interface intralink como acontece nas bridge interfaces de downlink, elas enviam todos os quadros da interface intralink para o uplink sem a realização de aprendizado. O comportamento recíproco consiste em quadros com endereços desconhecidos recebidos na interface de uplink sendo enviados para a bridge interface intralink.

A imagem a seguir exibe as bridges de downlinks para as ONTs e bridges intralinks na interconexão das OLTs. A bridge intralink oferece os meios para o encaminhamento de todos os quadros desconhecidos recebidos no uplink (core da rede) para o intralink. O dispositivo principal não precisa aprender os quadros recebidos na bridge intralink.



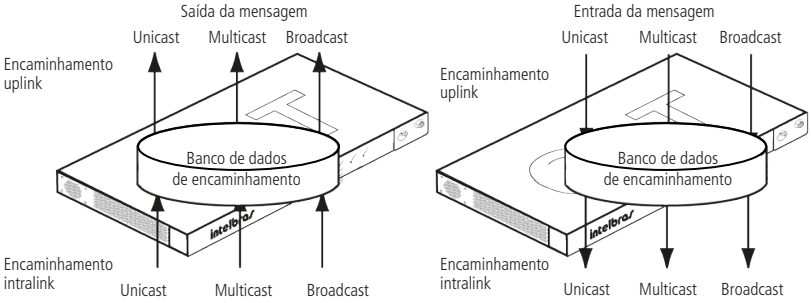
Modelo com bridges intralinks

Uma bridge interface intralink é usada em conjunto com uma bridge interface uplink, onde a bridge de uplink é o caminho upstream da rede. A bridge interface intralink encaminha o trágefo multicast ou tráfego de quadros com endereços MAC desconhecidos ao uplink sem realizar o aprendizado dos endereços dos dispositivos ou da rede. O tráfego que chega em uma interface intralink é encaminhado para a interface uplink, independentemente do endereço MAC de destino.

Broadcasts, multicasts e unicasts (conhecidos e desconhecidos) serão enviados à interface padrão, que é a bridge uplink da VLAN.

Em outras palavras, endereços de origem a partir de uma interface intralink não são aprendidas, de modo que o banco de dados de endereços aprendidos não será incrementado com o endereço. Do mesmo modo, quando um quadro unicast desconhecido é recebido na interface uplink, ele será transmitido para a interface intralink. Em algum lugar abaixo da cadeia, o endereço pode ser conhecido. Intralinks normalmente são usados em conjunto com uplinks e podem ser usados com downlinks.

Como na interface uplink, a interface intralink exige configuração adicional de um bridge-path. O bridge-path define um caminho padrão para a VLAN específica na bridge intralink. Se um intralink está fantando no bridge-path, o tráfego não fluirá pela VLAN assimétrica.



Encaminhamento em uma bridge intralink

A regra geral para intralinks é que os quadros que entram no intralink são encaminhados sem que o endereço MAC de origem seja aprendido. Todos os quadros com endereços desconhecidos são encaminhados.

Configuração da bridge intralink na OLT 8820 G

Este exemplo adiciona uma bridge interface intralink a uma bridge assimétrica uplink/downlink.

1. Adicione a bridge interface uplink. Para cada VLAN ID designado em um downlink, deve haver um uplink com o VLAN ID correspondente;

```
iSH> bridge add 1-1-4-0/eth uplink vlan 100 tagged
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth-100/bridge
Bridge-path added successfully
iSH> bridge add 1-1-4-0/eth uplink vlan 200 tagged
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth-200/bridge
Bridge-path added successfully
```

O bridge-path criado automaticamente designa a bridge como padrão. O padrão designa que todos os quadros unicast desconhecidos serão enviados ao intralink em vez de serem descartados como em uma bridge assimétrica sem uma bridge intralink.

```
iSH> bridge-path show
VLAN/SLAN     Bridge               Address
------------------------------------------------------------------
       100 1-1-4-0-eth-100/bridge  Default, Age: 3600, MCAST Age: 250, IGMP
Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
       200 1-1-4-0-eth-200/bridge  Default, Age: 3600, MCAST Age: 250, IGMP
Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

> **Observação:** a OLT 8820 G não suporta a palavra chave global. Para cada VLAN ou SLAN, a bridge de uplink deve ser definida como padrão

2. Para criar um perfil de tráfego GPON (GPT);

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------>       {0}: 512000
traffic-class: ---------------->       {ubr}:
compensated: ------------------>       {false}:
shared: ----------------------->       {false}:
dba-enabled: ------------------>       {false}:
dba-fixed-us-ubr-bw: ---------->       {0}:
dba-fixed-us-cbr-bw: ---------->       {0}:
dba-assured-us-bw: ------------>       {0}:
dba-max-us-bw: ---------------->       {0}:
dba-extra-us-bw-type: -------->       {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Adicione as bridges de downlink das ONTs;

```
iSH> bridge add 1-1-1-4/gpononu gem 501 gtp 1 downlink vlan 100 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-501-gponport-100/bridge
iSH> bridge add 1-1-1-3/gpononu gem 501 gtp 1 downlink vlan 200 tagged
Adding bridge on 1-1-1-3/gpononu
Created bridge-interface-record 1-1-3-501-gponport-200/bridge
```

4. Crie uma bridge interface intralink com um VLAN ID;

```
iSH> bridge add 1-1-2-0/eth intralink vlan 444 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-444/bridge
Bridge-path added successfully
```

```
iSH> bridge-path show
VLAN/SLAN     Bridge                          Address
      100 1-1-4-0-eth-100/bridge              Default, Age: 3600, MCAST Age: 250, IGMP
Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
      200 1-1-4-0-eth-200/bridge              Default, Age: 3600, MCAST Age: 250, IGMP Query
Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
      444 1-1-2-0-eth-444/bridge              Intralink
```

Esse comando define principalmente o comportamento de que os endereços de origem a partir do intralink não serão aprendidos.

> **Observação:** a OLT 8820 G não suporta a palavra chave *global-intralink*. Para cada VLAN ou SLAN, você deve definir o bridge-path como um intralink usando a palavra chave *intralink*

Esse comando define o comportamento de que qualquer quadro com endereços desconhecidos serão enviados para o intralink com VLAN ID 444.

5. Crie a bridge de uplink para o intralink com o mesmo VLAN ID para o tráfego poder ser passado para a rede;

```
iSH> bridge add 1-1-3-0/eth uplink vlan 444 tagged
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-444/bridge
Bridge-path added successfully
```

6. Verifique as bridges criadas;

```
iSH> bridge show
      Orig
Type  VLAN/SLAN VLAN/SLAN   Physical          Bridge                          St Table Data
dwn             Tagged 100  1/1/1/4/gpononu   1-1-1-501-gponport-100/bridge   DWN
dwn             Tagged 200  1/1/1/4/gpononu   1-1-1-501-gponport-200/bridge   DWN
int             Tagged 444  1/1/2/0/eth       1-1-2-0-eth-444/bridge          DWN S VLAN 444 Intralink
upl             Tagged 444  1/1/3/0/eth       1-1-3-0-eth-444/bridge          DWN S VLAN 444 default
upl             Tagged 100  1/1/4/0/eth       1-1-4-0-eth-100/bridge          DWN S VLAN 100 default
upl             Tagged 200  1/1/4/0/eth       1-1-4-0-eth-200/bridge          DWN S VLAN 200 default
```

7. Verifique os bridge-path.

```
iSH> bridge-path show
VLAN/SLAN     Bridge                          Address
      100 1-1-4-0-eth-100/bridge              Default, Age: 3600, MCAST Age: 250, IGMP
Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
      200 1-1-4-0-eth-200/bridge              Default, Age: 3600, MCAST Age: 250, IGMP
Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
      444 1-1-2-0-eth-444/bridge              Intralink
      444 1-1-3-0-eth-444/bridge              Default, Age: 3600, MCAST Age: 250, IGMP
Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

9.4. Operações de marcação (untagged, tagged e stagged)

Visão geral

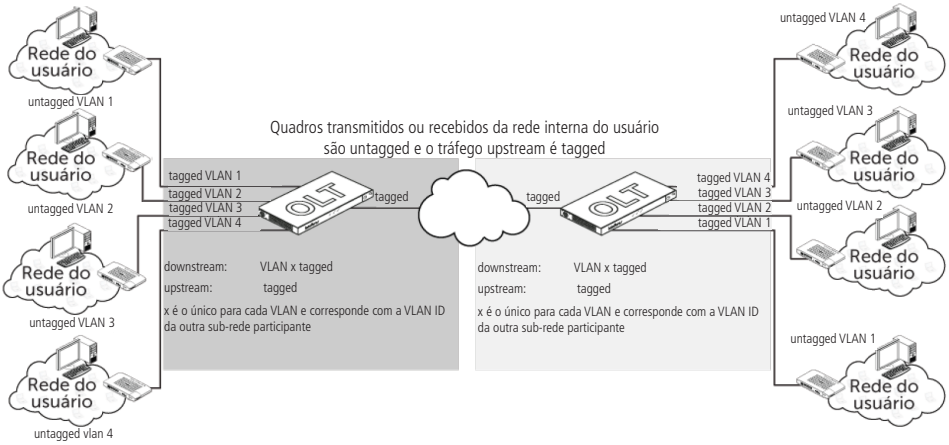
VLANs e SLANs definem a qual bridge um quadro recebido pertence. O tipo de bridge determina o comportamento de encaminhamento da bridge. Em conjunto com as características de encaminhamento e aprendizado dos tipos de bridge, você também pode configurar operações de marcação (untagged, tagged e stagged).

Operações de marcação oferecem a possibilidade de configurar filtros de entrada para as interfaces, promoção de VLAN/SLAN, saída e remoção de tags de VLAN.

Normalmente, essas operações, filtro de entrada, promoção, saída e remoção, são configuradas em interfaces de downstream. Definir se uma bridge interface deve ser untagged, tagged ou stagged depende do que os dispositivos conectados à interface estão esperando.

A OLT usa um mecanismo extremamente flexível para configurar operações de marcação. Antes de discutir as diversas combinações possíveis, é importante entender casos comuns:

VLAN tagging para redes de PC.



Tags de VLAN podem ser usadas para organizar sub-redes

Você pode adicionar uma tag VLAN a todos os quadros oriundos de uma rede de PC que enviam seus quadros sem marcação (untagged). Entretanto, se você deseja que sua rede de PC faça parte de uma LAN virtual com outra rede de PC remota, portanto você configura a bridge interface de downstream para aceitar quadros não marcados (untagged) e posteriormente adicionar uma tag. A Intelbras utiliza o termo *promotion* para representar a adição de tag. Os quadros são marcados na interface elétrica da ONU/ONT e enviados à bridge interface downstream que sempre é tagged e posteriormente direcionados para bridge uplink e a rede de PC remota.

Assim, ao receber um quadro da rede de PC remota (que possui a mesma tag de VLAN), o quadro é recebido no uplink e encaminhado ao link de downstream adequado, pois o VLAN ID é correspondente (presumindo que o endereço MAC de destino do quadro unicast seja correspondente a um endereço MAC aprendido). Entretanto, a rede de PC não aceita tags, portanto a tag de VLAN é removida na interface elétrica da ONT/ONU e o quadro é encaminhado ao dispositivo com o endereço MAC adequado. A Intelbras usa o termo *stripping* para a remoção de VLAN/SLAN IDs.

No exemplo anterior, as interfaces upstream e downstream recebem da ONU/ONT os quadros com o VLAN ID que identifica qual a rede de PC, ou seja, o stripp e promotion são feitos na interface elétrica das ONUs/ONTs.

> **Observação:** este exemplo não descreve se as bridges são bridges assimétricas ou bridges simétricas

As quatro operações de VLAN trabalham juntas ou estão implícitas no comando bridge add/modify.

» **Ingress Filtering (Filtro de entrada):** é a capacidade da bridge interface apenas aceitar quadros ethernet com determinadas TAGs de VLAN ou SLAN.

» **VLAN/SLAN Promotion (Promoção de VLAN/SLAN):** é a capacidade de adicionar TAGs de VLAN em quadros ethernet.

» **Egress (saída):** designa para onde encaminhar o quadro ethernet. O encaminhamento é baseado em VLAN, SLAN ou tags de VLAN/SLAN. Quando o quadro ethernet é recebido pela OLT, possivelmente será adicionado uma TAG (VLAN Promotion) para então encontrar a bridge interface de saída.

» **Stripping (Remoção):** é o inverso de VLAN Promotion, é a remoção da VLAN/SLAN ou tag de VLAN/SLAN do quadro ethernet.

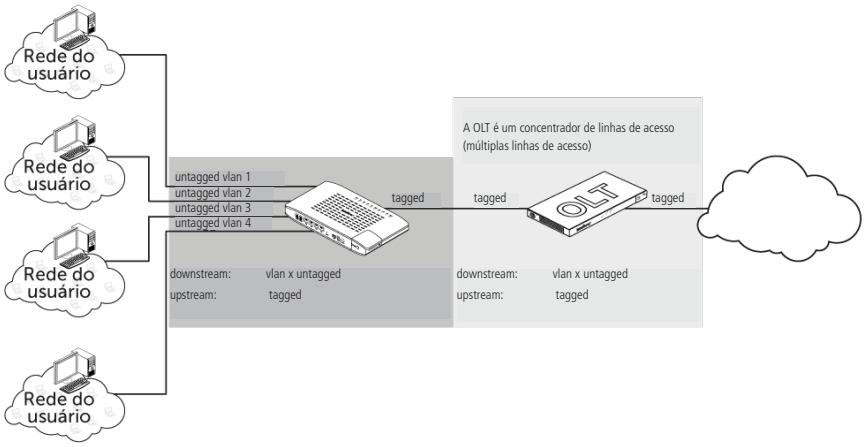
Promotion e Stripping sempre ocorrem juntos. Ingrees Filtering presume que o quadro ethernet de entrada já possui pelo menos 1 tag, você poderá filtrar por VLAN ou promover uma SLAN. O recebimento de um quadro encaminhado internamente e direcionado para a saída, presume que o quadro foi recebido com tag ou que foi promovido para possuir uma tag.

Observação: a OLT 8820 G não suporta stagged (dupla marcação/QinQ) com VLAN ID conhecido e SLAN ID desconhecido

Os quadros que entram na OLT 8820 G são não marcados (untagged), marcados (tagged) ou dupla marcação/QinQ (stagged).

Cenários com operações de tagging

Na imagem a seguir, a OLT 8820 G é o nível superior das ONTs e age como um concentrador de linha. O exemplo exibe apenas as operações de tagging de VLAN.

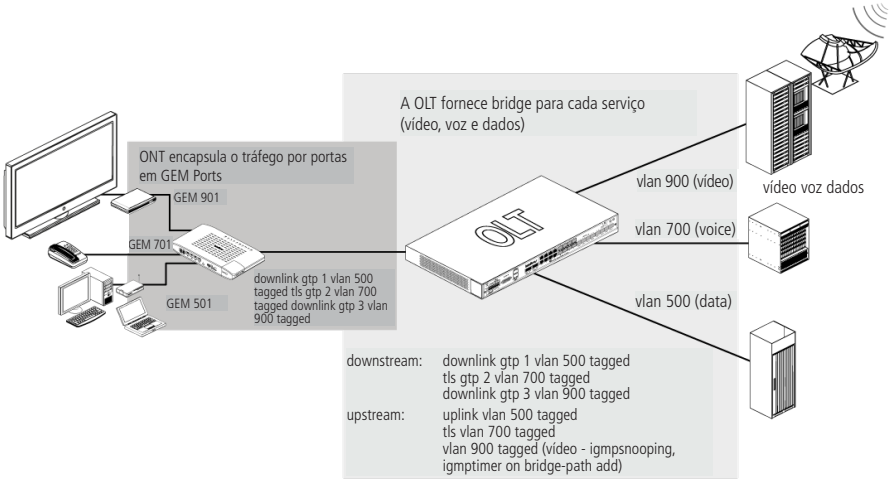


ONT fornecendo marcação e a OLT agindo como concentrador de linha

A imagem anterior exibe a promoção de quadros untagged na interface de downstream (e assim, atuando como filtro para a interface quando o quadro com esse VLAN ID é recebido na interface upstream - considerando que os outros fundamentos de bridge são atendidos, como a correspondência do endereço MAC e do VLAN ID na tabela de encaminhamento se for um downlink).

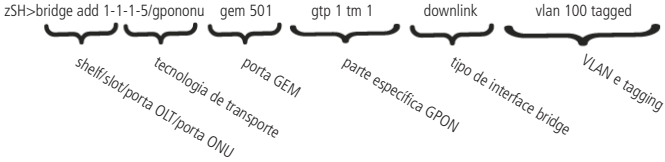
O quadro untagged é aceito na interface de downstream e a seguir é promovido, inserindo um VLAN ID. O upstream é tagged, de modo que o quadro marcado é enviado através da interface de upstream.

Os uplinks podem ser separados por VLAN, que é um caso comum, conforme exibido na imagem a seguir. Normalmente um cenário Triple Play, você teria VLANs separando os serviços de vídeo, voz ou dados. Assim, você pode manter o tráfego conhecido separado para definir a priorização de QoS ou outras adições de bridge como previsto por regras de pacote ou por GTPs (GPON Traffic Profiles).



Encapsulamento de GEM Port para separar VLANs privadas

Uma boa maneira de aprender fundamentos de marcação de pacotes é explorando alguns dos casos comuns. Conforme nas imagens anteriores, é exibido a promoção (e a retirada) de tags de VLAN tanto na ONT quanto na OLT. Essas múltiplas interfaces dos assinantes podem ser configuradas para diferentes serviços, como dados, voz e vídeo, mas todos em tecnologias de transporte GPON (vide a imagem anterior).



Partes do comando bridge add

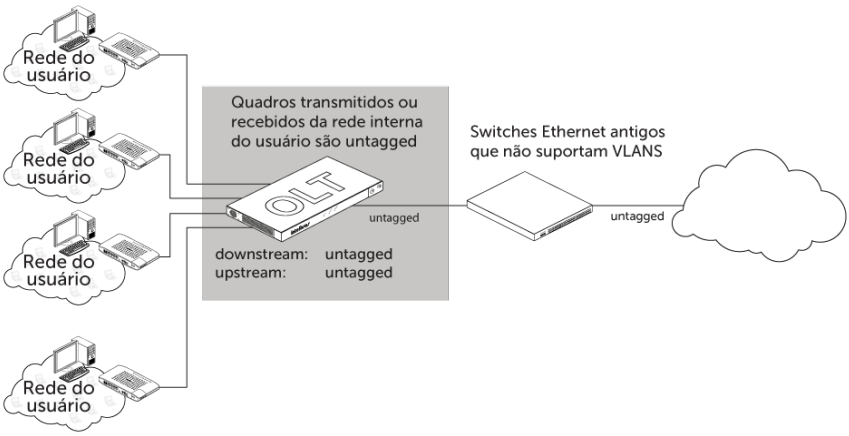
A criação da GEM Port é um bom exemplo para exibir as partes do comando *bridge add*. Partes do comando definem as características de bridging discutidas neste capítulo. O comando também inclui a tecnologia de transporte e qualquer informação associada.

O quadro untagged é recebido na interface de downstream. Lendo da esquerda para a direita, o quadro é promovido para ter um VLAN ID, dependendo da interface onde foi recebido. A interface upstream é tagged, portanto um quadro com VLAN ID (sem tag dupla) é encaminhado para a interface. Uma vez que a bridge interface é marcada (tagged), não há remoção (stripping) da tag de VLAN.

Um quadro na interface de upstream faz o caminho inverso. Um quadro marcado (tagged) é aceito na interface de upstream. Como nenhuma VLAN é definida, a interface aceita todos os quadros tagged (não aceita quadros com tag dupla), portanto qualquer VLAN ID. Desta forma não há promoção, o quadro é encaminhado à bridge interface com o VLAN ID correspondente ao VLAN ID contido no quadro ethernet. A saída do quadro na interface é untagged, portanto o VLAN ID é retirado (stripped) e o quadro é enviado à rede.

Neste caso, diversas interfaces com o mesmo VLAN não estão sendo discutidas, embora este seja um caso comum. Para existir uma discussão sobre isso, endereços MAC são encontrados na tabela de encaminhamento para a interface de saída.

A flexibilidade do mecanismo de marcação funciona para muitos casos. A OLT não somente suporta muitas tecnologias de transporte, como também suporta qualquer nível de tag, tanto na interface de downstream como na interface de upstream.



A OLT suporta a operação untagged na interface de upstream

Para separar informações untagged onde existe outro tráfego como teria com a VLAN 0 (quadros untagged que não pertencem a uma VLAN), você pode inserir uma tag na entrada e remover esta tag na saída da interface.

9.5. Comandos comuns de bridge

Comando bridge add

O comando *bridge add* combina tipos fundamentais de bridging, a interface física com suas especificações de meios de transporte, operações de marcação e outras adições à regra de bridge, como regras de pacote.

Verificação das configurações da bridge interface

Bridge interfaces geralmente são criadas com o comando *bridge add*. Visualize o perfil *bridge-interface-record* para investigação de problemas ou quando os padrões do perfil *bridge-interface-record* não apresentam o comportamento de bridging desejado.

Para visualizar as configurações da bridge interface, insira o comando *get bridge-interface-record interface/type.*

```
iSH> get bridge-interface-record 1-1-1-5-gponport-840/bridge
bridge-interface-record     1-1-1-509-gponport-840/bridge
vpi: ------------------------------------------>     {0}
vci: ------------------------------------------>     {0}
vlanId: ---------------------------------------->     {840}
stripAndInsert: -------------------------------->     {false}
customARP: ------------------------------------->     {false}
filterBroadcast: ------------------------------->     {false}
learnIp: --------------------------------------->     {true}
learnUnicast: ---------------------------------->      {true} maxUnicast: ----------------------
--------------->     {5}
learnMulticast: -------------------------------->     {true}
forwardToUnicast: ------------------------------>     {false}
forwardToMulticast: ---------------------------->     {false}
forwardToDefault: ------------------------------>     {true}
bridgeIfCustomDHCP: ---------------------------->     {false}:
bridgeIfIngressPacketRuleGroupIndex: ----------->     {0}
vlanIdCOS: ------------------------------------->     {0}
outgoingCOSOption: ----------------------------->     {disable}
outgoingCOSValue: ------------------------------>     {0}
s-tagTPID: ------------------------------------->     {0x8100}
s-tagId: --------------------------------------->     {0}
```

```
s-tagStripAndInsert: ---------------------------->     {true}
s-tagOutgoingCOSOption: ------------------------->     {s-tagdisable}
s-tagIdCOS: ------------------------------------->     {0}
s-tagOutgoingCOSValue: -------------------------->     {0}
mcastControlList: ------------------------------->     {}
maxVideoStreams: -------------------------------->     {0}
isPPPoA: ---------------------------------------->     {false}
floodUnknown: ----------------------------------->     {false}
floodMulticast: --------------------------------->     {false}
bridgeIfEgressPacketRuleGroupIndex: ------------>     {0}:
bridgeIfTableBasedFilter: ----------------------->     {NONE(0):
bridgeIfDhcpLearn: ------------------------------>     {NONE(0)}:
mvrVlan: ---------------------------------------->     {0}
vlan-xlate-from: -------------------------------->     {0}
slan-xlate-from: -------------------------------->     {0}
```

Um perfil *bridge-interface-record* é um conjunto de parâmetros pré-definidos. A configuração dos diferentes parâmetros define o comportamento da bridge interface. As bridges interface funcionam juntas e a combinação das bridges interfaces é considerada uma bridge.

9.6. Configurações para bridges assimétricas

A tabela a seguir lista o conjunto de parâmetros padrão definidos para as bridges assimétricas.

Parâmetro	Uplink	Downlink untagged	Downlink tagged	Intralink tagged
vlanId	Conforme especificado	Conforme especificado	Conforme especificado	Conforme especificado
stripAndInsert	False	True	False	False
customARP	True	False	False	False
filterBroadcast	True	False	False	False
learnIP	False	True	True	False
learnUnicast	False	True	True	False
maxUnicast	0	5	5	0
learnMulticast	False	True	True	False
forwardToUnicast	True	False	False	False
forwardToMulticast	True	False	False	False
forwardToDefault	False	True	True	True
bridgeIfCustomDHCP	True	False	False	False
bridgeIfIngressPacketRule GroupIndex	0	0	0	0
valndIdCOS	0	0	0	0
outgoingCOSOption	Disable	Disable	Disable	Disable
outgoingCOSValue	0	0	0	0
s-tagTPID	0x8100	0x8100	0x8100	0x8100
s-tagId	0	0	0	0
s-tagStripAndInsert	True	True	True	True
s-tagOutgoingCOSOption	s-tagdisable	s-tagdisable	s-tagdisable	s-tagdisable
s-tagIdCOS	0	0	0	0
s-tagOutgoingCOSValue	0	0	0	0
mcastControlList	As specified	As specified	As specified	As specified
maxVideoStreams	0	0	0	0
isPPPoA	False	False	False	False
floodUnknown	False	False	False	False
floodMulticast	False	False	False	False
bridgeIfEgressPacketRule GroupIndex	0	0	0	0
bridgeIfTableBasedFilter	NONE(0)	NONE(0)	NONE(0)	NONE(0)
bridgeIfDhcpLearn	NONE(0)	NONE(0)	NONE(0)	NONE(0)

Valores dos perfis bridge-interface-record para bridges assimétricas

9.7. Configurações para bridges simétricas

A tabela a seguir lista o conjunto de parâmetros padrão definidos para as bridges simétricas.

Parâmetro	TLS
vlanId	Conforme especificado
stripAndInsert	True
customARP	False
filterBroadcast	False
learnIP	False
learnUnicast	True
maxUnicast	100
learnMulticast	False
forwardToUnicast	True
forwardToMulticast	False
forwardToDefault	False
floodUnknown	True
floodMulticast	True
bridgeIfCustomDHCP	False
bridgeIfConfigGroupIndex	0
valndIdCOS	0
outgoingCOSOption	Disable
outgoingCOSValue	0
s-tagTPID	0x8100
s-tagId	0
s-tagStripAndInsert	False
s-tagOutgoingCOSOption	s-tagdisable
s-tagIdCOS	0
s-tagOutgoingCOSValue	0
mcastControlList	{}
maxVideoStreams	0
isPPPoA	false
floodUnknown	true
floodMulticast	true
bridgeIfEgressPacketRuleGroupIndex	0
bridgeIfTableBasedFilter	NONE(0)
bridgeIfDhcpLearn	NONE(0)

Valores dos perfis bridge-interface-record para bridge TLS

O comando *bridge show* exibe o tipo de bridge.

```
iSH> bridge show
       Orig
Type VLAN/SLAN  VLAN/SLAN    Physical            Bridge                          St Table Data
int             Tagged 444   1/1/2/0/eth         1-1-2-0-eth-444/bridge          UP S VLAN 444 Intralink
tls              300         1/1/5/0/eth         1-1-5-0-eth/bridge              DWN
upl             Tagged 444   1/1/3/0/eth         1-1-3-0-eth-444/bridge          UP S VLAN 444 default
upl             Tagged 100   1/1/4/0/eth         1-1-4-0-eth-100/bridge          DWN S VLAN 100 default
upl             Tagged 200   1/1/4/0/eth         1-1-4-0-eth-200/bridge          DWN S VLAN 200 default
dwn                    100   1/1/4/1/gpononu     1-1-4-501-gponport-100/bridge   DWN
dwn                    200   1/1/3/1/gpononu     1-1-3-601-gponport-200/bridge   DWN
tls                    300   1/1/5/1/gpononu     1-1-5-701-gponport-300/bridge   DWN
```

9.8. Modelagem de tráfego (Traffic Shapping): enfileiramento de Classes de Serviços (CoS)

As filas de classes de serviços (CoS) controlam o tráfego afim de otimizar ou garantir desempenho da rede. Essa definição de tráfego pode ser utilizada para aumentar a largura de banda para um determinado dispositivo, aumenando assim seu desempenho, ou pode ser utilizado para diminuir a latência, para casos onde o o fluxo de dados são sensiveis a esta variável, como por exemplo, tráfego de voz.

O congestionamento pode ocorrer por vários motivos. Se você tem um link (interface) com maior largura de banda alimentando um link (interface) com menor largura de banda ou se você tem diversos links (interfaces) com largura de banda semelhante alimentando um único link (interface). Ambos os casos podem ser considerados como congestionamento de dados (onde o canal de saída não consegue dar vazão ao canal de entrada).

O enfileiramento define o quanto de uma interface física uma VLAN poderá utilizar.

A OLT 8820 G suporta a configurações de valores CoS existente no cabeçalho da tag de VLAN inserido no quadro Ethernet. Este serviço permite que você designe um nível de serviço ou CoS a uma interface VLAN de Ethernet que é transportada para uma bridge tagged de uplink, intralink ou downlink. O nível de CoS configurado especifica a prioridade do pacote e os métodos de enfileiramento usados para transportar o pacote através da rede de Ethernet. A OLT 8820 G determina e preserva as configurações de CoS para garantir que essas configurações sejam repassadas a outros dispositivos Ethernet na rede para processamento de QoS.

Os valores de CoS variam de 0 - 7 com a prioridade inferior sendo 0 e a prioridade máxima sendo 7.

O tráfego é priorizado na OLT com base nos valores de CoS contidos no quadro durante sua entrada na interface. Entretanto, a OLT 8820 G suporta quatro filas por interface física, deste modo, os quadros com valor de CoS 0 ou 1 são colocados na fila número 1; quadros com valor de CoS 2 ou 3 são colocados na fila número 2; quadros com valor de CoS 4 ou 5 são colocados na fila número 3 e quadros com valor de CoS 6 ou 7 na fila número 4.

Estas filas de prioridade utilizam o algoritmo de escalonamento SP (Strict Priority) para a vazão dos dados. Todos os dados contidos na fila de maior prioridade (fila número 4, que possui os valores de CoS 6 e 7) são transmitidos, somente após esta fila ficar vazia é que a próxima fila será atendida (fila número 3, que possui valores de CoS 4 e 5) e assim sucessivamente com as demais filas, atendendo a fila número 2 (CoS 2 e 3) e por último atendendo a fila número 1 (CoS 0 e 1). Com este algoritmo de escalonamento é possível que as filas de menor prioridade fiquem sobrecarregadas enquanto os dados contidos nas filas de maior prioridade sejam transmitidos.

Os quadros que exigem maior rendimento ou que são sensíveis à latência devem estar nas filas de prioridade mais alta. Como o enfileiramento é relativo ao tipo de tráfego, as configurações de prioridade dependem do tipo de tráfego. Normalmente vídeo e voz são mais sensíveis a rendimento e latência.

Configuração de Classes de Serviço (CoS)

A tabela a seguir descreve o parâmetro contido no perfil *bridge-interface-record* utilizado para suporte a CoS.

Parâmetro	Descrição
vlanIdCOS	Especifica o valor carregado no campo CoS do cabeçalho de VLAN de um pacote untagged quando recebido por uma interface configurada como tagged (inserção do VLAN ID). Os valores de CoS variam de 0 a 7, por padrão o valor é *0*.

Parâmetros de COS no perfil bridge-interface-record

Para exibir o perfil bridge-interface- record, insira o comando show bridge-interface-record.

```
iSH> show bridge-interface-record
vpi:---------------------------------------->  {0 - 4095}
vci:---------------------------------------->  {0 - 65535}
vlanId:------------------------------------->  {0 - 4094}
stripAndInsert:----------------------------->  false    true
customARP:---------------------------------->  false    true
filterBroadcast:---------------------------->  false    true
learnIp:------------------------------------>  false    true
learnUnicast:------------------------------->  false    true
maxUnicast:--------------------------------->  {0 - 2147483647}
learnMulticast:----------------------------->  false    true
forwardToUnicast:--------------------------->  false    true
forwardToMulticast:------------------------->  false    true
forwardToDefault:--------------------------->  false    true
bridgeIfCustomDHCP:------------------------->  false    true
bridgeIfIngressPacketRuleGroupIndex:-------->  {0 - 2147483647}
vlanIdCOS:---------------------------------->  {0 - 7}
outgoingCOSOption:-------------------------->  disable  all
outgoingCOSValue:--------------------------->  {0 - 7}
```

Adição de uma bridge com valor de CoS

Neste exemplo será adicionada a GEM Port 601 na interface GPON ONU 1-1-1-4 com o valor de vlanIDCOS 7. Este valor é inserido no campo de prioridade do cabeçalho VLAN quando um pacote untagged (não marcado) é recebido pela interface que está configurada como tagged (inserção do VLAN ID). Certifique-se de que o GTP exista antes de especificar seu índice no comando *bridge add*.

```
iSH> bridge add 1-1-1-4/gpononu gem 601 gtp 1 downlink vlan 100 tagged COS 7
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-601-gpononu-100/bridge
```

Neste exemplo será adicionada a GEM Port 601 na interface GPON ONU 1-1-1-5 com o valor de vlanIDCOS 7 e habilita sobrescrever o VLAN ID em todos os pacotes de saída com o valor de CoS 7.

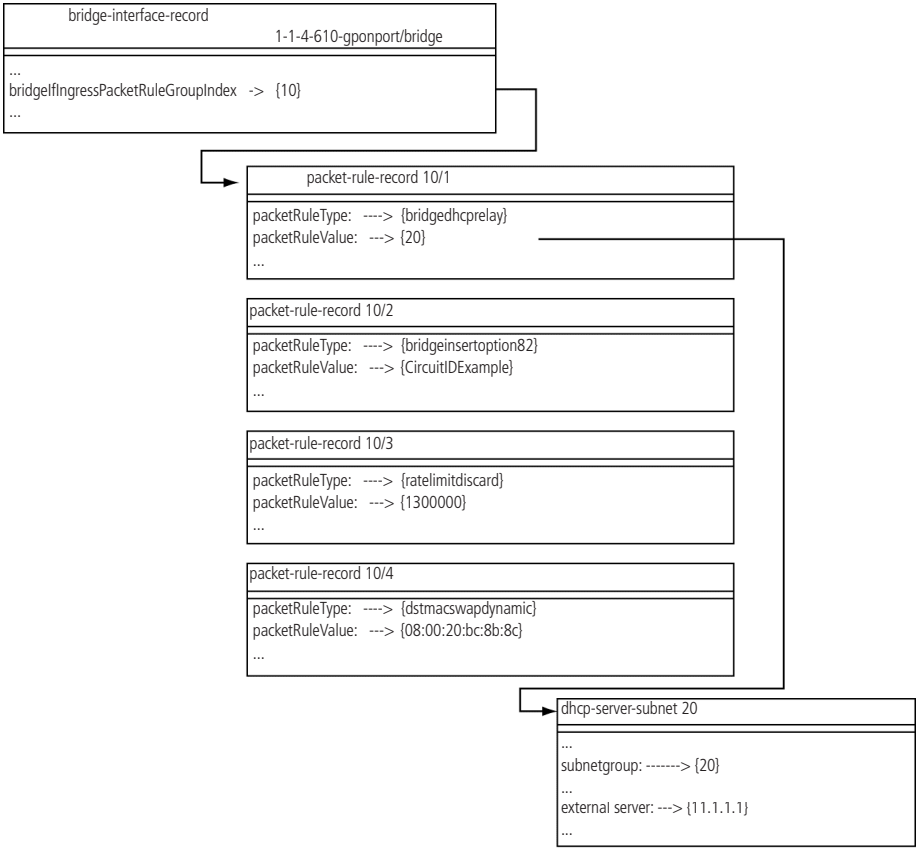
```
iSH> bridge add 1-1-1-5/gpononu gem 601 gtp 1 downlink vlan 100 tagged cos 7 outcosall 7
Adding bridge on 1-1-1-5/gpononu
Created bridge-interface-record 1-1-5-601-gpononu-100/bridge
```

9.9. Filtros para OLT 8820 G (packet-rule-record)

Visão geral de filtros de pacotes

A Interface de Linha de Comando (CLI) da OLT possui um mecanismo para a adição de filtros de pacotes para as interfaces de entrada, criando grupos de regras, dispostos no perfil *packet-rule-record*.

Múltiplas bridges podem usar o mesmo índice de grupo para regra de pacote da interface conforme exibido na imagem a seguir.



Múltiplos filtros de pacotes para a mesma bridge interface

Criação de filtros no perfil packet-rule-record

Você pode adicionar múltiplos filtros de pacotes com o comando *rule add* fornecendo tanto o índice de grupo como o índice do filtro ao adicionar uma regra.

O perfil *bridge-interface-record* acessa as regras pelo número do índice de grupo.

```
rule add <groupIndex/memberIndex> <packetRuleType>
<packetRuleValue...packetRuleValue2>
```

As opções *packetRuleValue* dependem do *packetRuleType* selecionado. Por exemplo, ao usar *bridgeinsertoption82*, você tem dois *packetRuleValues*, um para ID de circuito e um para ID remoto.

```
iSH> rule add bridgeinsertoption82 10/2 "circuitIDExample"
Created packet-rule-record 10/2 (bridgeinsertoption82)
iSH> rule add bridgeinsertoption82 10/3 "circuitIDExample" "remoteIDExample"
Created packet-rule-record 10/3 (bridgeinsertoption82)
```

Assim, o comando *bridge add* possui um parâmetro que se refere ao grupo com as variáveis *ipktrule* ou *epktrule*. Inserir *ipktrule* adiciona o filtro na entrada de bridge e *epktrule* adiciona o filtro na saída de bridge.

A tabela a seguir lista quais tipos de regra de pacote funcionam na entrada (*ipktrule*) e quais funcionam na saída (*epktrule*).

Regras de pacote	Entrada ou saída
bridgeinsertoption82	Entrada
bridgedhcprelay	Entrada
bridgeforbidoui	Entrada
ratelimitdiscard	Entrada, Saída
colorawareratelimitdiscard	Entrada, Saída
deny	Entrada, Saída

Regras de pacote de bridge que funcionam na entrada ou saída

Em bridges vinculadas na ONU é necessário habilitar o bridge stats para que a regra ratelimitdiscard de saída seja aplicada, porém é possível habilitar esse resurso para 128 bridges simultaneamente, dessa forma a Intelbras recomenda usar o gtp para limitar a banda de upstream.

Filtros são assimétricos, o que significa que o mesmo filtro pode ser aplicado à entrada e à saída da bridge usando valores diferentes.

Por exemplo:

```
iSH> bridge add 1-1-1-4/gpononu gem 601 gtp 1 vlan 777 ipktrule 10
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-601-gponport/bridge
```

Configuração de regras para filtros de pacotes

» **Criação de um índice de grupo para regra de pacote com registros de regra de pacote**

1. Use o comando *rule add* para adicionar um tipo de regra a um índice de grupo e os parâmetros que definem o tipo de regra;

   Este exemplo cria um índice de grupo com dois membros.

   A regra *dstmacswappingstatic* exibida exige um parâmero que seja um endereço MAC. Inserir ipktrule inserirá as regras na entrada da bridge.

```
iSH> rule add dstmacswapstatic 2/1 08:00:20:bc:8b:8c
Created packet-rule-record 2/1 (dstmacswapstatic)
```

2. Se necessário, adicione outra regra ao índice de grupo;

```
iSH> rule add bridgedhcprelay 3/1 20
Created packet-rule-record 3/1 (bridgedhcprelay)
```

3. Para visualizar o perfil *packet-rule-group* e seus membros;

```
iSH> rule show
Group/Member                          Type Value(s)
           2/1             dstmacswapstatic 08:00:20:bc:8b:8c
           3/1             bridgedhcprelay 20
2 record(s) found
```

4. Para criar um perfil de tráfego GPON;

```
iSH> new gpon-traffic-profile 1

gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: --->{0}: 512000
traffic-class: -------------> {ubr}:
compensated: --------------->{false}:
shared: -------------------->{false}:
dba-enabled: --------------->{false}:
dba-fixed-us-ubr-bw: ------->{0}:
dba-fixed-us-cbr-bw: ------->         {0}:
dba-assured-us-bw: -------->{0}:
dba-max-us-bw: ------------>{0}:
dba-extra-us-bw-type: ----->{nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

5. Crie bridges e inclua os grupos de regra de pacote IP.

```
iSH> bridge add 1-1-1-4/gpononu gem 601 gtp 1 downlink vlan 777 ipktrule 3
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-601-gponport/bridge
iSH> bridge add 1-1-2-0/eth uplink vlan 888 epktrule 2
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-888/bridge Bridge-path added successfully
```

» **Apagar uma regra de pacote**

Use o comando *rule delete* para apagar a regra.

```
iSH> rule delete 2/1
packet-rule-record 2/1 Delete complete
```

» **Verificação dos grupos de regra de pacote**

Use o comando *rule show* para exibir as regras.

```
iSH> rule show
Group/Member                                Type Value(s)
      2/1                  dstmacswapstatic 08:00:20:bc:8b:8c
     10/1                          bridgedhcprelay 20
     10/2                bridgeinsertoption82 circuitIDExample
     10/3        bridgeinsertoption82 circuitIDExample remoteIDExample
 4 record(s) found
```

Regra de pacote - DHCP opção 82 (bridgeinsertoption82)

Visão geral da opção 82 para DHCP relay

Ao atuar como um agente DHCP Relay, a OLT 8820 G inclui o campo opção 82 para identificar o cliente solicitante ao servidor DHCP. Há duas subopções para inserção da opção 82, Circuit ID (ID do Circuito) e Remote ID (ID Remoto). Ambas as opções são campos no formato de texto, embora tenham sido projetados para conter informações específicas.

Se o primeiro valor for definido, ele é considerado como uma sequência de texto literal a ser usado como o campo da subopção 1 no pacote DHCP. Se não for definido, é usada uma sequência de texto identificando a interface que receberam o pacote. Se o segundo valor for definido, ele é considerado como uma sequência de texto literal a ser usado como o campo da subopção 2 no pacote DHCP. Se não for definido, nenhuma subopção 2 é fornecida.

O uso deste recurso normalmente exigirá um grupo de regra distinto para cada interface, já que os valores de Circuit ID e Remote ID associados com as subopções 1 e 2 são distintos para cada interface.

O Circuit ID tem como objetivo fornecer informações sobre o circuito em que a solicitação chega. Normalmente são informações sobre a porta e a interface.

O RFC 3046 descreve possíveis usos do campo Circuit ID:

- » Número da interface do roteador
- » Número da porta do servidor de acesso remoto
- » Frame Relay DLC
- » Número do circuito virtual ATM
- » Número do circuito virtual de cabo de dados

O Remote ID tem como objetivo fornecer informações sobre o host remoto do circuito, no entanto, na prática a subopção geralmente contém informações sobre o agente DHCP Relay.

O RFC 3046 descreve possíveis usos do campo Remote ID:

- » Um "caller ID" número de telefone para conexão discada
- » Um "user name" solicitado por um servidor de acesso remoto
- » Um endereço de chamada ATM remoto
- » O endereço IP remoto de uma conexão ponto a ponto
- » Um endereço X.25 remoto para conexões X.25

Regra de pacote - DHCP opção 82 (bridgeinsertoption82) - configuração sem macros

As informações padrão inseridas no pacote durante o processo de DHCP Discovery é formatado como:

```
System 0_ip:IfName
```

O endereço systemIP é retirado do endereço IP configurado no perfil *system 0.* Se o endereço IP não está definido no perfil system 0, então o endereço *0.0.0.0* é inserido.

Criação de regra de pacote para bridgeinsertoption82 sem macros e definindo uma string (texto)

1. Crie o filtro bridgeinsertoption82 com informações padrão;

```
iSH> rule add bridgeinsertoption82 1/1
Created packet-rule-record 1/1 (bridgeinsertoption82)
```

2. Verifique a regra;

```
iSH> rule show
Group/Member                Type Value(s)
        1/1         bridgeinsertoption82
1 record(s) found
```

3. Para especificar o primeiro packetRuleType:

```
iSH> rule add bridgeinsertoption82 2/1 oakland
Created packet-rule-record 2/1 (bridgeinsertoption82)
```

4. Verifique a regra;

```
iSH> rule show
Group/Member                    Type Value(s)
        1/1         bridgeinsertoption82
        2/1         bridgeinsertoption82 oakland
2 record(s) found
```

5. Para especificar somente o segundo packetRuleType:

```
iSH> rule add bridgeinsertoption82 3/1 "" 510-555-1111
Created packet-rule-record 3/1 (bridgeinsertoption82)
```

6. Verifique a regra;

```
iSH> rule show
Group/Member                Type Value(s)
-------------------------------------------------------------------------
       1/1        bridgeinsertoption82
       2/1        bridgeinsertoption82 oakland
       3/1        bridgeinsertoption82        510-555-1111
3 record(s) found
```

7. Para especificar ambos os valores:

```
iSH> rule add bridgeinsertoption82 4/1 oakland 510-555-1111
Created packet-rule-record 4/1 (bridgeinsertoption82)
```

8. Verifique a regra.

```
iSH> rule show
Group/Member                  Type Value(s)
-------------------------------------------------------------------------
       1/1         bridgeinsertoption82
       2/1         bridgeinsertoption82 oakland
       3/1         bridgeinsertoption82        510-555-1111
       4/1         bridgeinsertoption82 oakland 510-555-1111
4 record(s) found
```

Regra de pacote - DHCP Opção 82 (bridgeinsertoption82) - configuração com macros

Se o campo *packetRuleValue* contém um ou mais caracteres de cifrão ($), a tag de texto do fornecedor que seria fornecida é substituído pelo conteúdo do campo, conforme segue:

- » Se nenhuma correspondência é encontrada, o cifrão é substituído pelo texto "Unknown".
- » Se uma correspondência é encontrada, o cifrão e o texto associado são substituídos pelo texto indicado.
- » O nome da macro e as abreviações são case-sensitive (há diferenciação entre letras maiúscula e minúscula).
- » As sequências de texto $macro podem ser integradas no texto literal. Esse texto é copiado à saída sem modificação.
- » Os formatos macro suportados podem ser inseridos no texto como $macroname ou $abbreviation. Assim, $SystemName e $NM dão o mesmo resultado, que é substituir o nome do sistema do perfil *system 0*.

Algumas das macros podem variar em efeito, dependendo do valor que se destinam a ser exibida.

- » $Gem e $Onu IDs são exibidos ou não dependendo de terem ou não um valor diferente de zero.
- » $Vlan exibe a SLAN-VLAN se o SLAN é diferente de zero, exibe apenas a VLAN se o SLAN for zero.

> **Observação:** o nome da macro e as abreviações são case-sensitive (há diferenciação entre letras maiúscula e minúscula)

Nome macro	Abreviação	Variações	Resultado
$SystemName	NM	NM	*sysname* do perfil *system 0*
$SystemIP	IP	Não	endereço *ipaddress* do perfil *system 0*
$IfName	IF	IF	*ifName* da bridge do perfil *IfTranslate*
$Address	AD	Não	*shelf-slot-port-subport-type* da interface física subjacente. Quando a interface é uma porta GPON, o tipo é apresentado como *gponport* e a subporta é a *GEM Port*
$Shelf	SH	Não	*Shelf* (atualmente sempre 1)
$Slot	SL	Não	*slot* do perfil I*fTranslate* da interface física subjacente
$Port	PT	Não	*port* (vide $Slot)
$SubPort	SP	Não	*subport* (vide $Slot.) Para GPON esta é a GEM Port
$Gem	GM	Sim	GEM Port (ou nada)
$Onu	ON	Yes	Número da ONU (ONUnumber ou nada)
$Type	TY	Não	Tipo (para GPON é *gponport*)
$Vlan	VN	Yes	SLAN-VLAN (ou -VLAN ou nada)
$Svlan	SV	Não	SLAN
$Cvlan	CV	Não	VLAN

$Vc	VC	Yes	VPI-VCI (ou nada)
$Vpi	VP	Não	VPI
$Vci	VI	Não	VCI
$Null	NL	Não	Nada (usado para alterar a manipilação de string constante do PPPoE)

Formato de macro suportado para texto definido com macro

Criação de regra de pacote para bridgeinsertoption82 com macros e definindo uma string (texto)

Crie um *packet-rule-record* usando nomes macro para criar uma sequência de texto definida pelo usuário. Sequências criadas com macros, incluindo as informações retiradas por macro, são limitadas a 48 caracteres.

1. Para criar uma sequência para o primeiro campo *packetRuleType*:
   a. Para criar uma sequência incluindo endereço IP do sistema, IfName (normalmente shelf/slot/port/subport) e VLAN ID para o primeiro *packetRuleType*, insira:

```
iSH> rule add bridgeinsertoption82 1/1 $SystemIP$IfName$Vlan
Created packet-rule-record 1/1 (bridgeinsertoption82)
```

A macro $SystemIP busca no system 0 o endereço IP e a configuração de bridge para o restante das informações.

Visualize o perfil *system 0.*

```
iSH> get system 0
system   0
syscontact: ---------------->          {}
sysname: ------------------->          {}
syslocation: --------------->          {}
leauthtraps: --------------->          {disabled}
setserialno: --------------->          {0}
zmsexists: ----------------->          {true}
connectionstatus: ---------->          {inactive}
zmsipaddress: -------------->          {172.16.89.220}
configsyncexists: ---------->          {false}
configsyncoverflow: --------->         {false}
configsyncpriority: -------->          {high}
configsyncaction: ---------->          {noaction}
configsyncfilename: --------->         {192.168.254.205_4_1307641204880}
configsyncstatus: ---------->          {synccomplete}
configsyncuser: ------------>          {}
configsyncpasswd: ---------->          ** private **
numshelves: ---------------->          {1}
shelvesarray: -------------->          {}
numcards: ------------------>          {1}
ipaddress: ------------------>         {192.168.254.205}
alternateipaddress: ------->           {0.0.0.0}
countryregion: ------------>           {brazil}
primaryclocksource: ------->           {0/0/0/0/0}
ringsource: ---------------->          {internalringsourcelabel}
revertiveclocksource: ----->           {true}
voicebandwidthcheck: ------>           {false}
alarm-levels-enabled: ----->           {critical+major+minor+warning}
userauthmode: -------------->          {local}
radiusauthindex: ---------->           {0}
secure: -------------------->          {disabled}
webinterface: -------------->          {enabled}
options: ------------------->          {NONE(0)}
```

b. Verifique *packet-rule-record.*

```
iSH> rule show
Group/Member                  Type Value(s)
-------------------------------------------------------------------------------
       1/1        bridgeinsertoption82 SystemIP$IfName$Vlan
1 record(s) found
```

c. Para criar um perfil de tráfego GPON.

```
iSH> new gpon-traffic-profile 1

gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: --->          {0}: 512000
traffic-class: ------------->           {ubr}:
compensated: --------------->           {false}:
shared: -------------------->           {false}:
dba-enabled: --------------->           {false}:
dba-fixed-us-ubr-bw: ------->           {0}:
dba-fixed-us-cbr-bw: ------->           {0}:
dba-assured-us-bw: -------->            {0}:
dba-max-us-bw: ------------>            {0}:
dba-extra-us-bw-type: ----->            {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

d. Adicione a regra *bridgeinsertoption82* para a bridge de downlink.

```
iSH> bridge add 1-1-1-4/gpononu gem 701 gtp 1 downlink vlan 101 ipktrule 1
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-701-gponport/bridge
```

Aplicar o filtro a esta bridge faz com que as sequências customizadas sejam inseridas nos pacotes durante o processo de DHCP discovery.

2. Para criar uma sequência para o segundo campo packetRuleType:

a. Para criar uma sequência somente para o segundo campo packetRuleType da regra bridgeinsertoption82:

```
iSH> rule add bridgeinsertoption82 2/1 "" $SystemName
Created packet-rule-record 2/1 (bridgeinsertoption82)
```

b. Verifique *packet-rule-record.*

```
iSH> rule show
Group/Member                Type Value(s)
-------------------------------------------------------------------------------
     1/1      bridgeinsertoption82 $SystemIP$IfName$Vlan
     2/1      bridgeinsertoption82        $SystemName
2 record(s) found
```

3. Para criar uma sequência para o primeiro e o segundo campo packetRuleType:

a. Para criar uma sequência para o primeiro e o segundo campo packetRuleType da regra bridgeinsertoption82:

```
iSH> rule add bridgeinsertoption82 3/1 $SystemName $SystemIP$IfName$Vlan
Created packet-rule-record 3/1 (bridgeinsertoption82)
```

b. Verifique *packet-rule-record.*

```
iSH> rule show
Group/Member                Type Value(s)
-------------------------------------------------------------------------------
     1/1      bridgeinsertoption82 $SystemIP$IfName$Vlan
     2/1      bridgeinsertoption82 $SystemName
     3/1      bridgeinsertoption82 $SystemName $SystemIP$IfName$Vlan
```

```
3 record(s) found
```

4. Adicione uma regra de pacote para bridgeinsertoption82 para uma bridge de downlink.

```
iSH> bridge add 1-1-1-5/gpononu gem 901 gtp 1 downlink vlan 1001 ipktrule 3
Adding bridge on 1-1-1-5/gpononu
Created bridge-interface-record 1-1-5-901-gponport/bridge
```

Aplicar o filtro a esta bridge faz com que as sequências customizadas sejam inseridas nos pacotes durante o processo de DHCP discovery.

Apagar um packet-rule-record

Use o *comando rule delete* para apagar uma regra de pacote.

```
iSH> rule delete 1/1
packet-rule-record 1/1 Delete complete
```

Regra de pacote - DHCP relay e Filtro OUI

DHCP relay

Crie um *packet-rule-record* para pacotes DHCP utilizando o comando *rule add* especificando a opção e grupo da regra.

packetRuleValue contém o ID do grupo da subre do DHCP. Se somente a opção DHCP relay for usada, as informações de "Opção 82" são exibidas em formato hexadecimal.

```
iSH> dhcp-relay add 20 11.1.1 NULL
Operation completed successfully.
This DHCP Relay Agent is available only for bridged connections; Routed interfaces will not be
able to use it.
Created DHCP Relay Agent: group: 20, index: 1
```

```
iSH> rule add bridgedhcprelay 10/1 20
Created packet-rule-record 10/1 (bridgedhcprelay)
```

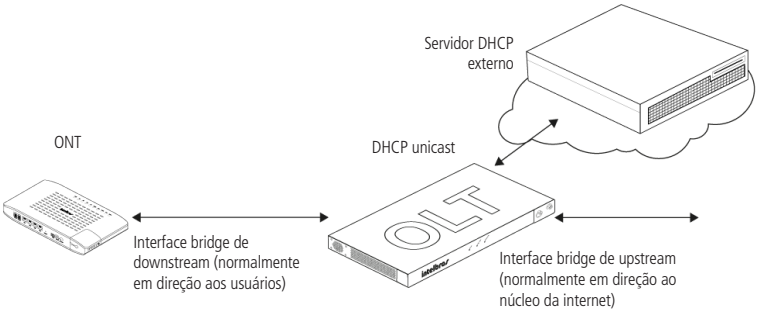
Verifique a regra.

```
iSH> rule show
Group/Member                    Type Value(s)
-------------------------------------------------------
       10/1        bridgedhcprelay 20
1 record(s) found
```

Configuração de bridge com DHCP relay

A OLT 8820 G permite que bridges sejam configuradas como agentes de DHCP Relay. Todas as mensagens DHCP na bridge terão informações de "Opção 82" inseridas para serem transmitidas através de uma interface IP para um servidor DHCP externo.

A imagem a seguir ilustra o fluxo de tráfego quando a OLT 8820 G é configurado com uma bridge com suporte a DHCP Relay.



Bridge com suporte a DHCP relay

Configuração de bridges para suportar DHCP relay

Este procedimento descreve como configurar bridges com suporte a DHCP Relay. A função de DHCP relay é inserida durante a criação da bridge ao utilizar o comando *bridge add* e adicionando a regra dhcp-relay.

Antes de adicionar o DHCP Relay, você deve ter uma interface IP Na OLT com uma rota disponível para o servidor DHCP.

Uma vez que os elementos acima estão configurados, basta utilizar o comando *dhcp-relay add* para configurar o suporte a DHCP relay na bridge desejada.

1. Para configurar suporte para DHCP Relay em uma bridge, use o comando *dhcp-relay add*, que utiliza o parâmetro *subnetgroup* como identificador:

```
dhcp-relay add [<subnetgroup>] <ip-address> NULL
```

O parâmetro *subnetgroup* é o identificador de índice do grupo da sub-rede do servidor DHCP externo.

O parâmetro *ip-address* é o endereço do servidor DHCP externo. Para configurar o DHCP Relay nas bridges, adicione o parâmetro *NULL*.

2. Adicione a regra *dhcp-relay* usando o comando *rule add* que define que o identificador subnetgroup está no grupo de regra de pacote;
3. Crie uma bridge (ou modifique uma bridge existente) incluindo o grupo de regra de pacote.

Exemplo de configuração de bridge com suporte a DHCP relay

1. Adicione uma interface IP com uma rota para o servidor DHCP;

```
iSH> interface add 1-1-2-0/eth 11.1.1.198/24
Created ip-interface-record 1-1-2-0-eth/ip
```

2. Configure o suporte a DHCP relay na bridge utilizando o comando dhcp-relay add;

```
iSH> dhcp-relay add 20 11.1.1.1 NULL
Operation completed successfully.
This DHCP Relay Agent is available only for bridged connections;
Routed interfaces will not be able to use it.
Created DHCP Relay Agent: group: 20, index: 2
```

3. Adicione a regra dhcp-relay ao grupo de regras de pacote;

```
iSH> rule add bridgedhcprelay 10/1 20
Created packet-rule-record 10/1 (bridgedhcprelay)
```

4. Para criar um perfil de tráfego GPON;

```
iSH> new gpon-traffic-profile 1

gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ---------->  {0}: 512000
traffic-class: ------------------->   {ubr}:
compensated: --------------------->  {false}:
shared: -------------------------->  {false}:
dba-enabled: --------------------->  {false}:
dba-fixed-us-ubr-bw: ------------->  {0}:
dba-fixed-us-cbr-bw: ------------->  {0}:
dba-assured-us-bw: --------------->  {0}:
dba-max-us-bw: ------------------->  {0}:
dba-extra-us-bw-type: ------------>  {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

5. Crie uma bridge e inclua os grupos de regra de pacote;

```
iSH> bridge add 1-1-1-4/gpononu gem 601 gtp 1 downlink vlan 700 ipktrule 10
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-601-gpononu-700/bridge
```

6. Você pode verificar as informações nos perfis:

a. Verifique o grupo de sub-rede *dhcp-server-subnet.*

```
iSH> get dhcp-server-subnet 20
dhcp-server-subnet 20
network: ------------------->        {0.0.0.0}
netmask: ------------------->        {0.0.0.0}
domain: -------------------->        {0}
range1-start: -------------->        {0.0.0.0}
range1-end: ---------------->        {0.0.0.0}
range2-start: -------------->        {0.0.0.0}
range2-end: ---------------->        {0.0.0.0}
range3-start: -------------->        {0.0.0.0}
range3-end: ---------------->        {0.0.0.0}
range4-start: -------------->        {0.0.0.0}
range4-end: ---------------->        {0.0.0.0}
default-lease-time: -------->        {-1}
min-lease-time: ------------>        {-1}
max-lease-time: ------------>        {-1}
boot-server: --------------->        {0.0.0.0}
bootfile: ------------------>        {}
default-router: ------------>        {0.0.0.0}
primary-name-server: ------->        {0.0.0.0}
secondary-name-server: ----->        {0.0.0.0}
domain-name: --------------->        {}
subnetgroup: --------------->        {20}  sub-rede do servidor dhcp
stickyaddr: ---------------->        {enable}
external-server: ----------->        {11.1.1.1}  endereço do servidor dhcp
external-server-alt: ------->        {0.0.0.0}
```

b. Verifique se o perfil *bridge-interface-record* contém o grupo de regra de pacote:

```
iSH> get bridge-interface-record 1-1-4-601-gpononu-700/bridge
bridge-interface-record 1-1-4-501-gpononu-700/bridge
vpi: ------------------------------------>              {0}
vci: ------------------------------------>              {0}
vlanId: ---------------------------------->             {840}
stripAndInsert: -------------------------->             {false}
customARP: ------------------------------->             {false}
filterBroadcast: ------------------------->             {false}
learnIp: --------------------------------->             {true}
learnUnicast: ---------------------------->             {true}
maxUnicast: ------------------------------>             {5}
learnMulticast: -------------------------->             {true}
forwardToUnicast: ------------------------>             {false}
forwardToMulticast: ---------------------->             {false}
forwardToDefault: ------------------------>             {true}
bridgeIfCustomDHCP: ---------------------->             {false}:
bridgeIfIngressPacketRuleGroupIndex: ----->             {10}: regra
vlanIdCOS: ------------------------------->             {0}
outgoingCOSOption: ----------------------->             {disable}
outgoingCOSValue: ------------------------>             {0}
s-tagTPID: ------------------------------->             {0x8100}
s-tagId: --------------------------------->             {0}
s-tagStripAndInsert: --------------------->             {true}
s-tagOutgoingCOSOption: ------------------>             {s-tagdisable}
s-tagIdCOS: ------------------------------>             {0}
agOutgoingCOSValue: ---------------------->             {0}
mcastControlList: ------------------------>             {}
maxVideoStreams: ------------------------->             {0}
isPPPoA: --------------------------------->             {false}
floodUnknown: ---------------------------->             {false}
floodMulticast: -------------------------->             {false}
IfEgressPacketRuleGroupIndex: ------------>             {0}:
bridgeIfTableBasedFilter: ----------------->            {NONE(0)}:
bridgeIfDhcpLearn: ----------------------->             {NONE(0)}:
mvrVlan: --------------------------------->             {0}
vlan-xlate-from: ------------------------->             {0}
slan-xlate-from: ------------------------->             {0}
```

c. Verifique se a regra existe (também é uma boa maneira de encontrar o número do grupo):

```
iSH> rule show
Group/Member          Type Value(s)
      10/1      bridgedhcprelay 20
1 record(s) found
```

d. Verifique as ligações do perfil *packet-rule-record* para o grupo da sub-rede do servidor DHCP:

```
iSH> get packet-rule-record 10/1
packet-rule-record 10/1
packetRuleType: -------->   {bridgedhcprelay}
packetRuleValue: ------->   {20}
packetRuleValue2: ------>   {}
packetRuleValue3: ------>   {}
packetRuleValue4: ------>   {}
packetRuleValue5: ------>   {}
```

Filtro OUI

A regra *bridgeforbidoui* é uma forma de filtro baseada no endereço OUI (Organizational Unique Indentifer).

Ao usar a opção *bridgeforbidoui* em uma regra de pacote, deve-se inserir os primeiros três bytes do endereço MAC, que são utilizados para identificar o fabricante. Esses três bytes são conhecidos como Organizational Unique Identifier (OUI).

Configuração de bridges com suporte a Filtro OUI

1. Adicione a regra *bridgeforbidoui* ao grupo de regra de pacote IP;

```
iSH> rule add bridgeforbidoui 10/1 00:aa:bb
Created packet-rule-record 10/1 (bridgeforbidoui)
```

Os pacotes de um dispositivo com endereço MAC que começa com "00:aa:bb", código do fabricante em formato hexadecimal (OUI - Organizational Unique Identifier) serão bloqueados.

2. Verifique a regra;

```
iSH> rule show
Group/Member                Type Value(s)
       10/1        bridgeforbidoui 00:aa:bb
1 record(s) found
```

3. Crie uma bridge na porta upstream ethernet;

```
iSH> bridge add 1-1-2-0/eth tls vlan 50 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-50/bridge
Bridge-path added successfully
```

4. Criar um perfil de tráfego GPON;

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: -------->    {0}: 512000
traffic-class: ----------------->    {ubr}:
compensated: ------------------->    {false}:
shared: ------------------------->    {false}:
dba-enabled: -------------------->    {false}:
dba-fixed-us-ubr-bw: ------------>    {0}:
dba-fixed-us-cbr-bw: ------------>    {0}:
dba-assured-us-bw: ------------->    {0}:
dba-max-us-bw: ----------------->    {0}:
dba-extra-us-bw-type: ---------->    {nonassured}:
.................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

5. Crie uma bridge e inclua os grupos de regra de pacote IP;

```
iSH> bridge add 1-1-1-4/gpononu gem 601 gtp 1 downlink vlan 700 ipktrule 10
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-601-gpononu-700/bridge
```

Controle de banda de porta e serviço, limite por taxa única ou taxa dupla

Visão geral do controle de banda

O controle de banda da OLT 8820 G permite ser configurada através de dois métodos de policiamentodo de limite de banda:

- » Limite por taxa única (CIR).
- » Limite por taxa dupla (CIR e PIR).

O limite por taxa única permite que os prestadores de serviços forneçam aos clientes serviços com largura de banda limitada ao CIR (Commited Information Rate) isto é, todo o tráfego de dados até a taxa configurada no CIR é garantida.

O limite por taxa dupla permite que os prestadores de serviços fornecam aos clientes serviços com largura de banda limitada a duas taxas, o CIR (Commited Information Rate) e ao PIR (Peak Information Rate). Neste caso, todo o tráfego até o CIR é garantido e todo o tráfego acima da PIR é descartado. O tráfego entre o CIR e o PIR é manuseado da melhor forma possível.

O limite por taxa única e o limite por taxa dupla são configurados por VLAN ID.

Após configurar uma interface com limite de banda, a taxa de transmissão do tráfego é monitorada e medida para verificar conformidade com um contrato estabelecido.O tráfego fora da conformidade é descartado e o tráfego em conformidade passa pela interface sem alterações. A OLT 8820 G segue a RFC 2697 e RFC 2698 para limitação de banda.

Os modos de limitação de taxa na OLT 8820 G são:

- » Limite por taxa única e dupla sem colorização (color blind).

O limite de banda é realizado na interface sem usar o campo Class of Service (CoS) do quadro ethernet, presumindo que todos os pacotes de um fluxo "não possuem cores" e são tratados igualmente quando estão no intervalo da CIR.

Para limites por taxa dupla sem colorização, os pacotes são tratados igualmente até o CIR e são tratados baseados no melhor esforço entre as taxas definidas no CIR e no PIR.

Você pode configurar marcações amarelas em regras de pacote de taxa dupla. Neste caso, um valor de CoS é inserido nos pacotes que excedem o CIR.

O modo sem colorização é usado com mais frequência quando é configurado um único serviço por VLAN.

- » Limite por taxa única e dupla com colorização (color aware).

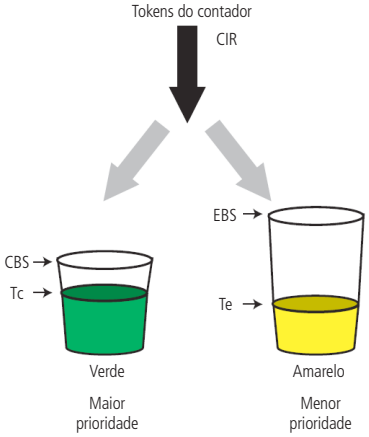
O limite de banda observa que o fluxo de pacote de entrada possui colorização e que cada pacote é marcado de verde, amarelo ou vermelho, indicando se um pacote tem alta, média ou baixa prioridade. O campo de cor mapeia o valor da prioridade CoS nos pacotes tagged (marcado) e o valor de ToS precedência IP em pacotes untagged (não marcados).

O modo com colorização é usado com mais frequência quando é configurado múltiplos serviços em uma única VLAN, garantindo que os pacotes de maior prioridade passem se houver contenção na largura de banda.

Esquema de contador de taxa única

O esquema de marcador de taxa única da RFC 2697 usa um contador para medir a capacidade na linha pela contagem de tokens. Os contadores são usados para determinar quais pacotes são descartados. A ideia é que o balde verde enche mais rápido do que o balde amarelo.

Há três parâmetros que determinam quais pacotes são descartados - um CIR que fornece tokens para serem contados e dois baldes, Committed Burst Size (CBS) e Excess Burst Size (EBS), que proporcionam dois níveis de prioridade.



Esquema de contador de taxa única

CIR é a taxa que determina a velocidade que os tokens enchem os baldes. Ambos os baldes começam estando cheios. É importante entender que este não é um esquema de buffering, já que os pacotes de entrada não são enfileirados para entrega posterior.

Para cada incremento do CIR os baldes são preenchidos.

```
if Tc < CBS
    then
      increment Tc
  else if Te < EBS
         then
           increment Te
         else
           do nothing (do not increment either because they are both full)
```

O balde verde encherá primeiro e mais rápido, caso não esteja cheio, o balde amarelo não será incrementado até que Tc >= CBS.

Existem regras sobre como o tamanho do balde verde (CBS) e do balde amarelo (EBS) deve ser configurado. No mínimo um dos CBS ou EBS deve ser maior que zero. Além disso, pelo menos um CBS ou EBS deve ser maior que o maior pacote esperado no fluxo de entrada, já que os pacotes maiores do que CBS ou EBS serão descartados.

Com limite de banda sem colorização, o tamanho do pacote de entrada determina se o pacote irá passar. Se há tokens suficientes em verde ou amarelo o pacote passará. Os tokens correspondentes ao tamanho do pacote serão decrementado do balde apropriado. Se houver pacotes que são maiores do que a quantidade de tokens em qualquer balde, esses pacotes são descartados. Os pacotes que são maiores do que qualquer tamanho de balde quando cheios são descartados.

if incoming packet smaller than Tc

then

decrement Tc by size of packet

send packet

else if packet smaller than Te

then

deccrement Te by size of packet

send packet

else

drop packet

Com limite de banda colorizado, presume-se que os pacotes estão sendo marcados por um dispositivo no upstream. Os pacotes marcados de vermelho são descartados. Os pacotes marcados de amarelo são com melhor esforço e os marcados de verde são de maior prioridade e devem ter a menor chance de descarte. O comportamento depende da configuração dos parâmetros de CBS e EBS.

Observação: os valores padrão para CBS e EBS são bons para a maioria das situações e são calculados pelo sistema para o desempenho ideal

Com limite de banda colorizado, o tamanho e a cor determinam se o pacote será descartado.

if incoming packet is green AND is smaller than Tc

then

decrement Tc by size of packet

send packet

else if packet is green or yellow AND is smaller than Te

then

decrement Te by size of packet

send packet

else

drop packet

Assim, todos os pacotes vermelhos são descartados. Normalmente, o dispositivo de marcação no upstream marcará de vermelho os pacotes que estão fora da faixa.

Configurar limite de banda sem colorização

O limite de banda sem colorização normalmente é definida quando um serviço é fornecido por VLAN. A taxa de informação comprometida, CIR, é definida em kilobytes por segundo. Para qualquer taxa acima da CIR definida, os pacotes serão descartados.

Por exemplo, na imagem a seguir, você deve usar o método sem colorização para definir a VLAN 100 para descartar pacotes quando a taxa for superior a 5 Mbps, já a VLAN 200 descartar pacotes quando a taxa for superiot a 3 Mbps e a VLAN 200 para descartar pacotes quando a taxa for superior a 6 Mbps.

Um serviço por VLAN em uma interface

Controles de limite de banda

A sintaxe para o limite de banda sem colorização é a seguinte:

```
rule add ratelimitdiscard <groupIndex/memberIndex> rate <rate> [peak <value>] [cbs
<value>] [ebs <value>] [ymark <value>]
```

Campo	Definição	Taxa	Descrição
rate	Committed Information Rate (CIR)	kbps	A taxa média garantida para um circuito virtual. Se a taxa real for maior do que o CIR, os pacotes serão descartados
peak rate	Peak Information Rate (PIR)	kbps	A taxa de pico em que o tráfego acima dessa taxa é descartado e o tráfego entre o CIR e o PIR é tratado numa base de melhor esforço
cbs	Committed Burst Size	bps	A taxa de dados máxima que pode ser transportada em condições normais. Essa taxa é superior à CIR, mas inferior à EBS
ebs	Excess Burst Size	bps	A taxa de dados máxima que o circuito tentará transportar
ymark	Marcação amarela		Os pacotes são marcados com o valor fornecido. Quando o parâmetro não é configurado, os pacotes não recebem marcação amarela. A valor varia de 0 a 7

Definição dos controles de limite de banda

Observação: os valores padrão para CBS e EBS são bons para a maioria das situações. Esses valores são calculados pelo sistema para um desempenho ideal

Configurar policiamento sem colorização para taxa única

O comando *rule add ratelimitdiscard* define a taxa a partir do qual os pacotes serão descartados para configuração de limite de banda por taxa única.

```
rule add ratelimitdiscard <groupIndex/memberIndex> rate <rate> [peak <value>] [cbs <value>] [ebs <value>] [ymark <value>]
```

O limite de banda por taxa dupla é permitida somente na saída da interface.

O policiamento sem colorização funciona tanto na entrada como na saída de uma interface para limite de banda por taxa única.

» **Caso 1:** configurar um filtro de policiamento sem colorização na entrada de uma bridge para limitar a banda através de uma uma única taxa

1. Criar a regra que será aplicada nos pacotes de entrada na bridge (do usuário final para a OLT);

```
iSH> rule add ratelimitdiscard 1/1 rate 1800
Created packet-rule-record 1/1 (ratelimitdiscard)
```

2. Para verificar a regra, use o comando *rule show*. Para visualizar as regras do tipo ratelimitdiscard inserir o comando *rule show ratelimitdiscard:*

```
iSH> rule show ratelimitdiscard
Group/Member                    Type Value(s)
        1/1         ratelimitdiscard cir 1800kbps cbs 120000bytes ebs 130000bytes
1 record(s) found
```

3. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de entrada na bridge;

```
iSH> bridge add 1-1-1-2/gpononu gem 701 gtp 1 downlink vlan 200 tagged ipktrule 1
Adding bridge on 1-1-1-2/gpononu
Created bridge-interface-record 1-1-1-701-gponport-200/bridge
```

4. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de entrada e saída da bridge.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 200 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-200/bridge
Bridge-path added successfully
```

» **Caso 2:** configurar um filtro de policiamento sem colorização na entrada e saída de uma bridge para limitar a banda através de uma única taxa

Esse exemplo descreve como os prestadores de serviço podem utilizar duas regras de filtro de pacote para limitar a banda dos assinantes. permitindo maior largura de banda de downstream (da OLT para o assinante) e menor largura de banda de upstream (tráfego do assinante que passa pela OLT e chega ao core da rede).

1. Criar a regra que será aplicada nos pacotes de entrada na bridge (do usuário final para a OLT);

```
iSH> rule add ratelimitdiscard 2/1 rate 1300
Created packet-rule-record 2/1 (ratelimitdiscard)
```

2. Criar a regra que será aplicada nos pacotes de saída da bridge (da OLT para o usuário final);

```
iSH> rule add ratelimitdiscard 3/1 rate 6000
Created packet-rule-record 3/1 (ratelimitdiscard)
```

3. Para verificar a regra, use o comando rule show. Para visualizar as regras do tipo ratelimitdiscard inserir o comando rule show ratelimitdiscard:

```
iSH> rule show ratelimitdiscard
Group/Member                Type Value(s)
       1/1        ratelimitdiscard cir 1800 kbps cbs 120000 bytes ebs 130000 bytes
       2/1        ratelimitdiscard cir 1300 kbps cbs 120000 bytes ebs 130000 bytes
       3/1        ratelimitdiscard cir 6000 kbps cbs 120000 bytes ebs 130000 bytes
3 record(s) found
```

4. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de entrada e saída da bridge;

```
iSH> bridge add 1-1-1-2/gpononu gem 901 gtp 1024 downlink vlan 100 tagged ipktrule 2 epktrule 3
Adding bridge on 1-1-1-2/gpononu
Created bridge-interface-record 1-1-1-901-gponport-100/bridge
```

> **Observação:** ambas as regras de pacote devem ser aplicadas à bridge interface no mesmo comando *bridge add*

5. Para verificar as regras de pacote configurada em uma bridge, utilizar o comando *get bridge-interface-record* na bridge desejada;

```
iSH> get bridge-interface-record      1-1-1-701-gponport/bridge
bridge-interface-record     1-1-1-701-gponport/bridge
vpi: ----------------------------------------> {0}
vci: ----------------------------------------> {0}
vlanId: -------------------------------------> {100}
stripAndInsert: ------------------------------> {true}
customARP: ----------------------------------> {false}
filterBroadcast: ----------------------------> {false}
learnIp: ------------------------------------> {true}
learnUnicast: -------------------------------> {true}
maxUnicast: ---------------------------------> {5}
learnMulticast: -----------------------------> {true}
forwardToUnicast: ---------------------------> {false}
forwardToMulticast: -------------------------> {false}
forwardToDefault: ---------------------------> {true}
bridgeIfCustomDHCP: -------------------------> {false}
bridgeIfIngressPacketRuleGroupIndex: --------> {2}
vlanIdCOS: ----------------------------------> {0}
outgoingCOSOption: --------------------------> {disable}
outgoingCOSValue: ---------------------------> {0}
s-tagTPID: ----------------------------------> {0x8100}
s-tagId: ------------------------------------> {0}
s-tagStripAndInsert: ------------------------> {true}
s-tagOutgoingCOSOption: ---------------------> {s-tagdisable}
s-tagIdCOS: ---------------------------------> {0}
s-tagOutgoingCOSValue: ----------------------> {0}
mcastControlList: ---------------------------> {}
maxVideoStreams: ----------------------------> {0}
isPPPoA: ------------------------------------> {false}
floodUnknown: -------------------------------> {false}
```

```
floodMulticast: ------------------------------> {false}
bridgeIfEgressPacketRuleGroupIndex: ---------> {3}
bridgeIfTableBasedFilter: -------------------> {NONE(0):
bridgeIfDhcpLearn: --------------------------> {NONE(0)}:
mvrVlan: ------------------------------------> {0}
vlan-xlate-from: ----------------------------> {0}
slan-xlate-from: ----------------------------> {0}
```

6. Configurar a bridge de uplink com VLAN 100.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 100 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-100/bridge
```

Configurar policiamento sem colorização para taxa dupla

O comando rule add ratelimitdiscard configura o intervalo para a taxa garantida (CIR) a taxa de pico (PIR). Os pacotes acima do PIR serão descartados e o tráfego entre o CIR e o PIR serão tratados baseados no melhor esforço.

» **Caso 3:** configurar um filtro de policiamento sem colorização para limitar a banda através de taxa dupla

Este exemplo descreve a configuração para a taxa garantida (CIR) a taxa de pico (PIR) a partir do qual os pacotes serão descartados na saída da bridge de downlink. Pacotes entre o CIR e o PIR serão tratados baseado no melhor esforço.

> **Observação:** o policiamento sem colorização com dupla taxa funciona apenas para pacotes de saída de uma bridge

1. Criar a regra de taxa dupla que será aplicada nos pacotes de saída da bridge downlink;

```
iSH> rule add ratelimitdiscard 4/1 rate 2000 peak 4000
Created packet-rule-record 4/1 (ratelimitdiscard)
```

2. Para verificar a regra, use o comando *rule show*. Para visualizar as regras do tipo ratelimitdiscard inserir o comando *rule show ratelimitdiscard:*

```
iSH> rule show ratelimitdiscard
Group/Member              Type Value(s)
-------------------------------------------------------------------
     1/1      ratelimitdiscard cir 1800k cbs 120000bytes ebs 130000bytes
     2/1      ratelimitdiscard cir 1300k cbs 120000bytes ebs 130000bytes
     3/1      ratelimitdiscard cir 6000k cbs 120000bytes ebs 130000bytes
     4/1      ratelimitdiscard cir 2000k cbs 120000bytes pir 4000k
ebs 130000bytes
4 record(s) found
```

3. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de saída da bridge;

```
iSH> bridge add 1-1-1-4/gpononu gem 601 gtp 1 downlink vlan 100 epktrule 4 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-601-gponport-100/bridge
```

4. Configurar a bridge de uplink com VLAN 100.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 100 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-100/bridge
Bridge-path added successfully
```

» **Caso 4:** configurar um filtro de policiamento sem colorização para limitar a banda através de taxa dupla com ymark

Este exemplo descreve a configuração para a taxa garantida (CIR) a taxa de pico (PIR) a partir do qual os pacotes serão descartados na saída da bridge de downlink. Pacotes entre o CIR e o PIR serão tratados baseado no melhor esforço.

Você pode usar o valor *ymark* para marcar pacotes que fluem entre o CIR e o PIR para dispositivos de upstream com policiamento com colorização.

> **Observação:** o policiamento sem colorização com dupla taxa funciona apenas para pacotes de saída de uma bridge

1. Criar a regra de taxa dupla que será aplicada nos pacotes de saída da bridge downlink.

```
iSH> rule add ratelimitdiscard 3/1 rate 18000 peak 36000 ymark 1
Created packet-rule-record 3/1 (ratelimitdiscard)
```

2. Para verificar a regra, use o comando *rule show*. Para visualizar as regras do tipo ratelimitdiscard inserir o comando *rule show ratelimitdiscard:*

```
iSH> rule show ratelimitdiscard
Group/Member              Type Value(s)
     3/1      ratelimitdiscard cir 1800k cbs 120000bytes pir 3600k
ebs 130000bytes ym 1
3 record(s) found
```

3. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de saída da bridge;

```
iSH> bridge add 1-1-1-4/gpononu gem 901 gtp 1 downlink vlan 200 tagged epktrule 3
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-901-gponport-200/bridge
```

4. Configurar a bridge de uplink com VLAN 200.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 200 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-200/bridge
Bridge-path added successfully
```

Configurar limite de banda colorizado

O controle de banda colorizado normalmente é definido quando mais de um serviço é fornecido por VLAN.

Os parâmetros de alta prioridade e baixa prioridade permitem que você designe quais valores na escala serão tratados como verde, amarelo e vermelho. Se a alta prioridade é definida em 5 e a baixa prioridade é definida em 3, o valor CoS da tabela de cores mudará para que 7, 6 e 5 sejam verdes e 4 e 3 serão amarelos e 2, 1 e 0 serão descartados.

Controles de limite de banda

A sintaxe de controle de banda colorizado é a seguinte:

```
rule add colorawareratelimitdiscard <groupIndex/memberIndex> rate <rate> [peak <value>] [cbs
<value>][ebs <value>] [ymark <value>] [hi-priority <value>] [low-priority <value>]
```

Campo	Definição	Taxa	Descrição
rate	Committed Information Rate (CIR)	kbps	A taxa média garantida para um circuito virtual. Se a taxa real for maior do que o CIR, os pacotes serão descartados
peak rate	Peak Information Rate (PIR)	kbps	A taxa de pico em que o tráfego acima dessa taxa é descartado e o tráfego entre o CIR e o PIR é tratado numa base de melhor esforço
cbs	Committed Burst Size	bps	A taxa de dados máxima que pode ser transportada em condições normais. Essa taxa é superior à CIR, mas inferior à EBS
ebs	Excess Burst Size	bps	A taxa de dados máxima que o circuito tentará transportar
ymark	Marcação amarela		Os pacotes são marcados com o valor fornecido. Quando o parâmetro não é configurado, os pacotes amarelos não são alterados. O valor varia de 0 a 7
hi	hi-priority		Os pacotes são marcados conforme as cores que correspondem aos valores CoS. O valor varia de 0 a 7
lo	low-priority		Os pacotes são marcados conforme as cores que correspondem aos valores CoS. O valor varia de 0 a 7

Definição dos controles de limite de banda colorizado

Observação: os valores padrão para CBS e EBS são bons para a maioria das situações. Esses valores são calculados pelo sistema para um desempenho ideal

Configurar policiamento colorizado para taxa única

O comando *rule add colorawareratelimitdiscard* define a prioridade de cor e a taxa acima da qual os pacotes serão descartados.

```
|rule add colorawareratelimitdiscard <groupIndex/memberIndex> rate <rate> [peak <value>] [cbs
<value>][ebs <value>] [ymark <value>] [hi-priority <value>] [low-priority <value>]
```

» **Caso 1:** configurar um filtro de policiamento colorizado na saída de uma bridge para limitar a banda através de uma uma única taxa

1. Criar a regra de policiamento colorizado que será aplicada nos pacotes de saída na bridge;

```
iSH> rule add colorawareratelimitdiscard 1/1 rate 1300
Created packet-rule-record 1/1 (colorawareratelimitdiscard)
```

A alta prioridade (hi-priority) e baixa prioridade (low-priority) são definidas nos padrões conforme exibido na tabela anterior.

2. Para verificar a regra, use o comando *rule show*. Para visualizar as regras do tipo ratelimitdiscard inserir o comando *rule show ratelimitdiscard:*

```
iSH> rule show
Group/Member              Type Value(s)
     1/1      colorawareratelimitdiscard cir 1300kbps cbs 120000bytes ebs
130000bytes hi 4 lo 0
1 record(s) found
```

3. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de saída da bridge;

```
iSH> bridge add 1-1-1-3/gpononu gem 901 gtp 1 downlink vlan 600 tagged epktrule 1
Adding bridge on 1-1-1-3/gpononu
Created bridge-interface-record 1-1-1-901-gponport-600/bridge
```

3. Configurar a bridge de uplink com VLAN 600.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 600 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-600/bridge
```

Configurar policiamento colorizado para taxa dupla

O comando *rule add colorawareratelimitdiscard* configura o intervalo para a taxa garantida (CIR) a taxa de pico (PIR). Os pacotes acima do PIR serão descartados e o tráfego entre o CIR e o PIR serão tratados baseados no melhor esforço.

» **Caso 2:** configurar um filtro de policiamento colorizado para limitar a banda através de taxa dupla

Este exemplo descreve a configuração para a taxa garantida (CIR) a taxa de pico (PIR) a partir do qual os pacotes serão descartados na saída da bridge de downlink. Pacotes entre o CIR e o PIR serão tratados baseado no melhor esforço.

> **Observação:** o policiamento colorizado com taxa dupla funciona somente para pacotes de saída em uma bridge

1. Criar a regra de policiamento colorizado com dupla taxa que será aplicada nos pacotes de saída na bridge;

```
iSH> rule add colorawareratelimitdiscard 2/1 rate 1800 peak 3600
Created packet-rule-record 2/1 (colorawareratelimitdiscard)
```

2. Para verificar a regra, use o comando *rule show*. Para visualizar as regras do tipo ratelimitdiscard inserir o comando *rule show ratelimitdiscard:*

```
iSH> rule show ratelimitdiscard
Group/Member              Type Value(s)
     1/1      colorawareratelimitdiscard cir 1300kbps cbs 120000bytes ebs
130000bytes hi 4 lo 0
     2/1      colorawareratelimitdiscard cir 1800kbps cbs 120000bytes pir
3600kbps ebs 130000bytes hi 4 lo 0
2 record(s) found
```

3. Criar a bridge de downlink e aplicar a regra configurada para os pacotes de saída da bridge;

```
iSH> bridge add 1-1-1-3/gpononu gem 701 gtp 1024 downlink vlan 400 tagged epktrule 2
Adding bridge on 1-1-1-3/gpononu
Created bridge-interface-record 1-1-1-701-gponport-400/bridge
```

4. Configurar a bridge de uplink com VLAN 400;

```
iSH> bridge add 1-1-2-0/eth uplink vlan 400 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-400/bridge
Bridge-path added successfully
```

» **Caso 3:** configurar um filtro de policiamento colorizado para limitar a banda através de taxa dupla com ymark

Este exemplo descreve a configuração para a taxa garantida (CIR) a taxa de pico (PIR) a partir do qual os pacotes serão descartados na saída da bridge de downlink. Pacotes entre o CIR e o PIR serão tratados baseado no melhor esforço.

Você pode usar o valor ymark para marcar pacotes que fluem entre o CIR e o PIR para dispositivos de upstream com policiamento com colorização.

> **Observação:** o policiamento colorizado com taxa dupla funciona somente para pacotes de saída em uma bridge

1. Criar a regra de policiamento colorizado com dupla taxa que será aplicada nos pacotes de saída na bridge;

```
iSH> rule add colorawareratelimitdiscard 3/1 rate 1800 peak 3600 ymark 1
Created packet-rule-record 3/1 (colorawareratelimitdiscard)
```

2. Para verificar a regra, use o comando *rule show.* Para visualizar as regras do tipo ratelimitdiscard inserir o comando *rule show* ratelimitdiscard:

```
iSH> rule show
Group/Member              Type Value(s)
     1/1      colorawareratelimitdiscard cir 1300kbps cbs 120000bytes ebs
130000bytes hi 4 lo 0
     2/1      colorawareratelimitdiscard cir 1800kbps cbs 120000bytes pir 3600kbps
ebs 130000bytes hi 4 lo 0
     3/1      colorawareratelimitdiscard cir 1800kbps cbs 120000bytes pir
3600kbps ebs 130000bytes ym 1 hi 4 lo 0
3 record(s) found
```

3. Criar a bridge de downlink e aplicar a regra configura para os pacotes de saída da bridge;

```
iSH> bridge add 1-1-1-3/gpononu gem 701 gtp 1024 downlink vlan 400 tagged epktrule 3
Adding bridge on 1-1-1-3/gpononu
Created bridge-interface-record 1-1-1-701-gponport-400/bridge
```

4. Configurar a bridge de uplink com VLAN 400.

```
iSH> bridge add 1-1-2-0/eth uplink vlan 400 tagged
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-400/bridge
Bridge-path added successfully
```

Valores padrão de cor para CoS

> **Observação:** a Intelbras recomenda a utilização dos valores padrão de cor para CoS

O controle de banda com policiamento colorizado normalmente é utilizado quando múltiplos serviços com diferentes prioridades são oferecidos em uma única VLAN. As cores verde, amarelo e vermelho são usadas para medir o tráfego e as cores correspondem aos valores de CoS, que variam de 0 a 7. Você pode definir quais cores correspondem a qual valor CoS.

O policiamento colorizado baseia-se na ideia de que os dispositivos de upstream policiam e marcam os quadros com base em um conjunto de regras. Um pacote verde deve possuir uma prioridade maior. Um pacote amarelo possui menor prioridade, portanto, se houver um congestionamento na largura de banda, ele deve ser descartado antes de um quadro verde. Um pacote vermelho violou alguma regra e deve ser descartado.

Isso significa que pacotes verdes são atendidos primeiro. Portanto, se houver espaço suficiente, os pacotes amarelos são atendidos. Os pacotes vermelhos sempre são descartados.

A tabela a seguir exibe o mapeamento padrão do valor CoS para a cor correspondente.

Valor CoS	Cor
7	verde
6	verde
5	verde
4	verde
3	amarelo
2	amarelo
1	amarelo
0	amarelo

Valores de CoS e sua cor correspondente

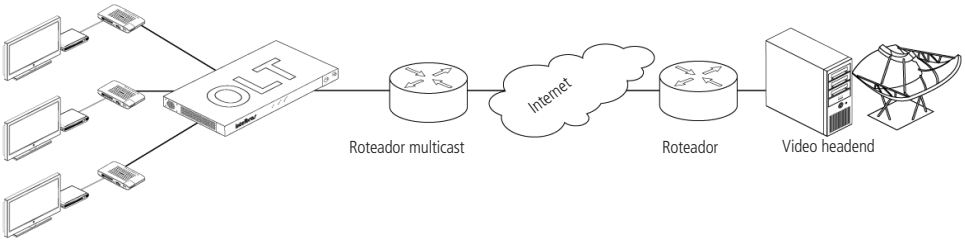
9.10. Tópicos avançados de bridging

Bridges com IGMP

Com IGMP Multicast, em vez de enviar quadros para todos os dispositivos como em uma transmissão broadcast, que pode prejudicar a performance da rede (pois estaria inundando todos os dispositivos da rede com o mesmo fluxo de dados) o fluxo de dados é enviado apenas para os dispositivos que solicitam o serviço.

O comportamento de brinding na OLT 8820 G em relação a tráfegos de vídeos multicast, possibilita que os fluxos sejam agregados em um canal, permitindo que os pacotes de vídeo sejam encaminhados por meio de uma bridge Layer 2 a partir do dispositivo headend para um assinante final. Como resultado, o vídeo trafega do headend, ou da central de controle e é encaminhado pela OLT, em modo passivo, como um único fluxo de stream, reduzindo largura de banda necessária para os pacotes de vídeo chegarem a seus destinos.

A OLT 8820 G suporta IGMPv1, v2, v3, IGMP snooping e IGMP proxy reporting.



Bridge de video com IGMP

O exemplo a seguir descreve uma bridge de vídeo em uma interface uplink e seu bridge-path. A bridge de downlink GPON insere o número de fluxos de vídeo e a lista de controle de multicast.

Para a bridge de uplink, insira:

```
iSH> bridge add 1-1-5-0/eth uplink vlan 777
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record 1-1-5-0-eth-777/bridge
Bridge-path added successfully
```

Para o bridge-path de uplink, adicione um aging time multicast e o intervalo de consultas IGMP.

```
iSH> bridge-path add 1-1-5-0-eth-777/bridge vlan 777 default mcast 90 igmptimer 30
Bridge-path added successfully
```

Adicionar uma lista de controle multicast e designar o máximo de fluxos de vídeo usando o formato m/n. O primeiro parâmetro "m" informa a lista de controle multicast, o segundo parametro "n" informa o fluxo máximo de vídeos.

Ao definir uma lista de controle, todos os endereços configurados serão permitidos e todos os endereços não especificados serão descartados. Ao especificar uma lista de controle de multicast como 0, é permitido todos os endereços multicasts.

```
iSH> new mcast-control-entry 1/1
mcast-control-entry         1/1
Please provide the following:[q]uit.
ip-address: ------------>   {0.0.0.0}: 224.1.1.1
type: ------------------>   {normal}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

```
iSH> bridge add 1-1-1-4/gpononu gem 701 gtp 1 downlink vlan 101 video 1/6
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-4-701-gponport/bridge
```

Remova a configuração de bridging se necessário.

```
iSH> bridge delete 1-1-5-0-eth-777/bridge
Bridge-path deleted successfully
1-1-5-0-eth-777/bridge delete complete
```

```
iSH> bridge delete 1-1-4-701-gponport/bridge
1-1-4-701-gponport/bridge delete complete
```

Verificando definições da bridge

Para verificar definições da bridge, utilize o comando *get bridge-interface-record* para cada bridge desejada. Este comando exibe configurações da bridge, incluindo *learnMulticast* e *forwardToMulticast*.

Bridging de vídeo precisa tanto da bridge uplink como da bridge downlink. Na bridge uplink, a função *forwardToMulticast* esta associada ao local de origem do conteúdo de vídeo, permitindo que a OLT 8820 G receba grupos de vídeo pela rede. Uma interface com este valor definido como true deveria apenas transmitir tráfego multicast para o qual uma solicitação de JOIN foi recebida. Qualquer bridge interface com parâmetro *forwardToMulticast* definido como false descarta tráfego IP multicast. Por padrão, o parâmetro *forwardToMulticast* é definido como true nas bridges de uplink.

Na bridge downlink, a função *learnMulticast* esta associada a interfaces que têm hosts conectados a elas, as quais, permitem a OLT 8820 G enviar grupos de vídeo das interfaces downlink para o core da rede. Por padrão, o parâmetro *learnMulticast* é definido como *true* nas bridges de downlink.

Observe que as operações JOIN entram em uma interface *learnMulticast* associada a uma bridge de downlink e passam por uma interface *forwardToMulticast* associada com uma bridge de uplink.

A tabela a seguir exibe os detalhes dos comportamentos das bridge de vídeo associadas pelas diferentes combinações de configurações dos parâmetros da bridge.

learnMulticast	forwardToMulticast	Comportamento
False	False	A interface descarta todos os pacotes multicast de entrada e não encaminha nenhum dos pacotes.
True	False	A interface encaminha os pacotes de sinalização multicast padrão e os pacotes multicast de controle.
True	False	A interface descarta os pacotes de entrada contendo os grupos multicast e encaminha solicitações contendo grupos.
False	True	A interface encaminha pacotes de controle recebidos na interface para todas as outras interfaces que têm o campo *learnMulticast* definido como *true*.
False	True	A interface encaminha os pacotes contendo os grupos multicast somente para interfaces que enviaram mensagens JOIN para um grupo.

True	True	Memso comportamento de uma interface com o campo *learnMulticast* definido como *false* e o campo *forwardToMulticast* definido como *true*.

Combinações e comportamento de learnMulticast e forwardToMulticast

Para a bridge de uplink, observe que a configuração *forwardToMulticast* é *true* e a configuração *learnMulticast* é *false*.

```
iSH> get bridge-interface-record 1-1-4-701-gponport/bridge
bridge-interface-record     1-1-4-701-gponport/bridge
vpi: ------------------------------------------>         {0}
vci: ------------------------------------------>         {0}
vlanId: ---------------------------------------->         {101}
stripAndInsert: -------------------------------->         {true}
customARP: ------------------------------------->         {false}
filterBroadcast: ------------------------------->         {false}
learnIp: --------------------------------------->         {true}
learnUnicast: ---------------------------------->         {true}
maxUnicast: ------------------------------------>         {5}
learnMulticast: -------------------------------->         {false}
forwardToUnicast: ------------------------------>         {false}
forwardToMulticast: ---------------------------->         {true}
forwardToDefault: ------------------------------>         {true}
bridgeIfCustomDHCP: ---------------------------->         {false}
fIngressPacketRuleGroupIndex: ------------------>         {2}
vlanIdCOS: ------------------------------------->         {0}
outgoingCOSOption: ----------------------------->         {disable}
outgoingCOSValue: ------------------------------>         {0}
s-tagTPID: ------------------------------------->         {0x8100}
s-tagId: --------------------------------------->         {0}
s-tagStripAndInsert: --------------------------->         {true}
s-tagOutgoingCOSOption: ------------------------>         {s-tagdisable}
s-tagIdCOS: ------------------------------------>         {0}
s-tagOutgoingCOSValue: ------------------------->         {0}
mcastControlList: ------------------------------>         {}
maxVideoStreams: ------------------------------->         {0}
isPPPoA: --------------------------------------->         {false}
floodUnknown: ---------------------------------->         {false}
floodMulticast: -------------------------------->         {false}:
bridgeIfEgressPacketRuleGroupIndex: ------------>         {0}:
bridgeIfTableBasedFilter: ---------------------->         {NONE(0)}:
bridgeIfDhcpLearn: ----------------------------->         {NONE(0)}:
mvrVlan: --------------------------------------->         {0}
vlan-xlate-from: ------------------------------->         {0}
slan-xlate-from: ------------------------------->         {0}
```

Para a bridge de downlink, a configuração *forwardToMulticast* é *false* e a configuração *learnMulticast* é *true*.

```
iSH> get bridge-interface-record 1-1-4-701-gponport/bridge
bridge-interface-record     1-1-4-701-gponport/bridge
vpi: ------------------------------------------>         {0}
vci: ------------------------------------------>         {0}
vlanId: ---------------------------------------->         {101}
stripAndInsert: -------------------------------->         {true}
customARP: ------------------------------------->         {false}
filterBroadcast: ------------------------------->         {false}
learnIp: --------------------------------------->         {true}
```

```
learnUnicast: ------------------------------->         {true}
maxUnicast: -------------------------------->         {5}
learnMulticast: ----------------------------->         {true}
forwardToUnicast: --------------------------->         {false}
forwardToMulticast: ------------------------->         {false}
forwardToDefault: --------------------------->         {true}
bridgeIfCustomDHCP: ------------------------->         {false}
bridgeIfIngressPacketRuleGroupIndex: --------->         {2}
vlanIdCOS: ---------------------------------->         {0}
outgoingCOSOption: -------------------------->         {disable}
outgoingCOSValue: --------------------------->         {0}
s-tagTPID: ---------------------------------->         {0x8100}
s-tagId: ------------------------------------>         {0}
s-tagStripAndInsert: ------------------------>         {true}
s-tagOutgoingCOSOption: --------------------->         {s-tagdisable}
s-tagIdCOS: --------------------------------->         {0}
agOutgoingCOSValue: ------------------------->         {0}
mcastControlList: --------------------------->         {}
maxVideoStreams: ---------------------------->         {0}
isPPPoA: ------------------------------------>         {false}
floodUnknown: ------------------------------->         {false}
floodMulticast: ----------------------------->         {false}:
bridgeIfEgressPacketRuleGroupIndex: ---------->         {0}:
bridgeIfTableBasedFilter: ------------------->         {NONE(0):
bridgeIfDhcpLearn: -------------------------->         {NONE(0)}:
mvrVlan: ------------------------------------>         {0}
vlan-xlate-from: ---------------------------->         {0}
slan-xlate-from: ---------------------------->         {0}
```

Além disso, você pode executar um comando *bridge igmp* para determinar se o IGMP está sendo executado no sistema.

```
iSH> bridge igmp
```

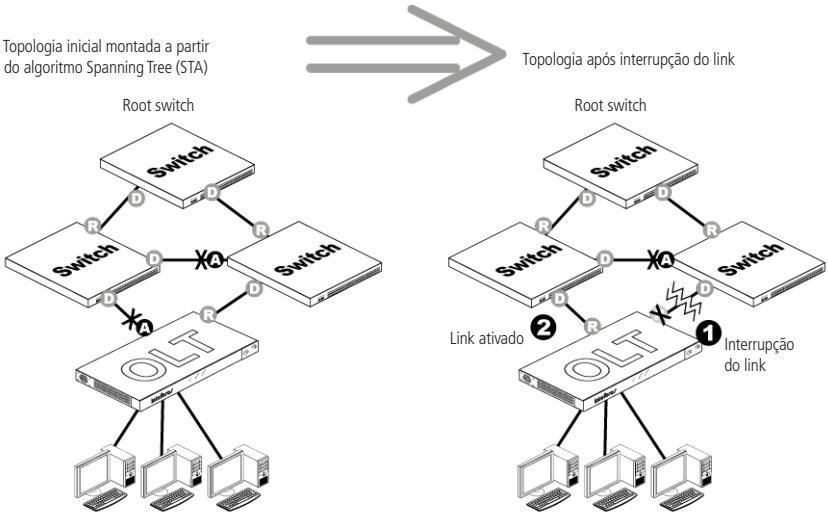
VlanID	MAC Address	MCAST IP	Ifndx	Host MAC	Last Join
999	01:00:5e:02:7f:fe	224.2.127.254	921	00:02:02:0b:4a:a0	2
999	01:00:5e:02:7f:fe	224.2.127.254	922	00:02:02:0a:bb:6d	106
999	01:00:5e:02:7f:fe	224.2.127.254	923	00:02:02:0a:c0:b7	87
999	01:00:5e:02:7f:fe	224.2.127.254	924	00:02:02:0b:4e:c5	172
999	01:00:5e:02:7f:fe	224.2.127.254	925	00:02:02:0b:4c:7e	65
999	01:00:5e:02:7f:fe	224.2.127.254	926	00:02:02:0b:4f:08	46
999	01:00:5e:02:7f:fe	224.2.127.254	927	00:02:02:09:c1:7d	90
999	01:00:5e:02:7f:fe	224.2.127.254	928	00:02:02:0b:44:cd	71
999	01:00:5e:02:7f:fe	224.2.127.254	929	00:02:02:0b:4c:ca	61
999	01:00:5e:02:7f:fe	224.2.127.254	930	00:02:02:0b:47:bd	7
999	01:00:5e:02:7f:fe	224.2.127.254	931	00:02:02:0b:47:c7	177
999	01:00:5e:02:7f:fe	224.2.127.254	932	00:02:02:0b:4d:35	181
999	01:00:5e:02:7f:fe	224.2.127.254	933	00:02:02:0b:4d:5b	144
999	01:00:5e:02:7f:fe	224.2.127.254	934	00:02:02:0b:4a:a5	59
999	01:00:5e:02:7f:fe	224.2.127.254	935	00:02:02:0b:4c:9e	3
999	01:00:5e:02:7f:fe	224.2.127.254	936	00:02:02:09:c1:78	6

999 01:00:5e:02:7f:fe 224.2.127.254 937 00:02:02:0a:c0:ca 131

Rapid Spanning Tree Protocol (RSTP)

O RSTP (802.1W - rapid spanning tree) é uma evolução do STP (802.1d - spanning tree) e assegura que haja somente um caminho lógico entre todos os destinos na camada de enlace de uma rede local, fazendo o bloqueio intencional dos caminhos redundantes que poderiam causar um loop. Uma porta é considerada bloqueada quando o tráfego da rede é impedido de entrar ou deixar aquela porta. Isto não inclui os quadros BPDU (Bridge Protocol Data Unit) que são utilizados pelo STP para impedir loops. BPDU (Bridge Protocol Data Unit) é o quadro de mensagem trocado entre os dispositivos que utilizam a função de sapnning tree.

Na rede em bridge, a Root Bridge é selecionada. O STA envia mensagens - Bridge Protocol Data Units (BPDU) - para determinar o caminho de menor custo à Root Bridge. As funções de porta são determinadas a partir dessa análise.



O STA define a topologia de bridging inicial e os ajustes posteriores

Função da porta RSTP

O STA atribui cinco tipos de função a porta:

» **ROOT:** Root Port

A root port é a porta mais próxima da Bridge Root (também conhecido como Switch Root ou equipamento central). A Bridge Root é o único swtich/bridge na rede que não possui nenhuma root port, pois ela é a bridge central e as root ports são definidas por sua relação com a Bridge Root. A root port receberá a melhor BPDU da Bridge Root em uma bridge.

Na imagem anterior, as root ports são designadas com "R".

Para o STA determinar a root port para um dispositivo, cinco parâmetros prioritários RSTP são comparados na seguinte sequência de prioridade:

1. Root bridge priority
2. Root path cost
3. Designated bridge priority
4. Designated port ID
5. Port priority

Somente uma porta pode ser escolhida como a root port por dispositivo. A porta com o menor valor de parâmetro de prioridade RSTP vence. Se o primeiro parâmetro de prioridade RSTP possui os mesmos valores nas portas, então o sistema irá comparar o próximo parâmetro até definir a root port.

» **DSNT:** designated port

A porta designada é a melhor porta para enviar BPDU do dispositivo RSTP ao dispositivo da rede.

Na imagem anterior, as portas designadas são nomeadas com "D".

» **ALT:** alternate port

A Alternate Port é a porta que pode ser utilizada como backup da Root Port. Esta porta permanece bloqueada pois está recebendo mais BPDUs úteis de outra bridge. A porta alternativa pode ser alterada para uma root port.

Na imagem anterior, as portas alternativas são identificadas com "A" e são exibidas como bloqueadas.

» **BKP:** backup port

A Backup Port é a porta que pode sert utilizada como backup da Designated Port da bridge. Esta porta permanece bloqueada pois está recebendo mais BPDUs úteis a partir da mesma bridge em que está conectada. Uma porta de backup fornece conectividade somente ao mesmo segmento de rede, portanto não pode ser alterada para root port.

» **N/A:** não aplicável.

Isso significa que o RSTP ainda não está em seu estado funcional. Normalmente isso aparecerá após a inicialização do sistema.

Para visualizar a função das porta RSTP, use o comando *bridge show* ou o comando *rstp-bridge show.*

Estado da porta RSTP

O IEEE 802.1w define três estados de porta no RSTP:

» **DIS:** descarte.
» **LRN:** apendizagem (é um estado de transição).
» **FWD:** encaminhamento (é o estado normal de operação).

Para exibir os estados das portas RSTP, use o comando *bridge show*. Para exibir informações RSTP, use o comando *stp-bridge show.*

RSTP em bridges uplink

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1W) é suportados nas interfaces de upstream.

> **Observação:** a interface *1-1-1-0/eth* não pode ser usada para RSTP. Esta interface é destinada somente para a gerencia da OLT

Configurar RSTP em bridges de uplink

O exemplo a seguir configura RSTP em bridges de uplink.

1. Criar bridges de uplink RSTP nas portas de upstream *1-1-4-0/eth* e *1-1-3-0/eth;*

```
iSH> stp-bridge add 1-1-4-0/eth uplink vlan 500
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth-500/bridge
Bridge-path added successfully

iSH> stp-bridge add 1-1-3-0/eth uplink vlan 500
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-500/bridge
Bridge-path added successfully
```

Utilizar *stp-bridge add interface/type uplink vlan x <tagged>* para adicionar uma interface VLAN à interface de upstream.

O bridge-path é automaticamente definido com o parâmetro default.

Mesmo se o parâmetro tagged não for especificado, a bridge de uplink é considerada como tagged por default.

2. Verificar as bridges;

```
iSH> bridge show
      Orig
Type VLAN/SLAN  VLAN/SLAN     Physical        Bridge                    St Table Data
upl             Tagged 500    1/1/3/0/eth     1-1-3-0-eth-500/bridge    DIS STP: ROOT
upl             Tagged 500    1/1/4/0/eth     1-1-4-0-eth-500/bridge    FWD S VLAN 500 default STP: ROOT
2 Bridge Interfaces displayed
```

A porta *1-1-4-0* foi escolhida como root port, o que significa que a porta está ativa, recebendo e encaminhando pacotes. A porta *1-1-3-0* é a porta que está bloqueada e descartando pacotes.

O comando *stp-bridge show* fornece informações das bridges STP.

```
iSH> stp-bridge show
Bridge is running IEEE 802.1W RSTP
Bridge ID has priority 36000, address 00:01:47:27:14:86
Configured: hello=2, forward=15, max_age=20
Current root has priority 32768, address 00:04:96:19:22:f0
Cost of root path 20000
1 bridge(s) present first-> 1-1-3-0-eth-500:
         is a DESIGNATED PORT in DISCARDING state
1 bridge(s) present first-> 1-1-4-0-eth-500:
         is a ROOT PORT in FORWARDING state
Root bridge has priority 32768, address 00:04:96:19:22:f0
Designated bridge has priority 32768, address 00:04:96:19:22:f0
Designated Port id is 16385:144, root path cost is 0
Timers: forward delay is 15, hello time is 2, message age is 0
sync: 0 synced: 0 reRoot: 0 rrWhile: 15 operEdge: 0 fdWhile: 0
learn: 1 forward: 1 agreed: 0 learning: 1 forwarding: 1 updtInfo: 0 selected: 1
```

3. Cinco parâmetros de prioridade serão comparados em sequencia nestas duas portas: Root bridge priority>Root path cost>Designated bridge priority>Designated port ID>Port priority.

   Se os primeiros quatro parâmetros de prioridade RSTP forem o mesmo, o sistema compara para verificar qual porta possui a menor prioridade de porta (Port priority) configurado. A porta com o menor valor será a prioritária.

   A prioridade de porta pode ser exibida utilizando o comando *get stp-bind<profile-storage-key>* e pode ser alterada usando o comando *update stp-bind<profile-storage-key>*.

   Para visualizar perfis *stp-bind* existentes e verificar a prioridade de porta, insira:

```
iSH> list stp-bind
stp-bind 1-1-4-0-eth/linegroup/0
stp-bind 1-1-3-0-eth/linegroup/0
2 entries found.
iSH> get stp-bind 1-1-4-0-eth/linegroup/0
stp-bind 1-1-4-0-eth/linegroup/0
portPriority: ------>       {128}
iSH> get stp-bind 1-1-3-0-eth/linegroup/0
stp-bind 1-1-3-0-eth/linegroup/0
portPriority: ------>       {144}
```

4. Para exibir os parâmetros globais da configuração RSTP, insira o comando *get stp-params 0;*

```
iSH> get stp-params 0
stp-params         0
name: -------------->       {}
revision: ---------->       {0}
```

```
bridgePriority: ---->       {36000}
forceVersion: ------>       {2}
fwdDelay: ---------->       {15}
helloTime: --------->       {2}
migrateTime: ------>        {3}
txHoldCount: ------->       {3}
maxAge: ------------>       {20}
```

5. Para remover uma porta de uma bridge stp;

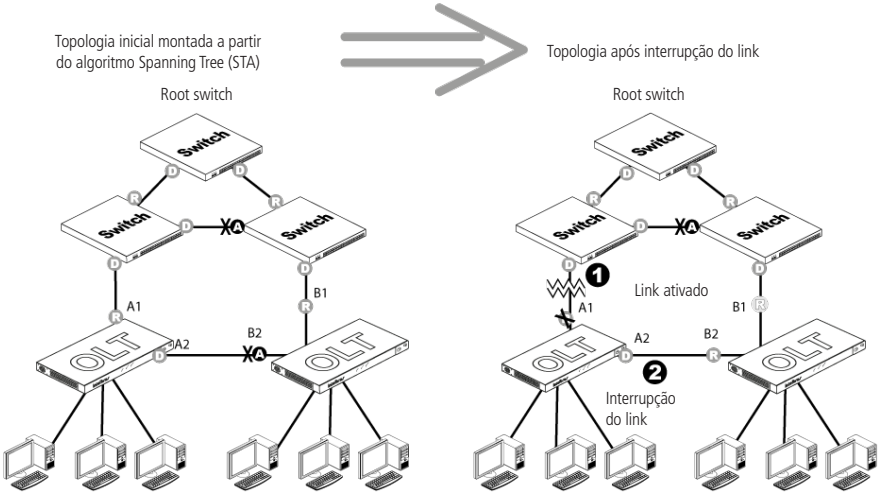
```
iSH> stp-bridge delete 1-1-3-0-eth-500/bridge
Bridge-path deleted successfully
1-1-3-0-eth-500/bridge delete complete iSH>
iSH> stp-bridge delete 1-1-4-0-eth-500/bridge
Bridge-path deleted successfully
1-1-4-0-eth-500/bridge delete complete
```

RSTP em bridges rlink

Com RSTP em bridges rlink em uma configuração de anel, em vez de ter um segundo link redundante em cada dispositivo, o tráfego pode prosseguir através dos outros dispositivos na mesma rede, que possui sua própria bridge de uplink.

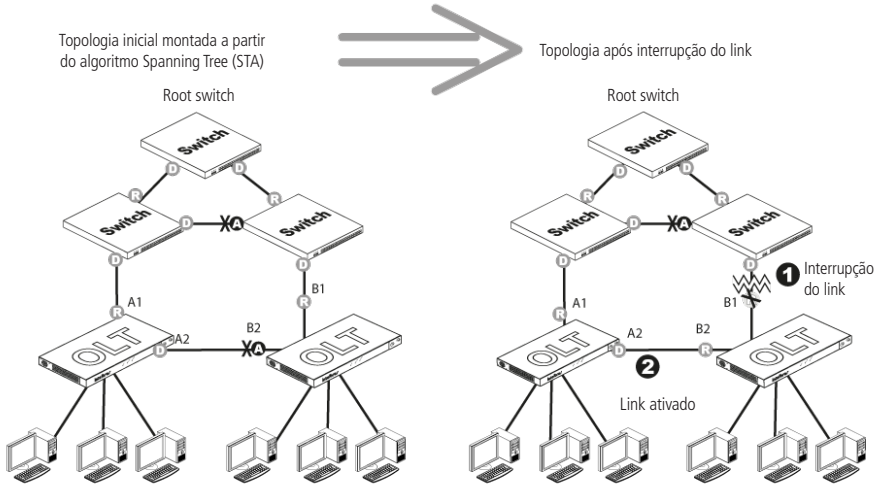
Neste exemplo, há o uso combinado de OLTs em uma rede. Cada OLT possui uma bridge interface com as características de uma bridge uplink em uma porta e uma bridge intralink em outra porta. Com o RSTP rlink habilitado na bridge intralink, a interface designada B2 na OLT será bloqueada. impedindo que o tráfego entre em loop.

O tráfego do root switch que chega na OLT A1 é verificado e caso haja correspondência em sua tabela de encaminhamento será transmitido para o downlink, se não houver correspondência, o pacote será descartado. O tráfego a partir das bridges de downstream das OLTs serão enviados em sentido upstream para o root switch através das respectivas interface A1 e B1.



Topologia de anel RSTP rlink

A imagem anterior também exibe que, se a conexão da OLT ao root switch através da interface A1 ficar indisponível, o protocolo RSTP tirará a porta B2 da outra OLT do estado de bloqueio e a colocará em estado de encaminhamento. O tráfego a partir das bridges de downlink nas OLTs sairão pela interface B1. O tráfego de downstream da OLT que teve sua interface indisponível será encaminhado para a interface B2 através da interface A2 e então, o tráfego será enviado pelo upstream em direção ao root switch através da interface B1.



Rlink RSTP com falha em um link

Nesta outra topologia, após a interface B1 da OLT ficar indisponível fará que todo o tráfego a partir de sua bridge de downlink seja encaminhado para a interface A2 da outra OLT através de sua interface B2, e então, o tráfego será enviado em direção ao root switch através da interface A1 da outra OLT.

Configurar rlinks RSTP

Os procedimentos de configuração para as topologias rlink RSTP estão listados a seguir.

> **Observação:** este exemplo exibe a bridge Rlink RSTP configurada na porta uplink e intralink da OLT. Você também pode configurar a bridge RSTP na porta uplink e configurar uma bridge Rlink RSTP na porta intralink

1. Conforme exibido na imagem anterior, para configurar a bridge rlink RSTP na interface uplink e intralink, realize os seguintes comandos:
   a. Crie a bridge Rlinks RSTP na porta uplink A1 (*1-1-4-0*) e na porta intralink A2 (*1-1-3-0*) com *stp-bridge add interface/type rlink vlan id*.

```
iSH> stp-bridge add 1-1-4-0/eth rlink vlan 500
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth-500/bridge
Bridge-path added successfully
Bridge-path added successfully

iSH> stp-bridge add 1-1-3-0/eth rlink vlan 500
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-500/bridge
Bridge-path added successfully
Bridge-path added successfully
```

Se o parâmetro *vlan id* não for especificado, será gerado um erro, se o parâmetro *tagged* não for especificado, a bridge de rlink assume por padrão a opção *tagged*. Verifique as bridges.

```
iSH> bridge show vlan 500
          Orig
Type VLAN/SLAN  VLAN/SLAN    Physical      Bridge                   St Table Data
rlk             Tagged 500   1/1/3/0/eth   1-1-3-0-eth-500/bridge   BLK
rlk             Tagged 500   1/1/4/0/eth   1-1-4-0-eth-500/bridge   FWD S VLAN 500 STP: ROOT
2 Bridge Interfaces displayed
```

b. Para criar bridges-path para as bridges de rlink, dois comandos *bridge-path add interface/type vlan vlanID* (*intralink* e *default*) podem ser manualmente fornecidos para cada interface rlink.

Embora o bridge-path seja criado automaticamente, você pode fornecer manualmente o bridge-path com variáveis adicionais usando o comando *bridge-path add*.

```
iSH> bridge-path add 1-1-3-0-eth-500/bridge vlan 500 default
Bridge-path added successfully

iSH> bridge-path add 1-1-3-0-eth-500/bridge vlan 500 intralink
Bridge-path added successfully

iSH> bridge-path add 1-1-4-0-eth-500/bridge vlan 500 default
Bridge-path added successfully

iSH> bridge-path add 1-1-4-0-eth-500/bridge vlan 500 intralink
Bridge-path added successfully
```

c. Verifique os bridge-path das bridges.

```
iSH> bridge-path show
VLAN/SLAN    Bridge        Address
500 1-1-4-0-eth-500/bridge   Intralink
500 1-1-4-0-eth-500/bridge   Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
500 1-1-3-0-eth-500/bridge   Intralink
500 1-1-3-0-eth-500/bridge   Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

d. Para verificar as bridges, insira:

```
iSH> bridge show vlan 500
        Orig
Type VLAN/SLAN  VLAN/SLAN  Physical      Bridge                      St Table Data
rlk             Tagged 500 1/1/3/0/eth   1-1-3-0-eth-500/bridge      BLK
rlk             Tagged 500 1/1/4/0/eth   1-1-4-0-eth-500/bridge      FWD S VLAN 500 STP: ROOT
2 Bridge Interfaces displayed
```

A porta A1 (1-1-4-0) foi escolhida como a root port, o que significa que a porta está no estado de encaminhamento. A porta A2 (1-1-3-0) é a porta de intralink e está bloqueada pela topologia Rlink RSTP para evitar loop.

2. Na OLT, para configurar Rlinks RSTP em bridges uplink e bridges intralink, realize os seguintes comandos:

a. Para criar Rlinks RSTP na porta uplink B1 (1-1-4-0) e na porta intralink B2 (1-1-5-0):

```
iSH> stp-bridge add 1-1-4-0/eth rlink vlan 500
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record ethernet4-500/bridge
Bridge-path added successfully
Bridge-path added successfully

iSH> stp-bridge add 1-1-5-0/eth rlink vlan 500
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record ethernet5-500/bridge
Bridge-path added successfully
Bridge-path added successfully
```

b. Verifique os bridge-path.

```
iSH> bridge-path show
VLAN/SLAN    Bridge        Address
500 1-1-4-0-eth-500/bridge    Intralink
500 1-1-4-0-eth-500/bridge    Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
500 1-1-5-0-eth-500/bridge    Intralink
500 1-1-5-0-eth-500/bridge    Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

c. Para exibir as bridges criadas:

```
iSH> bridge show vlan 500
        Orig
Type VLAN/SLAN VLAN/SLAN   Physical        Bridge                    St Table Data
rlk             Tagged 500  1/1/4/0/eth    1-1-4-0-eth-500/bridge    FWD S VLAN 500 STP: ROOT
rlk             Tagged 500  1/1/5/0/eth    1-1-5-0-eth-500/bridge    BLK
2 Bridge Interfaces displayed
```

A porta B1 (1-1-4-0) foi escolhida como a root port, que agora é a porta mais próxima ao root switch. Ela pode receber as melhores BPDUs do root switch. A porta B2 (1-1-5-0) é a porta de intralink que possui a função de porta designada. Ela pode enviar e encaminhar as melhores BPDUs.

3. Se a conexão entre a porta de uplink A1 da OLT 8820 G ao root switch não estiver ativa, a porta de intralink A2 na OLT 8820 G começará a encaminhar tráfego das bridges de downlink à porta de intralink B2 da outra OLT, já que esta OLT se tornou o dispositivo mais próximo do root switch após a alteração da topologia.
   a. Na OLT 8820 G, verifique se a porta de uplink A1(1-1-4-0) está inativa, e se a porta de intralink A2 (1-1-3-0) está no estado de encaminhamento e se assume a função da root port:

```
iSH> bridge show vlan 500
         Orig
Type VLAN/SLAN VLAN/SLAN    Physical      Bridge                  St Table Data
rlk            Tagged 500    1/1/3/0/eth  1-1-3-0-eth-500/bridge FWD S VLAN 500 STP: ROOT BLK
rlk            Tagged 500    1/1/4/0/eth  1-1-4-0-eth-500/bridge BLK
2 Bridge Interfaces displayed
```

4. Se necessário, remova a bridge STP da porta.

   Para remover bridge na OLT , use o comando *stp-bridge delete interface/type.*

```
iSH> stp-bridge delete 1-1-4-0-eth-500/bridge
Bridge-path deleted successfully
1-1-4-0-eth-500/bridge delete complete
```

Multiple Spanning Tree Protocol (MSTP)

Visão geral do MSTP

Multiple Spanning Tree Protocol (MSTP) inclui tanto IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) como IEE 802.1w Rapid Spanning Tree Protocol (RSTP). MSTP configura um processo de spanning tree separada para cada grupo de VLAN. O STP (tradicional) funciona apropriadamente quando há somente um VLAN ID na rede. Se a rede contém mais de uma VLAN, a rede lógica configurada por STP funcionaria, mas é possível fazer uso um melhor dos caminhos alternativos disponíveis utilizando um processo de spanning tree separado para os diferentes grupos de VLAN.

O MSTP executa esta função por região que codifica a informação adicional após a finalização das mensagens BPDU do padrão RSTP, bem como uma série de mensagens MSTI (Multiple Spanning Tree Instances). Cada uma dessas Instancias MST (MSTI) transmite a informação de spanning tree para cada uma das instâncias existentes. Em cada instância pode ser atribuído um número de VLANs e o spanning tree é sempre dentro desta região MST.

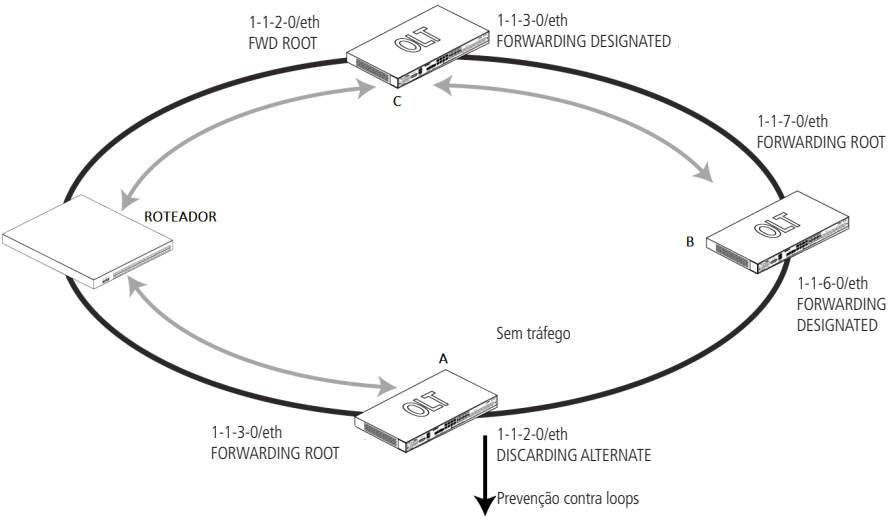
O MSTP fornece vários caminhos de encaminhamento, permitindo que o tráfego deixe o equipamento em qualquer direção do anel.

Operação em anel MSTP

» **Operação normal do anel MSTP**

Esse anel MSTP está formado por três OLTs e um roteador Ethernet.

Para que um anel MSTP deixe o tráfego circular de modo eficiente, um link do loop deve restringir o tráfego devido a uma porta em estado de DISCARDING, ou devido a uma porta em estado BLOCKED.



Exemplo de tráfego normal no anel MSTP

Nó 1: status da OLT 8820 G (A) conforme exibido na imagem anterior.

A bridge MSTP VLAN 100 na porta 1-1-3-0/eth é ROOT e FORWARDING.

A bridge MSTP VLAN 100 na porta 1-1-2-0/eth é DISCARDING e ALTERNATE. O tráfego não pode passar entre uma OLT e outra.

```
iSH> bridge show vlan 100
         Orig
Type VLAN/SLAN VLAN/SLAN  Physical             Bridge                    St
Table Data
-------------------------------------------------------------------------------
tls              Tagged 100  1/1/3/0/eth       1-1-3-0-eth-100/bridge     DIS STP: ALT
tls              Tagged 100  1/1/2/0/eth       1-1-2-0-eth-100/bridge     FWD STP: ROOT
2 Bridge Interfaces displayed
```

Nó 2: status da OLT 8820 G (B).

A bridge MSTP VLAN 100 na porta 1-1-7-0/eth é FORWARDING e ROOT.

A bridge MSTP VLAN 100 na porta 1-1-6-0/eth é FORWARDING e DESIGNATED.

```
iSH> bridge show vlan 100
         Orig
Type VLAN/SLAN  VLAN/SLAN         Physical      Bridge                    St Table Data
-------------------------------------------------------------------------------
tls              Tagged 100       1/1/7/0/eth   1-1-7-0-eth-100/bridge    FWD STP: ROOT
tls              Tagged 100       1/1/6/0/eth   1-1-6-0-eth-100/bridge    FWD STP: DSNT
2 Bridge Interfaces displayed
```

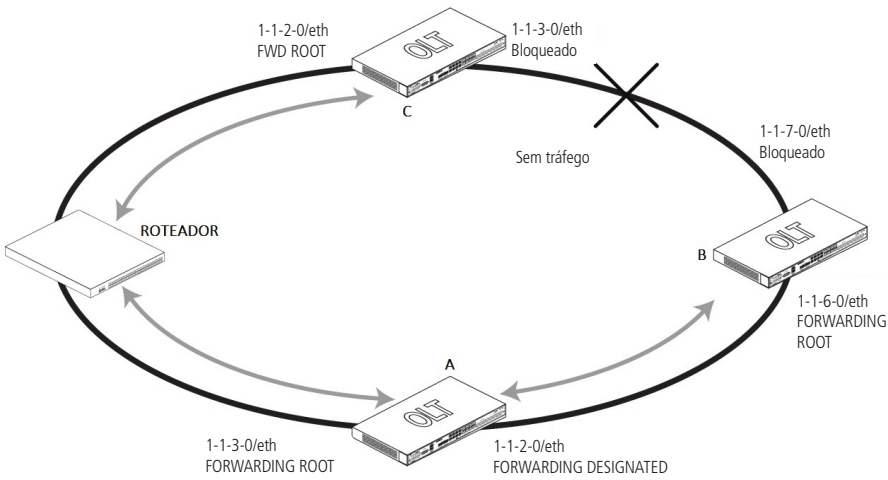
Nó 3: status da OLT 8820 G (C).

A bridge MSTP VLAN 100 na porta 1-1-2-0/eth é FORWARDING e ROOT.

A bridge MSTP VLAN 100 em 1-1-3-0/eth é FORWARDING e DESIGNATED.

```
iSH> bridge show vlan 100
          Orig
Type VLAN/SLAN     VLAN/SLAN         Physical    Bridge                    St Table Data
tls                Tagged 100      1/1/2/0/eth    1-1-2-0-eth-100/bridge   FWD STP: ROOT
tls                Tagged 100      1/1/3/0/eth    1-1-3-0-eth-100/bridge   FWD STP: DSNT
2 Bridge Interfaces displayed
```

Anel MSTP com porta bloqueada na OLT 8820 G (B)



Anel MSTP com porta bloqueada

Nó 1: status da OLT 8820 G (A) conforme exibido na imagem anterior.

Nesse exemplo, quando uma porta na OLT 8820 G (B) fica em down, o status da bridge MSTP VLAN 100 na porta 1-1-2-0/eth muda para FORWARDING DESIGNATED dado que o tráfego está BLOCKED em outro lugar do anel MSTP. O status da bridge MSTP VLAN 100 na porta 1-1-3-0/eth permanece FORWARDING ROOT.

```
iSH> bridge show
          Orig
Type VLAN/SLAN     VLAN/SLAN         Physical       Bridge                    St Table Data
tls                Tagged 100      1/1/3/0/eth    1-1-3-0-eth-100/bridge    FWD STP: ROOT
tls                Tagged 100      1/1/2/0/eth    1-1-2-0-eth-100/bridge    FWD STP: DSNT
2 Bridge Interfaces displayed
```

Nó 2: status da OLT 8820 G (B).

A porta 1-1-7-0/eth fica em down, mudando o status de todos as bridges para BLOCKED. A bridge MSTP VLAN 100 na porta 1-1-6-0/eth muda para FORWARDING ROOT e o tráfego pode circular entre a OLT 8820 G (B) e a OLT 8820 G (A).

```
iSH> bridge show vlan 100
          Orig
Type VLAN/SLAN     VLAN/SLAN         Physical   Bridge                    St
tls                Tagged 100      1/1/7/0/eth   1-1-7-0-eth-100/bridge   BLK A 00:00:00:00:00:00
tls                Tagged 100      1/1/6/0/eth   1-1-6-0-eth-100/bridge   FWD STP: ROOT
2 Bridge Interfaces displayed
```

Nó 3: status da OLT 8820 G (C).

Quando a porta 7 na OLT 8820 G (B) fica em down, a porta 3 na OLT 8820 G (C) também é bloqueada. A bridge MSTP VLAN 100 na porta 1-1-3-0/eth está bloqueada e o tráfego não passa por esse evitando assim o loop. O tráfego passa pelo anel MSTP através da porta 2, e a bridge MSTP VLAN 100 na porta 1-1-2-0/eth permanece no status FORWARD ROOT.

```
iSH> bridge show vlan 100
          Orig
Type VLAN/SLAN    VLAN/SLAN         Physical     Bridge                    St Table Data
tls               Tagged 100    1/1/3/0/eth      1-1-3-0-eth-100/bridge   BLK A 00:00:00:00:00:00
tls               Tagged 100    1/1/2/0/eth      1-1-2-0-eth-100/bridge   FWD STP: ROOT
2 Bridge Interfaces displayed
```

Instâncias MSTP

O MSTI suporta grupos de VLAN. Cada MSTI pode ser configurado com diferentes switches root e diferentes parâmetros STP.

Função da porta MSTP

Há cinco funções de porta atribuídas pelo MSTP:

» **ROOT:** Root port

A root port é determinada pelo switch como o modo mais eficiente de transmitir tráfego no anel MSTP.

Para determinar a root port para um dispositivo, cinco parâmetros de prioridade de MSTP são comparados na sequência de prioridade a seguir:

1. Root bridge priority
2. Root path cost
3. Designated bridge priority
4. Designated port ID
5. Port priority

Apenas uma porta MSTP pode ser escolhida como root port por dispositivo. A porta com o menor valor dos parâmetros de prioridade MSTP vence. Se o primeiro parâmetro de prioridade MSTP tem os mesmos valores nas portas, o sistema comparará o próximo até encontrar a root port.

» **DSNT:** porta designada

Uma porta designada é uma porta com prioridade inferior à da root port.

» **ALT:** porta alternativa

A porta alternativa é uma porta de backup.

» **BKP:** porta de backup

A porta de backup é uma porta que é bloqueada porque está recebendo mais BPDUs úteis da mesma bridge em que está. Uma porta de backup fornece conectividade somente ao mesmo segmento de rede, portanto não pode ser alterada para root port.

» **N/A:** não disponível

Isso significa que o MSTP ainda não está em seu estado funcional. Normalmente isso aparecerá após a inicialização do sistema.

» **MSTR:** mestre

Não suportado em dispositivos Intelbras.

Para visualizar as funções de porta MSTP, use o comando bridge show.

Estado da porta MSTP

O IEEE 802.1w define três estados de porta MSTP:

» **LRN:** aprendizagem (estado de transição quando é executada a configuração inicial de spanning tree). Por exemplo:

```
iSH> bridge show
          Orig
Type VLAN/SLAN      VLAN/SLAN       Physical     Bridge                    St Table Data
rlk                  Tagged 100     1/1/2/0/eth 1-1-2-0-eth-100/bridge LRN STP: ROOT
1 Bridge Interfaces displayed
```

» **FWD:** encaminhamento (estado normal de operação). Por exemplo:

```
iSH> bridge show
          Orig
Type VLAN/SLAN    VLAN/SLAN    Physical     Bridge                     St Table Data
rlk               Tagged 100  1/1/2/0/eth    1-1-2-0-eth-100/bridge     FWD S VLAN 100 Default STP: ROOT
1 Bridge Interfaces displayed
```

» **DIS:** descarte (estado quando o tráfego não é encaminhado para o próximo dispositivo do anel). Por exemplo:

```
iSH> bridge show
          Orig
Type VLAN/SLAN VLAN/SLAN      Physical    Bridge                     St Table Data
rlk             Tagged 100    1/1/2/0/eth    1-1-2-0-eth-100/bridge     FWD S VLAN 100 Default STP: ROOT
rlk             Tagged 100    1/1/3/0/eth    1-1-3-0-eth-100/bridge     DIS STP: ALT
2 Bridge Interfaces displayed
```

Para exibir os estados de porta MSTP, use o comando *bridge show*:

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN    Physical    Bridge                    St Table Data
rlk             Tagged 100  1/1/2/0/eth    1-1-2-0-eth-100/bridge   FWD S VLAN 100 Default STP: ROOT
rlk             Tagged 100  1/1/3/0/eth    1-1-3-0-eth-100/bridge   DIS STP: ALT
2 Bridge Interfaces displayed
```

ou o comando *stp-bridge show*:

```
iSH> stp-bridge show
Bridge is running IEEE 802.1S (MSTP)
-- TreeID 0 --- (numTrees=3)
Bridge ID has priority 36864, address 00:01:47:d9:99:a0
lostCistRoot=0 lostMstiRoot=0 alt2Root[0,0]
Configured: hello=2, forward=15, max_age=20 hops=20
Root port is 0, externalCost=20002 internalCost=20000
1 bridge(s) present:
tree=0(0xea76dd8) is a ROOT PORT in FORWARDING state prtState[]= 0xea76e44
Root bridge has priority 24577, address f8:66:f2:0d:3c:41
Designated bridge has priority 32768, address 2c:36:f8:b3:c2:80
Designated Portid is 32788, externalCost=20002 internalCost=0
1 bridge(s) present:
tree=0(0xea77e00) is a ALTERNATE PORT in DISCARDING state prtState[]= 0xea77e6c
Root bridge has priority 24577, address f8:66:f2:0d:3c:41
Designated bridge has priority 36864, address 00:01:47:22:99:f8
Designated Portid is 128, externalCost=20002 internalCost=40000
```

Se a VLAN em uma porta no estado forwarding fica em down, o sistema altera a porta que estava em estado alternativo para o estado ROOT. Por exemplo, quando a porta 2 na VLAN 100 fica em down, a porta 3 na VLAN 100 se torna a porta forwarding.

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN    Physical       Bridge                    St Table Data
rlk             Tagged 100  1/1/2/0/eth   1-1-2-0-eth-100/bridge   ADN
rlk             Tagged 100  1/1/3/0/eth   1-1-3-0-eth-100/bridge   FWD S VLAN 100 Default STP: ROOT
2 Bridge Interfaces displayed
```

Planejamento da topologia de rede para anel MSTP

Ao implementar o MSTP na OLT 8820 G e quaisquer outros dispositivos no anel MSTP, deve-se projetar cuidadosamente a topologia de rede antes de criar as bridge interface MSTP com o comando *stp-bridge add.*

Componentes da topologia de rede MSTP

Componentes de topologia de rede MSTP

- Perfil stp-params 0.
- Perfil mstp-instance.
- Perfil stp-bind.
- STP bridges.

» **Perfil stp-params 0**

O perfil *stp-params 0* define a região MSTP, a prioridade da bridges e a versão do spanning tree. Existe somente uma configuração de perfil *stp-params 0* para cada dispositivo na topologia de rede.

O perfil *stp-params 0* para cada um dos dispositivos na rede MSTP deve ter a mesma região MSTP, uma definição de prioridade para cada uma das bridges e a mesma versão de sapnning tree, pois cada comando *stp-bridge add* irá referenciar as mesmas definições de parâmetro no arquivo *stp-params 0*.

Típica configuração do perfil *stp-params 0* para MSTP:

```
iSH> get stp-params 0
stp-params          0
name: ----------------->      {Region1}  igual a todos os dispositivos do anel
revision: ------------>      {0}
bridgePriority: ------>      {36864}  deve ser um múltiplo de 4096
forceVersion: -------->      {3}  indicação de uso da versão MSTP
fwdDelay: ------------>      {15}
helloTime: ----------->      {2}
migrateTime: --------->      {3}
txHoldCount: --------->      {3}
maxAge: -------------->      {20}
```

A tabela a seguir define os parâmetros do perfil *stp-params 0*.

Os parâmetros configuráveis pelo usuário no perfil *stp-params 0* são *name, bridgePriority, and forceVersion.*

Parâmetro	Descrição
name	O campo especifica um nome utilizado pela região MSTP. Deve ser igual a todos os nós do anel MSTP.
revision	Esse parâmetro é utilizado somente na versão MSTP. A OLT 8820 G atualmente não suporta revisões de MSTP, por isso o padrão de revision é *0*. Não configurável. Padrão: *0*
bridgePriority	ID de prioridade da bridge. Deve ser múltiplo de 4096. Padrão: *36864*
forceVersion	Versão utilizada no processo de Spanning Tree. 3- MSTP 2- RSTP 0- STP
fwdDelay	Tempo para a porta alterar seu estado durante uma alteração de topologia de rede. Padrão: *15*
helloTime	Intervalo de envio de quadros BPDUs. Atualmente, somente é suportado hello time igual a 2. Padrão: *2*

migrateTime	Valor inicial dos temporizadores mdelayWhile e edgeDelayWhile. 3 é o único valor suportado para esse temporizador. Padrão: *3*
txHoldCount	Quantidade de BPDUs transmitidos por intervalo de helloTime. Padrão: *3*
maxAge	Tempo máximo que o dispositivo ficará aguardando as informações transmitidas pela bridge antes de se reconfigurar. Padrão: *20*

Parâmetros do perfil stp-params 0

» Perfil mstp-instance

O perfil mstp-instance vincula Instância MST a VLAN IDs.

Ao projetar a rede MST, o perfil *mstp-instance* deve conter grupos de VLAN e essas instancias devem ser iguais em todos os dispositivo da rede MST. Isto deve-se pelo fato que uma chave é gerada baseada no nome da região e na instância MSTP. Caso uma dessas informações esteja diferente, a chave criada não será correspondente entre os dispositivos da rede MST.

A tabela a seguir define os parâmetros do perfil *mstp-instance*.

O perfil *mstp-instance* vincula uma instância MSTP a um grupo de VLAN IDs. O sistema utiliza o comando *mstp-instance/ VLAN ID* permitindo que o parâmetro mstpName seja definido.

Parâmetro	Descrição
mstpName	Seqüência de caracteres que define a instância MSTP e o VLAN ID.

Perfil mstp-instance

» Perfil stp-bind

O perfil *stp-bind* é um perfil gerado pelo sistema quando o primeiro comando *stp-bridge add* é inserido em cada porta física.

```
iSH> list stp-bind
stp-bind ethernet2/linegroup/1
stp-bind ethernet3/linegroup/2
2 entries found.

iSH> get stp-bind  ethernet2/linegroup/1
stp-bind ethernet2/linegroup/1
portPriority: --------->     {176}
```

Parâmetro	Descrição
portPriority	Utilizado para especificar a prioridade STP dessa porta.

Perfil stp-bind

» Bridges STP

O comando *stp-bridge add* é utilizado para configurar as bridges interface no anel da rede MSTP.

Configurando o perfil stp-params 0

Deve-se configurar o perfil stp-params 0 exatamente do mesmo modo em cada dispositivo da rede MSTP. Cada comando *stp-bridge add* referencia o perfil *stp-params 0*.

O perfil *stp-params 0* deve estar configurado em cada dispositivo antes de executar o comando *stp-bridge add*.

1. Modifique o parâmetro *name,* configure o campo *bridgePriority* com um múltiplo de 4096, e configure o parâmetro *forceVersion* em 3 para operar na versão MSTP;

```
iSH> update stp-params 0
stp-params         0
Please provide the following: [q]uit.
name: -------------->       {}: Region1
revision: ---------->       {0}:
bridgePriority: ---->       {36000}: 36864
forceVersion: ------>       {2}: 3
fwdDelay: ---------->       {15}:
helloTime: --------->       {2}:
migrateTime: ------->       {3}:
```

```
txHoldCount: ------->       {3}:
maxAge: ------------>       {20}
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

2. Verifique as alterações:

```
iSH> get stp-params 0
stp-params          0
name: -------------->       {Region1}
revision: ---------->       {0}
bridgePriority: ---->       {36864}
forceVersion: ------>       {3}
fwdDelay: ---------->       {15}
helloTime: --------->       {2}
migrateTime: ------->       {3}
txHoldCount: ------->       {3}
maxAge: ------------>       {20}
```

Configurando perfis mstp-instance

Depois de projetar a rede MSTP, crie perfis *mstp-instance* em cada dispositivo da rede MSTP para associar uma instância a grupo de VLAN IDs.

Todos os dispositivos da rede MSTP devem possuir perfis *mstp-instance* iguais, para que o tráfego circule no anel MSTP.

1. Crie todos os perfis *mstp-instance* para a instância 1 no primeiro nó da configuração MSTP. Associe a instância 1 a um VLAN ID;

```
iSH> new mstp-instance 1/111
mstp-instance       1/111
Please provide the following: [q]uit.
mstpName: -------->         {}: 1/111
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

2. Crie todos os perfis *mstp-instance* para a instância 2 no primeiro nó da configuração MSTP. Associe a instância 2 a um VLAN ID;

```
iSH> new mstp-instance 2/122
mstp-instance       2/122
Please provide the following: [q]uit.
mstpName: --------->        {}: 2/122
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Verifique as instâncias e suas VLAN associadas;

```
iSH> list mstp-instance
mstp-instance       1/111
mstp-instance       1/112
mstp-instance       1/113
mstp-instance       1/114
mstp-instance       1/115
mstp-instance       2/121
mstp-instance       2/122
mstp-instance       2/123
mstp-instance       2/124
mstp-instance       2/125
```

```
mstp-instance      1/116
mstp-instance      1/117
mstp-instance      1/119
mstp-instance      1/120
mstp-instance      2/126
mstp-instance      2/127
mstp-instance      2/128
mstp-instance      2/129
mstp-instance      2/130
mstp-instance      1/100
mstp-instance      1/101
mstp-instance      2/999
mstp-instance      1/118
mstp-instance      2/502
24 entries found.
```

Ou para visualizar uma única instância:

```
iSH> get mstp-instance 1/111
mstp-instance      1/111
mstpName: --------->        {1/111}
```

4. Quando tiver criado todas as instâncias em todos os nós da sua rede MSTP, verifique se todas as instâncias estão configuradas da mesma forma em todos os nós da rede MSTP. Uma amostra de configuração do anel MSTP é exibida na tabela a seguir.

Nó 1 no anel MSTP	**Nó 2 no anel MSTP**	**Nó 3 no anel MSTP**
iSH> *list mstp-instance*	iSH> *list mstp-instance*	iSH> *list mstp-instance*
mstp-instance 1/111	mstp-instance 1/111	mstp-instance 1/111
mstp-instance 1/112	mstp-instance 1/112	mstp-instance 1/112
mstp-instance 1/113	mstp-instance 1/113	mstp-instance 1/113
mstp-instance 1/114	mstp-instance 1/114	mstp-instance 1/114
mstp-instance 1/115	mstp-instance 1/115	mstp-instance 1/115
mstp-instance 2/121	mstp-instance 2/121	mstp-instance 2/121
mstp-instance 2/122	mstp-instance 2/122	mstp-instance 2/122
mstp-instance 2/123	mstp-instance 2/123	mstp-instance 2/123
mstp-instance 2/124	mstp-instance 2/124	mstp-instance 2/124
mstp-instance 2/125	mstp-instance 2/125	mstp-instance 2/125
mstp-instance 1/116	mstp-instance 1/116	mstp-instance 1/116
mstp-instance 1/117	mstp-instance 1/117	mstp-instance 1/117
mstp-instance 1/119	mstp-instance 1/119	mstp-instance 1/119
mstp-instance 1/120	mstp-instance 1/120	mstp-instance 1/120
mstp-instance 2/126	mstp-instance 2/126	mstp-instance 2/126
mstp-instance 2/127	mstp-instance 2/127	mstp-instance 2/127
mstp-instance 2/128	mstp-instance 2/128	mstp-instance 2/128
mstp-instance 2/129	mstp-instance 2/129	mstp-instance 2/129
mstp-instance 2/130	mstp-instance 2/130	mstp-instance 2/130
mstp-instance 1/100	mstp-instance 1/100	mstp-instance 1/100
mstp-instance 1/101	mstp-instance 1/101	mstp-instance 1/101
mstp-instance 2/999	mstp-instance 2/999	mstp-instance 2/999
mstp-instance 1/118	mstp-instance 1/118	mstp-instance 1/118
mstp-instance 2/502	mstp-instance 2/502	mstp-instance 2/502
24 registros encontrados	24 registros encontrados	24 registros encontrados

Instâncias MST com seus respectivos grupos de VLAN IDs nos dispositivos do anel MSTP

Removendo um perfil mstp-instance

Quando necessário, pode-se remover as instâncias MSTP.

```
iSH> delete mstp-instance 1/111
mstp-instance 1/111
1 entry found.
Delete mstp-instance 1/111? [y]es, [n]o, [q]uit : yes
mstp-instance      1/111 deleted.
```

Configurando bridges interface MSTP

Em um anel MSTP, uma porta será utilizada para descarte, evitando a circulação do tráfego e consequentemente um loop na rede.

Quando o VLAN ID está relacionado a uma instância, a instância determina o caminho preferencial. No entanto, quando a bridge é configurado na porta Ethernet, todas as instâncias de uma porta devem ser iguais.

Os tipos válidos de bridge para anéis MSTP são *rlink* e *tls.*

1. Configure as bridges para o anel MSTP na primeira porta Ethernet para a instância 1. Cada VLAN nessa porta terá a instância 1 independente de como a VLAN foi vinculada no perfil *mstp-instance;*

O mecanismo para determinar a prioridade das portas MSTP ocorre na primeira vez que a porta e o VLAN ID são configurados durante a configuração da bridge MSTP.

```
iSH> stp-bridge add 1-1-2-0/eth rlink vlan 0 slan 502 stagged instance 1
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-0/bridge
Bridge-path added successfully
Bridge-path added successfully
```

Verifique a bridge e os diferentes status pelos quais uma bridge passa em um anel MSTP.

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN     Physical       Bridge                        St Table Data
rlk             ST    0/502  1/1/2/0/eth    1-1-2-0-eth-0-502/bridge    DIS STP: DSNT
1 Bridge Interfaces displayed

iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN        Physical     Bridge                        St Table Data
rlk              ST    0/502     1/1/2/0/eth 1-1-2-0-eth-0-502/bridge    LRN STP: DSNT
1 Bridge Interfaces displayed

iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN        Physical    Bridge                    St Table Data
rlk             ST    0/502     1/1/2/0/eth 1-1-2-0-eth-0/bridge    FWD S SLAN 502 VLAN 0
1 Bridge Interfaces displayed
```

2. Crie a topologia de bridge restante na primeira porta Ethernet da sua configuração utilizando todos os VLAN ID na configuração MSTP para a instância 1;

```
iSH> stp-bridge add 1-1-2-0/eth rlink vlan 999 tagged instance 1
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-999/bridge
Bridge-path added successfully
Bridge-path added successfully

iSH> stp-bridge add 1-1-2-0/eth tls vlan 100 tagged instance 1
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-100/bridge
Bridge-path added successfully

iSH> stp-bridge add 1-1-2-0/eth tls vlan 101 tagged instance 1
Adding bridge on 1-1-2-0/eth
```

```
Created bridge-interface-record 1-1-2-0-eth-101/bridge
Bridge-path added successfully

iSH> stp-bridge add 1-1-2-0/eth tls vlan 111 tagged instance 1
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-111/bridge
Bridge-path added successfully
```

Continue até que todas as bridges MSTP para a instância 1 estejam configuradas.

Visualize as bridges criados para a instância 1 na porta uplink 1-1-2-0/eth da topologia de rede MSTP.

```
iSH> bridge show 1-1-2-0/eth
                Orig
Type VLAN/SLAN  VLAN/SLAN          Physical      Bridge                   St Table Data
rlk             Tg       0/502     1/1/2/0/eth   1-1-2-0-eth-0/bridge     DIS STP: ALT
tls             Tagged   100       1/1/2/0/eth   1-1-2-0-eth-100/bridge   DIS STP: ALT
tls             Tagged   101       1/1/2/0/eth   1-1-2-0-eth-101/bridge   DIS STP: ALT
tls             Tagged   111       1/1/2/0/eth   1-1-2-0-eth-111/bridge   DIS STP: ALT
tls             Tagged   112       1/1/2/0/eth   1-1-2-0-eth-112/bridge   DIS STP: ALT
tls             Tagged   113       1/1/2/0/eth   1-1-2-0-eth-113/bridge   DIS STP: ALT
tls             Tagged   114       1/1/2/0/eth   1-1-2-0-eth-114/bridge   DIS STP: ALT
tls             Tagged   115       1/1/2/0/eth   1-1-2-0-eth-115/bridge   DIS STP: ALT
tls             Tagged   116       1/1/2/0/eth   1-1-2-0-eth-116/bridge   DIS STP: ALT
tls             Tagged   117       1/1/2/0/eth   1-1-2-0-eth-117/bridge   DIS STP: ALT
tls             Tagged   118       1/1/2/0/eth   1-1-2-0-eth-118/bridge   DIS STP: ALT
tls             Tagged   119       1/1/2/0/eth   1-1-2-0-eth-119/bridge   DIS STP: ALT
tls             Tagged   120       1/1/2/0/eth   1-1-2-0-eth-120/bridge   DIS STP: ALT
tls             Tagged   121       1/1/2/0/eth   1-1-2-0-eth-121/bridge   DIS STP: ALT
tls             Tagged   122       1/1/2/0/eth   1-1-2-0-eth-122/bridge   DIS STP: ALT
tls             Tagged   123       1/1/2/0/eth   1-1-2-0-eth-123/bridge   DIS STP: ALT
tls             Tagged   124       1/1/2/0/eth   1-1-2-0-eth-124/bridge   DIS STP: ALT
tls             Tagged   125       1/1/2/0/eth   1-1-2-0-eth-125/bridge   DIS STP: ALT
tls             Tagged   126       1/1/2/0/eth   1-1-2-0-eth-126/bridge   DIS STP: ALT
tls             Tagged   127       1/1/2/0/eth   1-1-2-0-eth-127/bridge   DIS STP: ALT
tls             Tagged   128       1/1/2/0/eth   1-1-2-0-eth-128/bridge   DIS STP: ALT
tls             Tagged   129       1/1/2/0/eth   1-1-2-0-eth-129/bridge   DIS STP: ALT
tls             Tagged   130       1/1/2/0/eth   1-1-2-0-eth-130/bridge   DIS STP: ALT
rlk             Tagged   999       1/1/2/0/eth   1-1-2-0-eth-999/bridge   DIS STP: ALT
24 Bridge Interfaces displayed
```

3. Crie a topologia de bridge restante na segunda porta Ethernet da sua configuração utilizando todos os VLAN ID da configuração MSTP para a instância 2;

```
iSH> stp-bridge add 1-1-3-0/eth rlink vlan 999 tagged instance 2
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-999/bridge
Bridge-path added successfully
Bridge-path added successfully

iSH> stp-bridge add 1-1-3-0/eth tls vlan 100 tagged instance 2
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-100/bridge
Bridge-path added successfully

iSH> stp-bridge add 1-1-3-0/eth tls vlan 101 tagged instance 2
Adding bridge on 1-1-3-0/eth
```

```
Created bridge-interface-record 1-1-3-0-eth-101/bridge
Bridge-path added successfully

iSH> stp-bridge add 1-1-3-0/eth tls vlan 111 tagged instance 2
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-111/bridge
Bridge-path added successfully
```

4. Visualize as bridges criadas para a instância 2 na porta uplink *1-1-3-0/eth* da topologia de rede MSTP;

```
iSH> bridge show 1-1-3-0/eth
     Orig
Type VLAN/SLAN VLAN/SLAN       Physical     Bridge                        St Table Data
rlk            ST      0/502   1/1/3/0/eth  1-1-3-0-eth-0-502/bridge  FWD S SLAN 502 VLAN 0
default STP: ROOT
tls            Tagged    100   1/1/3/0/eth  1-1-3-0-eth-100/bridge    FWD STP: ROOT
tls            Tagged    101   1/1/3/0/eth  1-1-3-0-eth-101/bridge    FWD STP: ROOT
tls            Tagged    111   1/1/3/0/eth  1-1-3-0-eth-111/bridge    FWD STP: ROOT
tls            Tagged    112   1/1/3/0/eth  1-1-3-0-eth-112/bridge    FWD STP: ROOT
tls            Tagged    113   1/1/3/0/eth  1-1-3-0-eth-113/bridge    FWD STP: ROOT
tls            Tagged    114   1/1/3/0/eth  1-1-3-0-eth-114/bridge    FWD STP: ROOT
tls            Tagged    115   1/1/3/0/eth  1-1-3-0-eth-115/bridge    FWD STP: ROOT
tls            Tagged    116   1/1/3/0/eth  1-1-3-0-eth-116/bridge    FWD STP: ROOT
tls            Tagged    117   1/1/3/0/eth  1-1-3-0-eth-117/bridge    FWD STP: ROOT
tls            Tagged    118   1/1/3/0/eth  1-1-3-0-eth-118/bridge    FWD STP: ROOT
tls            Tagged    119   1/1/3/0/eth  1-1-3-0-eth-119/bridge    FWD STP: ROOT
tls            Tagged    120   1/1/3/0/eth  1-1-3-0-eth-120/bridge    FWD STP: ROOT
tls            Tagged    121   1/1/3/0/eth  1-1-3-0-eth-121/bridge    FWD STP: ROOT
tls            Tagged    122   1/1/3/0/eth  1-1-3-0-eth-122/bridge    FWD STP: ROOT
tls            Tagged    123   1/1/3/0/eth  1-1-3-0-eth-123/bridge    FWD STP: ROOT
tls            Tagged    124   1/1/3/0/eth  1-1-3-0-eth-124/bridge    FWD STP: ROOT
tls            Tagged    125   1/1/3/0/eth  1-1-3-0-eth-125/bridge    FWD STP: ROOT
tls            Tagged    126   1/1/3/0/eth  1-1-3-0-eth-126/bridge    FWD STP: ROOT
tls            Tagged    127   1/1/3/0/eth  1-1-3-0-eth-127/bridge    FWD STP: ROOT
tls            Tagged    128   1/1/3/0/eth  1-1-3-0-eth-128/bridge    FWD STP: ROOT
tls            Tagged    129   1/1/3/0/eth  1-1-3-0-eth-129/bridge    FWD STP: ROOT
tls            Tagged    130   1/1/3/0/eth  1-1-3-0-eth-130/bridge    FWD STP: ROOT
rlk            Tagged    999   1/1/3/0/eth  1-1-3-0-eth-999/bridge    FWD S VLAN 999 de-
                                                                       fault
STP: ROOT
24 Bridge Interfaces displayed
```

5. Configure cada nó no anel MSTP com a mesma VLAN e configurações das instâncias 1 e 2.

As configurações de bridge para a instância 1 e 2 devem ser iguais. No entanto, as interfaces físicas (número da porta) dos dispositivo não precisam ser iguais entre os dispositivos.

9.11. Configurações de bridging na OLT 8820 G

Configurar bridge uplink (tagged e untagged)

É possível configurar as bridges de uplink como tagged ou untagged.

Quando o dispositivo de upstream não espera ou não reconhece VLAN IDs a bridge uplink deve ser configurada como *untagged*. O modo *untagged* modifica o perfil *bridge-interface-record* colocando o parâmetro stripAndInsert como *true*, fazendo com que a VLAN ID seja removida do pacote ethernet quando estiver indo em direção do dispositivo upstream.

O modo *tagged* modifica o perfil *bridge-interface-record* colocando os parâmetros stripAndInsert como *false* e vlanID com o valor da VLAN ID inserida no comando *bridge add*, fazendo com que a VLAN ID seja mantida no pacote ethernet quando estiver indo em direção do dispositivo upstream. Por padrão, quando omitido o modo (tagged ou untagged) no comando *bridge add* durante a criação da bridge uplink é assumido a opção *tagged*.

> **Observação:** recomenda-se não mudar as configurações padrão da bridge, exceto quando é necessária alguma configuração avançada para a bridge

Criando uma bridge uplink

Crie uma bridge de uplink na interface uplink.

1. Crie a bridge de uplink e depois verifique a bridge;

```
iSH> bridge add 1-1-2-0/eth uplink vlan 555
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-555/bridge
Bridge-path added successfully

iSH> bridge show
        Orig
Type    VLAN/  VLAN/SLAN       Physical   Bridge                St Table Data
SLAN
upl            Tagged 555       1/1/2/0/ 1-1-2-0-eth-555/      DWN S VLAN 555 default
               eth                       bridge
1 Bridge Interfaces displayed
```

2. Visualize o parâmetro *stripAndInsert* no perfil *bridge-interface-record* da bridge de uplink.

```
iSH> get bridge-interface-record 1-1-2-0-eth-555/bridge
bridge-interface-record     1-1-2-0-eth-555/bridge
vpi: ------------------------------->         {0}
vci: ------------------------------->         {0}
vlanId: ---------------------------->         {555}
stripAndInsert: -------------------->         {false}
```

A criação dessa bridge de uplink com o comando bridge add insere 555 no parâmetro *vlanId* e coloca o parâmetro *stripAndInsert* em *false* no perfil *bridge-interface-record*.

Configurar bridge downlink (tagged e untagged)

Também é possível configurar as bridges de downlink utilizando as opções tagged ou untagged. Sua utilização depende da configuração do dispositivo de downstream.

> **Observação:** deve-se configurar a bridge de downlink como tagged SEMPRE que a bridge configurada esteja utilizando uma interface GPON, ou seja, quando estiver configurando alguma ONU Intelbras

Bridge de downlink untagged na interface Ethernet

É possível configurar bridges de downlink como untagged quando o dispositivo de downstream não espera ou não reconhece VLAN IDs. O modo untagged modifica o *perfil bridge-interface-record* colocando os parâmetros *stripAndInsert* como *true* e vlanID com o valor da VLAN ID inserida no comando, fazendo com que a VLAN ID seja removida do pacote ethernet quando estiver indo em direção do dispositivo downstream. Quando um pacote retorna da interface upstream, o VLAN ID é incluído novamente no pacote Ethernet.

Por padrão, quando omitido o modo (tagged ou untagged) no comando *bridge add* durante a criação da bridge downlink é assumido a opção *untagged*.

```
iSH> bridge add 1-1-10-0/eth downlink vlan 55 untagged
Adding bridge on 1-1-10-0/eth
Created bridge-interface-record 1-1-10-0-eth/bridge
```

Bridge de downlink tagged na interface GPON

É possível configurar bridges de downlink como tagged quando o dispositivo de downstream espera e reconhece VLAN IDs. O modo tagged modifica o perfil *bridge-interface-record* colocando os parâmetros *stripAndInsert* como *false* e vlanID com o valor da VLAN ID inserida no comando, fazendo com que a VLAN ID seja mantida no pacote ethernet durante a circulação em direção ao upstream.

Ao configurar uma bridge de downlink utilizando a interface GPON, ou seja, estiver associando uma ONU a uma bridge de downlink, DEVE-SE utilizar a opção *tagged*.

Configurando bridge de downlink tagged

1. Crie uma bridge de downlink *tagged* com um VLAN ID;

```
iSH> bridge add 1-1-1-4/gpononu gem 510 gtp 1 downlink vlan 555 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-555/bridge
```

2. Para exibir a bridge de downlink, insira *bridge show;*

```
iSH> bridge show
        Orig
Type VLAN/SLAN   VLAN/SLAN    Physical          Bridge                          St Table Data
dwn              Tagged 555   1/1/1/4/gpononu   1-1-1-257-gponport-555/bridge   DWN
1 Bridge Interfaces displayed
```

3. Visualize o parâmetro *stripAndInsert* de *bridge-interface-record*.

```
iSH> get bridge-interface-record 1-1-1-257-gponport-555/bridge
bridge-interface-record     1-1-1-257-gponport-555/bridge
vpi: ---------------------------------->        {0}
vci: ---------------------------------->        {0}
vlanId: ------------------------------->        {555}
stripAndInsert: ------------------> {false}
...
```

O parâmetro vlanId é colocado em 555. Dado que a bridge de downlink é *tagged*, o parâmetro stripAndInsert é colocado em *false* indicando que o VLAN ID não será removido do pacote Ethernet, permanecendo intacto em ambas as direções.

Remoção de bridges de uplink e downlink

» **Removendo uma bridge de uplink**

Para remover uma bride de uplink, deve-se utilizar o comando *bridge delete nome_bridge*. O nome da bridge é visualizado através do comando *bridge show.*

```
iSH> bridge delete 1-1-10-0-eth/bridge
1-1-10-0-eth/bridge delete complete
```

» **Removendo uma bridge de downlink**

Para remover uma bride de downlink, deve-se utilizar o comando *bridge delete nome_bridge.* O nome da bridge é visualizado através do comando *bridge show.*

```
iSH> bridge delete 1-1-1-257-gponport-555/bridge
1-1-1-257-gponport-555/bridge delete complete
```

Configuração de bridges Q-in-Q (VLAN ID e SLAN ID)

O padrão IEEE 802.1Q-in-Q expande o espaço no quadro Ethernet para suportar a marcação de pacotes previamente marcados. Esta segunda tag (SLAN) cria um quadro Ethernet "double-tag". Em configurações "double-tagged" ou "stagged", existirá uma *VLAN ID* e um *SLAN ID.*

Quando uma bridge interface com ambas marcações (VLAN ID e SLAN ID) é configurada como *tagged*, a VLAN ID não é removida ou inserida, já o SLAN ID é removido e inserido do frame ethernet, isto significa que o VLAN ID é transmitido sem qualquer alteração, mas o SLAN ID é removido durante o tráfego de saída e inserido no tráfego de entrada.

Quando uma bridge interface com ambas marcações (VLAN ID e SLAN ID) é configurada como *stagged*, ambas (VLAN ID e SLAN ID) não são removidas ou inseridas do frame ethernet, isto significa que a VLAN ID e SLAN ID permanecem no frame ethernet sem nenhuma alteração e em qualquer sentido de tráfego (entrada ou saída).

A OLT 8820 G também suporta a configuração de valores CoS nos cabeçalhos ethernet SLAN. Esse serviço possibilita atribuir um nível de serviço ou classe de serviço (CoS) a um quadro Ethernet SLAN transportado por uma bridge s-tagged uplink, intralink ou downlink. O nível CoS configurado especifica a prioridade do pacote e os métodos de solicitação utilizados para transportar o pacote pela rede Ethernet. A OLT determina e preserva as configurações de CoS para garantir que essas configurações sejam repassadas a outros dispositivos Ethernet na rede para processamento do QoS.

Configurações de bridging Q-in-Q

A OLT 8820 G suporta dois modos de configuração de bridging Q-in-Q. A primeira utiliza a variável *stagged* e a segunda utiliza a variável *tagged*.

Algumas configurações de bridging necessitam de uma bridge de uplink *stagged* para uma bridge de downlink *stagged* ou de uma bridge de uplink *stagged* para uma bridge de downlink *tagged*.

> **Observação:** a OLT 8820 G suporta apenas a variável stagged durante a configuração da bridge interface de uplink

Bridge uplink stagged e bridge downlink stagged (stagged para stagged)

Nesse caso, a designação da bridge de downlink como stagged coloca o parâmetro SLAN ID *s-tagstripAndInsert* em false e o parâmetro VLAN ID *stripAndInsert* em *false* no perfil *bridge-interface-record*. Com esta configuração tanto o SLAN ID quanto VLAN ID não são removidos do quadro ethernet. A informação de VLAN ID e SLAN ID permanece inalterada nos dois sentidos do tráfego.

Esse tipo de configuração possibilita que um dispositivo de downstream como uma ONU receba tanto a VLAN ID quanto a SLAN ID.

Configurando bridge de uplink stagged e bridge de downlink stagged

1. Crie uma bridge *uplink QinQ stagged* com VLAN ID and SLAN ID;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 102 slan 502 stagged
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record 1-1-5-0-eth-102-502/bridge
Bridge-path added successfully
```

Ao designar a variável stagged tanto o VLAN ID e o SLAN ID são repassados para o dispositivo de upstream.

2. Crie uma bridge de downlink *QinQ stagged* com o mesmo VLAN ID e SLAN ID da bridge de uplink;

```
iSH> bridge add 1-1-1-4/gpononu downlink vlan 102 slan 502 stagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-102-502/bridge
```

Ao designar a variável *stagged* tanto o VLAN ID e o SLAN ID são repassados para o dispositivo de downstream e permanecem inalterados em ambos os sentidos do tráfego.

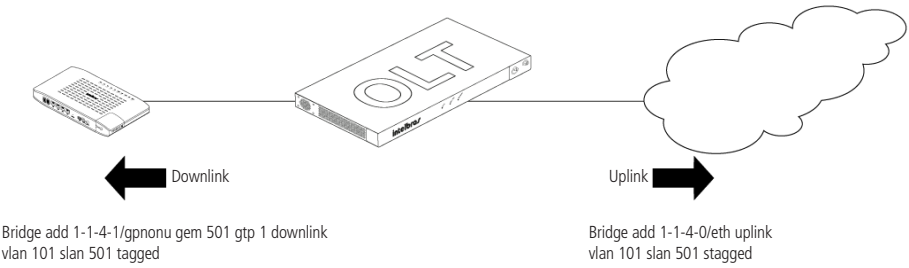
3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN  Physical          Bridge                        St Table Data
dwn             ST 102/502 1/1/1/4/gpononu   1-1-1-257-eth-102-502/bridge  UP
up              ST 102/502 1/1/5/0/eth       1-1-5-0-eth-102-502/bridge    DWN
2 Bridge Interfaces displayed
```

Bridge uplink stagged e bridge downlink tagged (stagged para tagged)

Nesse caso, a designação da bridge de downlink como tagged coloca o parâmetro SLAN ID *s-tagstripAndInsert* em *true* e o parâmetro VLAN ID *stripAndInsert* em *false* no perfil *bridge-interface-record*. Com esta configuração apenas o SLAN ID é removido do quadro ethernet durante o envio do pacote ao dispositivo de downstream, e no retorno o SLAN ID é inserida novamente ao quadro ethernet para seu encaminhamento para o upstream. A VLAN ID permanece inalterada nos dois sentidos do tráfego.

Esse tipo de configuração possibilita que um dispositivo de downstream como uma ONU receba a VLAN ID e não a SLAN ID.



Exemplo de uplink stagged e downlink tagged

Configurando bridge de uplink stagged e bridge de downlink tagged

1. Crie uma bridge uplink QinQ stagged com VLAN ID and SLAN ID;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 102 slan 502 stagged
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record 1-1-5-0-eth-102-502/bridge
Bridge-path added successfully
```

Ao designar a variável stagged tanto o VLAN ID e o SLAN ID são repassados para o dispositivo de upstream.

2. Crie uma bridge de downlink QinQ tagged com o mesmo VLAN ID e SLAN ID da bridge de uplink;

```
iSH> bridge add 1-1-1-4/gpononu downlink vlan 102 slan 502 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-102/bridge
```

Ao designar a variável tagged apenas o VLAN ID é repassado para o dispositivo de downstream já o SLAN ID é removido. Na volta do pacote o SLAN ID é novamente inserido no quadro ethernet e encaminhado para a bridge de uplink.

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN   Physical          Bridge                        St Table Data
dwn             Tg 102/502  1/1/1/4/gpononu   1-1-1-257-eth-102/bridge      UP
up              ST 102/502  1/1/5/0/eth       1-1-5-0-eth-102-502/bridge    DWN
2 Bridge Interfaces displayed
```

Remoção de bridges QinQ de uplink e downlink

» **Removendo uma bridge QinQ de uplink**

Para remover uma bride QinQ de uplink, deve-se utilizar o comando *bridge delete nome_bridge*. O nome da bridge é visualizado através do comando *bridge show.*

```
iSH> bridge delete 1-1-5-0-eth-102-502/bridge
Bridge-path deleted successfully
1-1-5-0-eth-102-502/bridge delete complete
```

» **Removendo uma bridge QinQ de downlink**

Para remover uma bride de downlink QinQ, deve-se utilizar o comando *bridge delete nome_bridge*. O nome da bridge é visualizado através do comando *bridge show.*

```
iSH> bridge delete 1-1-1-257-gponport-102-502/bridge
1-1-1-257-gponport-102-502/bridge delete complete
```

Bridges usando VLAN 0

Na OLT 8820 G, a VLAN 0 funciona como um coringa que reconhecerá todas as VLAN ID, mas somente pode ser utilizado em conjunto com uma SLAN ID. É possível designar VLAN 0 em bridges intralink, TLS, uplink e downlink.

Comportamentos de bridging com VLAN 0

Cada um dos exemplos de configuração de bridging a seguir assume uma configuração uplink com VLAN 0 SLAN X stagged:

» Bridge uplink *stagged* e a bridge downlink VLAN x e SLAN x *stagged.*

» Bridge uplink *stagged* e a bridge downlink VLAN x e SLAN x *tagged.*

» Bridge uplink *stagged* e a bridge downlink VLAN 0 e SLAN x *stagged.*

Configurando bridge de uplink stagged (VLAN 0 e SLAN X) e bridge de downlink stagged (VLAN X e SLAN X)

1. Crie uma bridge uplink QinQ *stagged* com VLAN ID 0 e SLAN ID 501;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 0 slan 501 stagged
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record 1-1-5-0-eth-0-501/bridge
Bridge-path added successfully
```

2. Crie uma bridge de downlink QinQ *stagged* com VLAN ID 100 e SLAN ID 501;

```
iSH> bridge add 1-1-1-4/gpononu downlink vlan 100 slan 501 stagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-100-501/bridge
```

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN    Physical         Bridge                          St Table Data
dwn             ST 100/501   1/1/1/4/gpononu 1-1-1-257-eth-100-501/bridge UP
up              ST   0/501  1/1/5/0/eth      1-1-5-0-eth-0-501/bridge     DWN
2 Bridge Interfaces displayed
```

Configurando bridge de uplink stagged (VLAN 0 e SLAN X) e bridge de downlink tagged (VLAN X e SLAN X)

1. Crie uma bridge uplink QinQ *stagged* com VLAN ID 0 e SLAN ID 501;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 0 slan 501 stagged
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record 1-1-5-0-eth-0-501/bridge
Bridge-path added successfully
```

2. Crie uma bridge de downlink QinQ *tagged* com VLAN ID 200 e SLAN ID 501;

```
iSH> bridge add 1-1-1-4/gpononu downlink vlan 200 slan 501 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-200/bridge
```

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN   Physical         Bridge                       St Table Data
dwn             Tg 200/501  1/1/1/4/gpononu 1-1-1-257-eth-200/bridge  UP
up              ST   0/501  1/1/5/0/eth      1-1-5-0-eth-0-501/bridge  DWN
2 Bridge Interfaces displayed
```

Configurando bridge de uplink stagged (VLAN 0 e SLAN X) e bridge de downlink tagged (VLAN 0 e SLAN X)

1. Crie uma bridge uplink QinQ *stagged* com VLAN ID 0 e SLAN ID 501;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 0 slan 101 stagged
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record 1-1-5-0-eth-0-101/bridge
Bridge-path added successfully
```

Todos as VLAN IDs serão repassadas para o upstream na SLAN 501.

2. Crie uma bridge de downlink QinQ *stagged* com VLAN ID 0 e SLAN ID 501;

```
iSH> bridge add 1-1-1-4/gpononu downlink vlan 0 slan 501 stagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-0-501/bridge
```

Todos as VLAN IDs serão repassadas para o downstream na SLAN 501.

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN   VLAN/SLAN  Physical         Bridge                          St Table Data
dwn              ST   0/501  1/1/1/4/gpononu 1-1-1-257-eth-0-501/bridge   UP
up               ST    0/501  1/1/5/0/eth     1-1-5-0-eth-0-501/bridge     DWN
2 Bridge Interfaces displayed
```

Configurando bridges TLS com VLAN 0 para conexões multiponto

Em configurações de bridging onde são necessárias conexões multiponto, é possível configurar bridges TLS com VLAN 0 para um mesmo SLAN ID. Uma conexão multiponto é um conjunto de duas ou mais conexões para um mesmo SLAN ID (interface que está voltada ao assinante). A bridge TLS voltada ao assinante deve ser configurada como tagged, fazendo com que a SLAN ID do quadro ethernet seja removida durante o envio do pacote ao assinante, no retorno do pacote, a OLT insere a SLAN ID para o encaminhamento do pacote ao uplink. A bridge TLS voltada para o core da rede deve ser stagged, mantendo sempre as marcações de VLAN ID e SLAN ID em ambos os sentido do tráfego.

Configurando bridge TLS para uma conexão multiponto

Primeiro, crie a bridge TLS com VLAN 0 e SLAN ID na porta Ethernet para o tráfego no sentido upstream, depois crie as bridges TLS na porta GPON no sentido downstream (ao assinte) com a mesma SLAN ID.

1. Crie a bridge TLS *stagged* em uma porta Ethernet;

```
iSH> bridge add 1-1-10-0/eth tls vlan 0 slan 200 stagged
Adding bridge on 1-1-10-0/eth
Created bridge-interface-record 1-1-10-0-eth-0-200/bridge
```

2. Crie as bridges TLS *tagged* para os assinantes GPON;

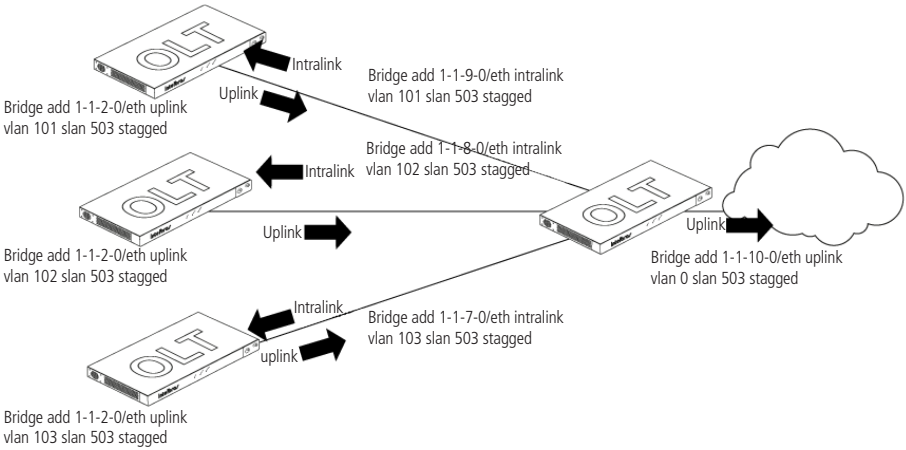
```
iSH> bridge add 1-1-1-35/gpononu tls vlan 0 slan 200 tagged
Adding bridge on 1-1-1-35/gpononu
Created bridge-interface-record 1-1-1-257-gponport-0/bridge

iSH> bridge add 1-1-1-25/gpononu tls vlan 0 slan 200 tagged
Adding bridge on 1-1-1-25/gpononu
Created bridge-interface-record 1-1-1-258-gponport-0/bridge

iSH> bridge add 1-1-1-20/gpononu tls vlan 0 slan 200 tagged
Adding bridge on 1-1-1-20/gpononu
Created bridge-interface-record 1-1-1-259-gponport-0/bridge
```

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN   VLAN/SLAN  Physical            Bridge                          St Table Data
tls              Tg 0/200    1/1/1/20/gpononu    1-1-1-259-gponport-0/bridge     UP
tls              Tg 0/200    1/1/1/25/gpononu    1-1-1-258-gponport-0/bridge     UP
tls              Tg 0/200    1/1/1/35/gpononu    1-1-1-257-gponport-0/bridge     UP
tls              ST 0/200    1/1/10/0/eth        1-1-10-0-eth-0-200/bridge       UP
4 Bridge Interfaces displayed
```

Configurando bridges intralink tagged com VLAN 0

Conforme exibido na imagem a seguir, ao conectar várias OLTs a uma única OLT, é possível definí-las com diferentes VLAN IDs porém todas com o mesmo SLAN ID. Neste caso, a VLAN ID 0 na bridge uplink aceitará todas as VLAN IDs que estejam dentro da SLAN ID pré-determinada. Desta forma é possível configurar uma bridge de uplink que reconhecerá cada VLAN ID e SLAN ID das OLTs.



Bridge uplink stagged com VLAN 0

Configurando bridge intralink (stagged para tagged)

As bridges intralink são tagged, definindo o parâmetro *stripAndInsert* em *false* para a VLAN ID e o parâmetro *s-tagStripAndInsert* para *true* para a SLAN ID. Este comportamento faz com que apenas a SLAN ID seja removida do quadro ethernet quando trafega no sentido de dowstream (ao assinante), no retorno do quadro (sentido upstream) a SLAN ID é inserida pela OLT. A VLAN ID do quadro ethernet não sofre alterações e é transmitida em ambas as direções.

A bridge de uplink é *stagged,* que define os parâmetros *stripAndInsert* e *s-tagStripAndInsert* como *false*. Esse comportamento faz com que tanto a VLAN ID e SLAN ID sejam transmitidos para o dispositivo de upstream.

1. Crie a bridge uplink *stagged* utilizando a VLAN 0;

```
iSH> bridge add 1-1-10-0/eth uplink vlan 0 slan 503 stagged
Adding bridge on 1-1-10-0/eth
Created bridge-interface-record 1-1-10-0-eth-0-503/bridge
Bridge-path added successfully
```

2. Crie as bridges intralinks *tagged* para as OLTs conectadas a OLT principal;

```
iSH> bridge add 1-1-7-0/eth intralink vlan 101 slan 503 tagged
Adding bridge on 1-1-7-0/eth
Created bridge-interface-record 1-1-7-0-eth-101/bridge
Bridge-path added successfully

iSH> bridge add 1-1-8-0/eth intralink vlan 102 slan 503 tagged
Adding bridge on 1-1-8-0/eth
Created bridge-interface-record 1-1-8-0-eth-102/bridge
Bridge-path added successfully

iSH> bridge add 1-1-9-0/eth intralink vlan 103 slan 503 tagged
Adding bridge on 1-1-9-0/eth
Created bridge-interface-record 1-1-9-0-eth-103/bridge
Bridge-path added successfully
```

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type  VLAN/SLAN  VLAN/SLAN    Physical        Bridge                        St Table Data
upl               ST   0/503   1/1/10/0/eth    1-1-10-0-eth-0-503/bridge   UP
int               Tg 101/503   1/1/7/0/eth     1-1-7-0-eth-103/bridge      UP
int               Tg 102/503   1/1/8/0/eth     1-1-8-0-eth-103/bridge      UP
4 Bridge Interfaces displayed
```

Configuração de bridges TLS

As bridges TLS aprendem os endereços MAC de origem (pacotes unicast) e encaminham os pacotes para seus respectivos destinos previamente aprendidos. Pacotes de broadcasts e unicasts desconhecidos são inundados para todas as interfaces, exceto na interface de entrada desses pacotes. Os pacotes recebidos no sistema através de uma interface TLS possuem seus respectivos endereços MAC de origem aprendido e associado com a respectiva interface, de forma que o pacote no sentido upstream para downstream possa ser enviado para a interface correta.

Bridge TLS é uma bridge simétrica e somente pode ser utilizada em conjunto com outras bridges TLS.

Configurando bridge intralink (stagged para tagged)

1. Crie a bridge TLS na interface GPON (sentido downstream - ONU);

```
iSH> bridge add 1-1-1-4/gpononu tls vlan 900 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-900/bridge
```

2. Crie a bridge TLS na interface Ethernet (sentido upstream – core da rede);

```
iSH> bridge add 1-1-2-0/eth tls vlan 900
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth/bridge
Bridge-path added successfully
```

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN   Physical          Bridge                          St Table Data
tls             Tagged 900  1/1/1/4/gpononu   1-1-1-257-gponport-900/bridge   UP
tls                    900  1/1/2/0/eth       1-1-2-0-eth/bridge              UP
2 Bridge Interfaces displayed
```

Configuração de bridges wire

Uma bridge wire é uma bridge TLS reservada. Ao configurar bridges wire, a VLAN ID utilizada nas duas bridge interfaces que formam a bridge wire é reservada e com uso exclusivo, isto é, a VLAN ID utilizada em uma bridge wire não pode ser utilizada em outra configuração da OLT. Cada bridge wire está restrita a apenas duas bridge interface em um VLAN ID.

Configurando bridge wire

1. Crie a bridge wire na interface Ethernet (sentido upstream – core da rede);

```
iSH> bridge add 1-1-4-0/eth wire vlan 500
Created bridge-interface-record 1-1-4-0-eth/bridge
Bridge-path added successfully
```

2. Crie a bridge wire na interface GPON (sentido downstream - ONU);

```
iSH> bridge add 1-1-1-4/gpononu wire vlan 500 tagged
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-500/bridge
```

3. Verifique as bridges:

```
iSH> bridge show
        Orig
Type VLAN/SLAN  VLAN/SLAN   Physical          Bridge                          St Table Data
wre             Tagged 500  1/1/1/4/gpononu   1-1-1-257-gponport-500/bridge  UP  No Learnig
wre                    500  1/1/4/0/eth       1-1-4-0-eth/bridge             UP  No Learnig
2 Bridge Interfaces displayed
```

Parâmetros floodUnknown e floodMulticast da bridge TLS

Bridges TLS podem fornecer serviços similares a VPN com os parâmetros *floodUnknown* e *floodMulticast* que possibilitam a OLT 8820 G encaminhar o tráfego desconhecido a todas as bridge interfaces dentro da VLAN.

floodUnknown

O parâmetro *floodUnknown* possibilita a inundação de quadros unicast desconhecido (mac address desconhecido) em todas as interfaces da VLAN. Um caso em que pode precisar fazer isso é quando os pacotes de voz são inundados na VLAN para verificar se há uma interface que dê uma resposta. Quando o parâmetro *floodUnknown* é colocado em true, a OLT 8820 G encaminha (inunda) para todas as interfaces da VLAN o endereços MAC unicast desconhecidos. O parâmetro *learnUnicast* é colocado em *true*. Se uma interface responde a um pacote encaminhado, o endereço é aprendido, e esse pacote não é mais inundado.

Quando esse parâmetro é colocado em *false*, a OLT 8820 G descarta quadros com endereços MAC unicast desconhecidos. Quadros sem correspondência na tabela de encaminhamento são descartados.

Para bridges TLS, a configuração padrão desses parâmetros é *true*. Para bridges de uplink, downlink e intralink, a configuração padrão desses parâmetros é *false*.

Esse exemplo exibe que as configurações padrão de *floodUnknown* e *learnUnicast* são colocadas em *true* na bridge TLS.

```
iSH> bridge add 1-1-1-4/gpononu tls vlan 500
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-500/bridge

iSH> get bridge-interface-record 1-1-1-257-gponport-500/bridge
bridge-interface-record     1-1-1-4-gponport/bridge
vpi: ---------------------------------------> {0}
vci: ---------------------------------------> {0}
vlanId: ------------------------------------> {500}
stripAndInsert: ----------------------------> {true}
customARP: ---------------------------------> {false}
filterBroadcast: ---------------------------> {false}
learnIp: -----------------------------------> {false}
learnUnicast: ------------------------------> {true}
```

```
maxUnicast: ---------------------------------> {100}
learnMulticast: -----------------------------> {false}
forwardToUnicast: ---------------------------> {true}
forwardToMulticast: -------------------------> {false}
forwardToDefault: ---------------------------> {false}
bridgeIfCustomDHCP: -------------------------> {false}
bridgeIfIngressPacketRuleGroupIndex: --------> {0}
vlanIdCOS: ----------------------------------> {0}
outgoingCOSOption: --------------------------> {disable}
outgoingCOSValue: ---------------------------> {0}
s-tagTPID: ----------------------------------> {0x8100}
s-tagId: ------------------------------------> {0}
s-tagStripAndInsert: ------------------------> {true}
s-tagOutgoingCOSOption: ---------------------> {s-tagdisable}
s-tagIdCOS: ---------------------------------> {0}
s-tagOutgoingCOSValue: ----------------------> {0}
mcastControlList: ---------------------------> {}
maxVideoStreams: ----------------------------> {0}
isPPPoA: ------------------------------------> {false}
floodUnknown: -------------------------------> {true}
floodMulticast: -----------------------------> {true}
bridgeIfEgressPacketRuleGroupIndex: ---------> {0}
bridgeIfTableBasedFilter: -------------------> {NONE(0)}
bridgeIfDhcpLearn: --------------------------> {NONE(0)}
mvrVlan: ------------------------------------> {0}
vlan-xlate-from: ----------------------------> {0}
slan-xlate-from: ----------------------------> {0}
```

floodMulticast

O parâmetro *floodMulticast* possibilita a OLT 8820 G inundar todo o tráfego multicast recebido em uma bridge para todas as portas da VLAN. Neste caso, o tráfego multicast não está relacionado ao tráfego de vídeo multicast, por exemplo, muitos protocolos de roteamento utilizam pacotes multicast para comunicação. Por padrão, esse parâmetro é colocado em *true* para bridges TLS e em *false* para bridges uplink e downlink.

Quando colocado em *true*, esse parâmetro faz com que todos os quadros multicast sejam encaminhados para todas as bridge interfaces da VLAN, exceto para a bridge interface onde o pacote multicast foi recebido.

Para visualizar as configurações desse parâmetro, insira o comando *get bridge-interface-record:*

```
iSH> bridge add 1-1-1-4/gpononu tls vlan 500
Adding bridge on 1-1-1-4/gpononu
Created bridge-interface-record 1-1-1-257-gponport-500/bridge

iSH> get bridge-interface-record 1-1-1-257-gponport-500/bridge
bridge-interface-record     1-1-1-4-gponport/bridge
vpi: ----------------------------------->    {0}
vci: ----------------------------------->    {0}
vlanId: -------------------------------->    {500}
stripAndInsert: ------------------------>    {true}
customARP: ----------------------------->    {false}
filterBroadcast: ------------------------>    {false}
learnIp: -------------------------------->    {false}
learnUnicast: --------------------------->    {true}
maxUnicast: ----------------------------->    {100}
```

```
learnMulticast: ------------------------->    {false}
forwardToUnicast: ------------------------>    {true}
forwardToMulticast: ---------------------->    {false}
forwardToDefault: ------------------------>    {false}
bridgeIfCustomDHCP: ---------------------->    {false}
bridgeIfIngressPacketRuleGroupIndex: ----->    {0}
vlanIdCOS: ------------------------------->    {0}
outgoingCOSOption: ----------------------->    {disable}
outgoingCOSValue: ------------------------>    {0}
s-tagTPID: ------------------------------->    {0x8100}
s-tagId: --------------------------------->    {0}
s-tagStripAndInsert: --------------------->    {true}
s-tagOutgoingCOSOption: ------------------>    {s-tagdisable}
s-tagIdCOS: ------------------------------>    {0}
s-tagOutgoingCOSValue: -------------------->   {0}
mcastControlList: ------------------------->   {}
maxVideoStreams: -------------------------->   {0}
isPPPoA: --------------------------------->    {false}
floodUnknown: ---------------------------->    {true}
floodMulticast: --------------------------->   {true}
bridgeIfEgressPacketRuleGroupIndex: ------->   {0}
bridgeIfTableBasedFilter: ----------------->   {NONE(0)}
bridgeIfDhcpLearn: ------------------------>   {NONE(0)}
mvrVlan: --------------------------------->    {0}
vlan-xlate-from: -------------------------->   {0}
slan-xlate-from: -------------------------->   {0}
```

Configuração de prevenção de loop de bridge

Prevenção de loop de bridge pode ser configurado tanto em bridges assimétricas quanto bridges simétricas, afim de solucionar comportamentos incorretos de endereços MAC.

Prevenção de loop de bridge em bridges assimétricas

Prevenção de loop de bridge pode ser configurado no bridge-path da bridge interface onde o endereço MAC é visto como entrando tanto no uplink quanto no downlink.

Quando ocorre o comportamento de loop de bridge e a opçpão blockAsym é configurada na bridge interface de uplink, o sistema bloqueia o downlink após detectar este comportamento incorreto do endereço MAC. Após a bridge bloqueada receber o endereço MAC infrator, o sistema envia um alarme MAJOR indicando que a bridge foi bloqueada para previnir o loop, este alarme exibe a bridge interface e o endereço MAC infrator. Neste caso a bridge interface bloqueada DEVE ser desbloqueada com o comando *bridge unblock interface/type.*

Quando ocorre o comportamente de loop de bridge e a opçpão blockAsymAuto é configurada na bridge interface de uplink, o sistema inicia uma série de 3 controles de monitorização cíclica, para verificar se a condição de loop foi resolvida. Se o comportamente de loop de bridge for resolvido, a bridge interface é automaticamente desbloqueada e um alarme de informação é enviado. Se o comportamento de loop não for resolvido, o alarme MAJOR é removido e um alarme CRITICAL é enviado. Neste caso a bridge interface DEVE ser desbloqueada com o comando *bridge unblock interface/type.*

Prevenção de loop de bridge em bridges simétricas (TLS)

Prevenção de loop de bridge pode ser configurado no bridge-path da bridge TLS onde o endereço MAC é visto entrando em uma bridge TLS e em seguida entrando em outra bridge TLS.

Quando ocorre o comportamento de loop de bridge e a opçpão blockall é configurada na bridge TLS, o sistema bloqueia a segunda bridge TLS e em seguida envia um alarme MAJOR indicando que a segunda bridge TLS viu o endereço MAC. A bridge é então bloqueada evitando um loop. Neste caso a bridge interface bloqueada DEVE ser desbloqueada com o comando *bridge unblock interface/type.*

Quando ocorre o comportamente de loop de bridge e a opçpão blockAsymAuto é configurada na bridge TLS, o sistema inicia uma série de 3 controles de monitorização cíclica, para verificar se a condição de loop foi resolvida.

Se um comportamente de loop de bridge é resolvido, a bridge interface é automaticamente desbloqueada e um alarme de informação é enviado. Se o comportamento de loop não for resolvido, o alarme MAJOR é removido e um alarme CRITICAL é enviado. Neste caso a bridge interface DEVE ser desbloqueada com o comando *bridge unblock interface/type*.

Configuração da prevenção de loop em bridge assimétrica

1. Para visualizar o bridge-path da bridge desejada, insire o comando *bridge-path show;*

```
iSH> bridge-path show
VLAN/SLAN   Bridge                      Address
------------------------------------------------------------------------------
100         1-1-4-0-eth-100/bridge  Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0,
            IGMP DSCP: 0, Flap Mode: Default, Block: Asym/Auto
```

2. Para configurar o modo de prevenção de loop como blockAsym, deve-se modificar o bridge-path da bridge desejada:

Sintaxe: *bridge-path modify bridge-path vlan VLAN-ID default block blockAsym.*

iSH> bridge-path modify 1-1-4-0-eth-100/bridge vlan 100 default block blockAsym

3. Para configurar o modo de prevenção de loop como blockAsymAuto, deve-se modificar o bridge-path da bridge desejada:

Sintaxe: *bridge-path modify bridge-path vlan VLAN-ID default block blockAsymAuto*

iSH> bridge-path modify 1-1-4-0-eth-100/bridge vlan 100 default block blockAsymAuto

Configuração da prevenção de loop em bridge simétrica (TLS)

1. Para visualizar o bridge-path da bridge desejada, insire o comando bridge-path show;

```
iSH> bridge-path show
VLAN/SLAN    Bridge     Address
------------------------------------------------------------------------------
999          N/A        VLAN, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0,
                        IGMP DSCP: 0, Flap Mode: Fast, Block: None
```

2. Para configurar o modo de prevenção de loop como blockAll, deve-se modificar o bridge-path da bridge desejada:

Sintaxe: *bridge-path modify vlan VLAN-ID block blockAll.*

iSH> bridge-path modify vlan 999 block blockAll

3. Para configurar o modo de prevenção de loop como blockAllAuto, deve-se modificar o bridge-path da bridge desejada:

Sintaxe: *bridge-path modify bridge-path vlan VLAN-ID block blockAllAuto*

iSH> bridge-path modify vlan 999 block blockAllAuto

Visualizando os alarmes de detecção de loop

1. No console, a seguinte mensagem é exibida ao ser detectado um loop;

```
iSH> JUN 22 02:12:40: alert : 1/a/1093: bridge: BridgeTrapSend():
l=1223:tBridgeMain: Bridge Loop detected on 1-10-1-501-gponport-100:(0/100/00:15:C5:3A:A3:B8)
```

2. Insira o comando *alarm show* para visualizar os alarmes de detecção de loop a nível de sistema;

```
iSH> alarm show
************ Central Alarm Manager ************
ActiveAlarmCurrentCount     :13
AlarmTotalCount             :16
ClearAlarmTotalCount        :3
OverflowAlarmTableCount     :0
ResourceId AlarmType AlarmSeverity
---------- --------- -------------
1-a-2-0/eth linkDown critical
1-a-3-0/eth linkDown critical
1-a-6-0/eth linkDown critical
1-a-7-0/eth linkDown critical
1-a-8-0/eth linkDown critical
```

```
1-a-9-0/eth linkDown critical
1-a-10-0/eth linkDown critical
1-a-11-0/eth linkDown critical
1-10-2-0/gponolt linkDown critical
1-10-3-0/gponolt linkDown critical
1-10-4-0/gponolt linkDown critical
system not_in_redundant_mode major
```

1-10-1-501-gponport-100 bridgeLoopDetect 0/100/00:15:C5:3A:A3:B8 major

3. Insira o comando *bridge show block*. Este comando também exibe as bridge que são bloqueadas normalmente pelas funções EAPS e STP.

iSH> bridge show block

Desbloqueando uma bridge bloqueada

Para desbloquear uma bridge bloqueada por causa da função de prevenção de loop de bridge utilizando o nome da bridge interface.

iSH> bridge unblock 1-10-1-501-gponport/bridge

Para desbloquear uma bridge bloqueada por causa da função de prevenção de loop de bridge utilizando a VLAN ID.

iSH> bridge unblock vlan 100

9.12. Comandos administrativos

A OLT 8820 G oferece os seguintes comandos administrativos de bridging:

- bridge delete.
- bridge show.
- bridge showall.
- bridge-path add.
- bridge-path show.
- bridge-path delete.
- bridge stats.
- bridge flush.

Comando bridge delete

O comando bridge *delete* remove uma bridge específica do sistema.

Comando bridge show/showall

Os comandos *bridge show* e *bridge showall* exibem o registro da bridge-path ou a tabela de bridges completa.

```
iSH> bridge showall
         Orig
Type VLAN/SLAN  VLAN/SLAN   Physical          Bridge                          St Table Data
-------------------------------------------------------------------------------------------
dwn             Tagged  998  1/1/1/1/gpononu   1-1-1-701-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/2/gpononu   1-1-1-702-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/3/gpononu   1-1-1-703-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/4/gpononu   1-1-1-704-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/5/gpononu   1-1-1-705-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/6/gpononu   1-1-1-706-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/7/gpononu   1-1-1-707-gponport-998/bridge  UP
dwn             Tagged  998  1/1/1/8/gpononu   1-1-1-708-gponport-998/bridge  UP
dwn             Tagged  109  1/1/4/1/gpononu   1-1-4-546-gponport-109/bridge  UP
upl             Tagged  998  1/1/8/0/eth       1-1-8-0-eth-998/bridge         UP S VLAN 998 default
upl             Tagged  840  1/1/9/0/eth       1-1-9-0-eth-840/bridge         UP S VLAN 840 default
11 Bridge Interfaces displayed
         Aging counter:       7513
         Renew failed:        0
         Filter renewed:      0
Flap Suppresses: 0

iSH> bridge show
         Orig
Type VLAN/SLAN   VLAN/SLAN        Physical            Bridge                          St Table Data
-------------------------------------------------------------------------------------------
dwn              Tagged    998    1/1/1/1/gpononu     1-1-1-701-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/2/gpononu     1-1-1-702-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/3/gpononu     1-1-1-703-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/4/gpononu     1-1-1-704-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/5/gpononu     1-1-1-705-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/6/gpononu     1-1-1-706-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/7/gpononu     1-1-1-707-gponport-998/bridge   UP
dwn              Tagged    998    1/1/1/8/gpononu     1-1-1-708-gponport-998/bridge   UP
dwn              Tagged    109    1/1/4/1/gpononu     1-1-4-546-gponport-109/bridge   UP
upl              Tagged    998    1/1/8/0/eth         1-1-8-0-eth-998/bridge          UP
upl              Tagged    840    1/1/9/0/eth         1-1-9-0-eth-840/bridge          UP
11 Bridge Interfaces displayed
```

10. Configuração de vídeo

10.1. Bridge de vídeo na OLT 8820 G

A bridging de vídeo permite o encaminhamento de pacotes de vídeo a um dispositivo downstream. Nesse caso, o vídeo viaja do headend (dispositivo de origem), utilizando um stream de vídeo para "atravessar" passivamente a OLT 8820 G. A bridge de vídeo exige a configuração de uma bridge de uplink e uma de downlink. Na bridge de uplink, a função *forwardToMulticast* é associada a um local com o conteúdo de vídeo que possibilita a OLT receber streaming de vídeo da rede. Uma interface com esse valor colocado em *true* somente transmite tráfego multicast para o qual foi recebida uma solicitação JOIN. A bridge interface com o parâmetro *forwardToMulticast* colocado em *false* descarta o tráfego multicast dessa interface. Por padrão, o parâmetro *forwardToMulticast* é colocado em true para bridges de uplink e em *false* para bridges de downlink.

Na bridge de downlink, a função *learnMulticast* é associada a interfaces com hosts conectados a elas e possibilita a OLT enviar os grupos de vídeo das interfaces de downlink para a rede. Por padrão, o parâmetro *learnMulticast* é colocado em *true* para bridges de downlink.

Perceba que as solicitações JOIN entram em uma interface *learnMulticast* associada a uma bridge de downlink e passam por uma interface *forwardToMulticast* associada a uma bridge de uplink.

A tabela a seguir detalha vários comportamentos de bridge de vídeo associadas a diferentes combinações de configurações para os parâmetros de bridge.

learnMulticast	forwardToMulticast	Comportamento
False	False	A interface descarta todos os pacotes multicast de entrada e não encaminha nenhum dos pacotes.
True	False	A interface encaminha os pacotes de sinalização multicast padrão e os pacotes multicast de controle.
False	True	A interface encaminha os pacotes contendo os grupos multicast somente para interfaces que enviaram mensagens JOIN para um grupo.
True	True	Memso comportamento de uma interface com o campo *learnMulticast* definido como *false* e o campo *forwardToMulticast* definido como *true*.

Combinações e comportamento de learnMulticast e forwardToMulticast

10.2. Configuração da bridge de vídeo na OLT 8820 G

Bridge de vídeo com IGMP Proxy

Resumo do IGMP Proxy

A ativação do IGMP Proxy reduz o tráfego entre a OLT e o headend (servidor multicast) de upstream, alterando o comportamento da OLT para o agrupamento e rastreio eficiente das solicitações JOIN e LEAVE . A OLT ao habilitar o IGMP Proxy também suporta os seguintes itens:

- Relatórios de consulta solicitados ou não.
- As consultas são enviadas somente a hosts que enviaram uma solicitação JOIN.
- Conformidade com rfc4541 a respeito de encaminhamento e regras IGMP.
- Os relatórios de membro em bridges de downlink não são encaminhados.
- Quando solicitações JOIN são recebidas sem LEAVE, assume-se que a set top box está controlando ambos os canais.
- O IGMP Proxy da OLT 8820 G suporta a função de número máximo de streaming de vídeo e lista de controle multicast.

Solicitações JOIN e LEAVE do IGMP Proxy

Para vídeos sem IGMP Proxy, as solicitações JOIN de hosts downstream são encaminhadas pela OLT ao servidor multicast. Para vídeos com IGMP Proxy, as solicitações JOIN de hosts downstream não são encaminhadas pela OLT ao servidor multicast da rede, mas sim rastreadas em uma tabela de informações onde os hosts estão organizados em um grupo. Quando o host envia uma solicitação JOIN que é a primeira do grupo, a OLT finaliza a solicitação JOIN do host e origina uma nova solicitação JOIN e a envia ao servidor multicast na rede com o endereço IP padrão *10.10.10.1* e um endereço MAC.

Quando o host envia uma solicitação LEAVE que é a última do grupo, a OLT finaliza a solicitação LEAVE do host e origina uma nova solicitação LEAVE e a envia ao servidor multicast na rede. Todas as solicitações LEAVE, independente de ser a última do grupo ou não, são finalizadas na OLT. Desse modo, o servidor multicast começa e para a transmissão de vídeo processando solicitações enviadas diretamente da OLT, e não de hosts de downstream. O IGMP Proxy acontece quando a OLT envia solicitações JOIN e LEAVE para a rede e controla solicitações JOIN e LEAVE enviadas de hosts para a OLT 8820 G.

Resumo básico da configuração da bridge de vídeo com IGMP Proxy

As conexões de bridge de vídeo exigem configurações específicas para as bridges de uplink e downlink. Geralmente, esses são os passos necessários para configurar bridge de vídeo na OLT 8820 G.

Configuração básica da conexão de vídeo na OLT 8820 G

1. Crie uma bridge de uplink com VLAN ID e IGMP Proxy;
2. Se necessário, crie listas de controle multicast;
3. Crie uma bridge de downlink com VLAN ID e especifique o número máximo de streaming de vídeo e uma lista de controle multicast.

Criando uma bridge de uplink em uma porta Ethernet uplink para vídeo

Crie uma bridge uplink de vídeo em uma porta Ethernet com o comando *bridge add* utilizando um VLAN ID. Depois, insira o período de espera multicast e o intervalo de consulta IGMP para o tráfego de vídeo ao inserir o comando *bridge-path add*.

1. Crie uma bridge de uplink tagged com um VLAN ID e a palavra-chave *igmpporxy*. Ao designar *igmpproxy* será habilitado esta função na bridge;

```
iSH> bridge add 1-1-3-0/eth uplink vlan 101 igmpproxy
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-101/bridge
Bridge-path added successfully
```

2. Verifique a bridge:

```
iSH> bridge show
          Orig
Type VLAN/SLAN   VLAN/SLAN    Physical          Bridge                  St Table Data
upl              Tagged 101   1/1/3/0/eth       1-1-3-0-eth-101/bridge  UP S VLAN 101 default
1 Bridge Interfaces displayed
```

3. Visualize a bridge-path para a bridge interface com o IGMP Proxy ativo;

```
iSH> bridge-path show
VLAN/SLAN   Bridge              Addredd
101 1-1-3-0-eth-101/bridge      Default, Age: 3600, MCAST Age: 250,
IGMP Query Interval: 120, IGMP Proxy, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

Criando listas de controle multicast

A especificação de uma lista de controle multicast 0 ativa todos os endereços IPs multicasts.

A bridge de downlink é configurada para vídeo inserindo a palavra-chave *vídeo*, a lista de controle multicast e o número máximo de streaming de vídeo é inserida no no formato *m/n.*

new mcast-control-entry <m>/<n>

<m> é o ID da lista de controle multicast e <n> é o índice de registro da lista de controle multicast *<m>*

Cada lista de controle multicast *<m>* normalmente possui vários registros *<n>*.

1. O exemplo a seguir adiciona três registros à lista de controle multicast 1:

```
iSH> new mcast-control-entry 1/1
mcast-control-entry         1/1
Please provide the following:[q]uit.
ip-address: ----->          {0.0.0.0}: 224.1.1.1
type: ----------->          {normal}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.

iSH> new mcast-control-entry 1/2
mcast-control-entry         1/2
Please provide the following:[q]uit.
```

```
ip-address: ------>          {0.0.0.0}:224.1.1.24
type: ------------>          {normal}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.

iSH> new mcast-control-entry 1/3
mcast-control-entry          1/3
Please provide the following:[q]uit.
ip-address: ------->         {0.0.0.0}:224.1.1.25
type: ------------->         {normal}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Continue adicionando quantos registros multicast forem necessários.

2. Verifique os registros multicast:

```
iSH> mcast show mcl 1
MCAST CONTROL LIST : 1
224.1.1.1 224.1.1.24   224.1.1.25
```

Criando uma bridge downlink para serviços de vídeo

A sintaxe para a bridge de downlink é:

bridge add <interface/type> gem <GEM port number> gtp <GPON traffic profile index> vlan <vlanid> [untagged]|[tagged] video <mcastControlListID>/<maxMulticast>

1. Crie uma bridge de downlink com VLAN ID em uma porta GPON da OLT;

Uma lista de controle multicast de registro *0* ativa todos os multicasts do IP.

```
iSH> bridge add 1-1-2-1/gpononu gem 501 gtp 1 downlink vlan 101 tagged video 0/7
Adding bridge on 1-1-2-1/gpononu
Created bridge-interface-record 1-1-2-501-gponport-101/bridge
```

2. Verifique a bridge.

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN     Physical          Bridge                          St Table Data
dwn-vid         Tagged 101    1/1/2/1/gpononu   1-1-2-501-gponport-101/bridge   UP
upl             Tagged 101    1/1/3/0/eth       1-1-3-0-eth-101/bridge          UP S VLAN 101 default
2 Bridge Interfaces displayed
```

Removendo a configuração de vídeo

Se necessário, pode remover a bridge de uplink, a bridge-path, as listas de controle multicast e as bridges de downlink.

1. Remova as listas de controle multicast;

```
iSH> delete mcast-control-entry 1/1
mcast-control-entry          1/1
1 entry found.
Delete mcast-control-entry 1/1? [y]es, [n]o, [q]uit : y
mcast-control-entry          1/1 deleted.

iSH> delete mcast-control-entry 1/2
mcast-control-entry          1/2
1 entry found.
Delete mcast-control-entry 1/2? [y]es, [n]o, [q]uit : y
mcast-control-entry          1/2 deleted.
```

```
iSH> delete mcast-control-entry 1/3
mcast-control-entry         1/3
1 entry found.
Delete mcast-control-entry 1/3? [y]es, [n]o, [q]uit : y
mcast-control-entry         1/3 deleted.
```

2. Remova a bridge de vídeo downlink;

```
iSH> bridge delete 1-1-2-501-gponport-101/bridge
1-1-2-501-gponport-991/bridge delete complete
```

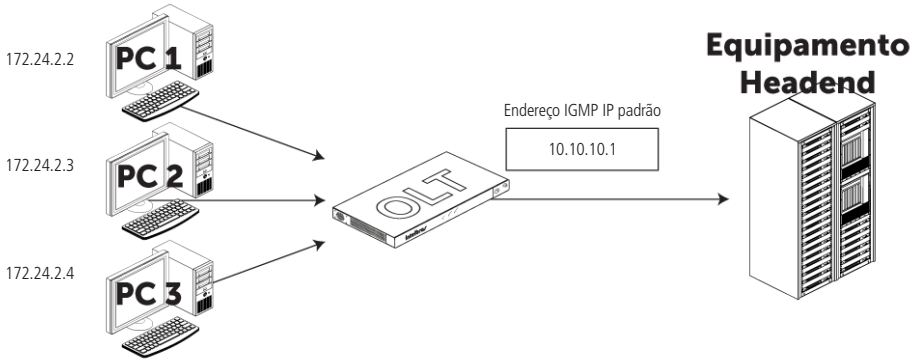
3. Remova a bridge de uplink;

```
iSH> bridge delete 1-1-3-0-eth-101/bridge vlan 101
Bridge-path deleted successfully
1-1-3-0-eth-101/bridge delete complete
```

10.3. Configurações avançadas de bridge de vídeo IGMP

Configuração do IGMP Proxy com endereço IP padrão

Quando o IGMP Proxy está ativo em uma bridge de uplink, o endereço IP padrão de origem no pacote Ethernet enviado pela bridge é 10.10.10.1, como exibido na imagem a seguir.



Solicitações JOIN e LEAVE da OLT 8820 G e do servidor multicast, e endereço IP IGMP padrão

Configurando IGMP Proxy com endereço IP padrão

1. Crie uma bridge uplink com VLAN ID e insira a palavra-chave *igmpproxy;*

```
iSH> bridge add 1-1-3-0/eth uplink vlan 101 igmpproxy
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-101/bridge
Bridge-path added successfully
```

Por padrão, a bridge uplink será configurada como tagged, caso essa opção for omitida no comando bridge add.

2. Verifique a bridge;

```
iSH> bridge show
          Orig
Type VLAN/SLAN   VLAN/SLAN     Physical      Bridge                    St Table Data
upl              Tagged 101    1/1/3/0/eth   1-1-3-0-eth-101/bridge    DWN S VLAN 101 default
1 Bridge Interfaces displayed
```

3. Verifique a bridge-path.

```
iSH> bridge-path show
VLAN/SLAN   Bridge                    Address
      101 1-1-3-0-eth-101/bridge      Default, Age: 3600, MCAST Age: 250,
IGMP Query Interval: 120, IGMP Proxy, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

O parâmetro *age* determina a idade máxima, em segundos, para remoção um pacote unicast da tabela de filtros. O padrão é *3600*.

O parâmetro *mcast* determina a idade máxima, em segundos, para eliminar um pacote multicast da tabela de filtros. O padrão é *250*.

O parâmetro *igmptimer* indica um valor de tempo em segundos para a frequência de envio de relatórios e solicitações de membros IGMP pela bridge. Se modificar a bridge-path inserindo 0 para esse valor, a função de consulta é desativada. O padrão é *120*.

Criando uma bridge de downlink para serviços de vídeo

Crie uma bridge de downlink na porta GPON OLT com VLAN ID e número máximo de streaming de vídeo, inserindo se necessário a lista de controle multicast.

Adicione a lista de controle multicast e determine o número máximo de streaming de vídeos utilizando o formato *m/n*.

A lista de controle multicast é configurada primeiro e o número máximo de streaming de vídeo depois. O padrão para a lista de controle multicast é *0*.

Uma lista de controle multicast de registro *0* permite todos os endereços IP multicasts.

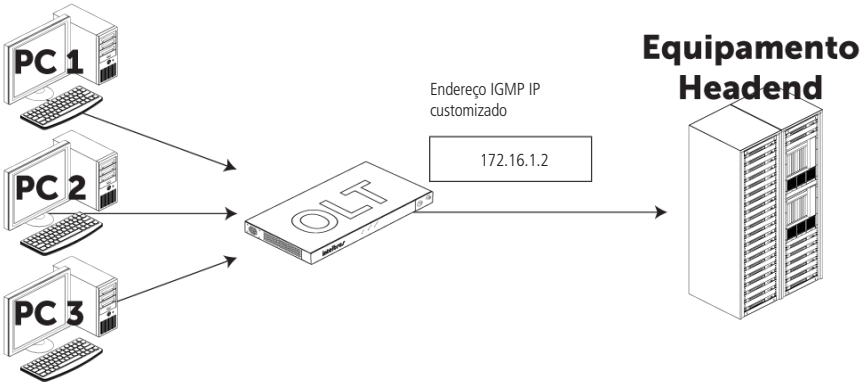
```
iSH> bridge add 1-1-2-1/gpononu gem 501 gtp 1 downlink vlan 101 tagged video 0/7
Adding bridge on 1-1-2-1/gpononu
Created bridge-interface-record 1-1-2-501-gponport-101/bridge
```

Verifique a bridge.

```
iSH> bridge show
          Orig
Type VLAN/SLAN   VLAN/SLAN   Physical          Bridge                          St Table Data
dwn-vid          Tagged 101  1/1/2/1/gpononu   1-1-2-501-gponport-101/bridge   DWN
upl              Tagged 101  1/1/3/0/eth       1-1-3-0-eth-101/bridge          UP S VLAN 101 default
2 Bridge Interfaces displayed
```

Configurando IGMP Proxy com endereço IP customizado

Quando o snooping do IGMP com relatório de proxy está ativo em uma bridge de uplink estável, o endereço IP padrão de origem no pacote Ethernet enviado pela bridge é 10.10.10.1. Quando o IGMP Proxy está ativo em uma bridge de uplink, o endereço IP padrão de origem no pacote Ethernet enviado pela bridge é 10.10.10.1. Em certos casos pode ser necessário alterar o endereço 10.10.10.1 conforme necessário. Por exemplo, quando um roteador na rede implementou Reverse Path Forwarding e espera um endereço IP na sub-rede do roteador.



Solicitações JOIN e LEAVE da OLT 8820 G e do servidor multicast, e endereço IP IGMP customizado

Configurando IGMP Proxy com endereço IP customizado

1. Crie uma bridge de uplink com VLAN ID e insira a palavra-chave *igmpproxy;*

```
iSH> bridge add 1-1-3-0/eth uplink vlan 202 igmpproxy
Adding bridge on 1-1-3-0/eth
Created bridge-interface-record 1-1-3-0-eth-202/bridge
Bridge-path added successfully
```

Verifique a bridge.

```
iSH> bridge show
          Orig
Type VLAN/SLAN   VLAN/SLAN   Physical     Bridge                    St Table Data
upl              Tagged 202  1/1/3/0/eth  1-1-3-0-eth-202/bridge    DWN S VLAN 202 default
1 Bridge Interfaces displayed
```

Verifique a bridge-path.

```
iSH> bridge-path show
VLAN/SLAN   Bridge                    Address
202 1-1-3-0-eth-202/bridge            Default, Age: 3600, MCAST Age: 250, IGMP Query
Interval: 120, IGMP Proxy, IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

2. Modifique a bridge-path para o endereço IP customizado inserindo a palavra-chave *igmpsendip <ipaddress>* para fornecer o novo endereço IP para todas as mensagens IGMP em direção upstream, da OLT para o servidor multicast;

```
iSH> bridge-path modify 1-1-3-0-eth-202/bridge vlan 202 default igmpsendip enable 172.16.1.3
Bridge-path 1-1-3-0-eth-202/bridge/3/202/0/0/0/0/0/0/0 has been modified
```

Verifique a bridge-path.

```
iSH> bridge-path show
VLAN/SLAN   Bridge                          Address
202 1-1-3-0-eth-202/bridge                  Default, Age: 3600, MCAST Age: 241,
IGMP Query Interval: 120, IGMP Proxy, Custom IP 172.16.1.3, IGMP DSCP: 0, Flap
Mode: Default, Block: Asym
```

Para voltar a configuração para o endereço IP padrão 10.10.10.1, insira o comando *igmpsendip disable*.

3. Crie uma bridge de downlink para vídeo em uma porta GPON da OLT.

```
iSH> bridge add 1-1-2-1/gpononu gem 501 gtp 1 downlink vlan 202 tagged video 0/7
Adding bridge on 1-1-2-1/gpononu
Created bridge-interface-record 1-1-2-501-gponport-0/bridge
```

Removendo a bridge de vídeo com IGMP Proxy com endereço IP customizado

1. Remova a bridge de uplink;

```
iSH> bridge delete 1-1-3-0-eth-202/bridge
Bridge-path deleted successfully
1-1-3-0-eth-202/bridge delete complete
```

2. Remova a bridge de downlink.

```
iSH> bridge delete 1-1-2-501-gponport-202/bridge
1-1-2-501-gponport-202/bridge delete complete
```

10.4. Estatísticas de bridging IGMP

Visualizando as estatísticas de bridging IGMP

Visualize as estatísticas de bridging IGMP.

```
iSH> bridge igmpstat
                                        Received                                Transmitted
Interface                       GenQuery  SpecQuery  v2Re-    Leave  GenQuery  SpecQuery  v2Report  Leave
                                                     port
1-1-1-501-gponport-510/bridge   627       0          0        0      0         0          0         0
1-1-2-0-eth-105/bridge          0         0          0        0      0         0          0         0
2 Bridge Interfaces displayed
```

11. Serviços Ethernet

Esse capítulo explica os serviços Ethernet na OLT 8820 G.

As interfaces FE/GE são identificadas como *1-1-x-0/eth* na linha de comando, onde x vai de 2 até 9. As interfaces uplink 10GE são identificadas como *1-1-x-0/eth* na linha de comando, onde x é 10 ou 11.

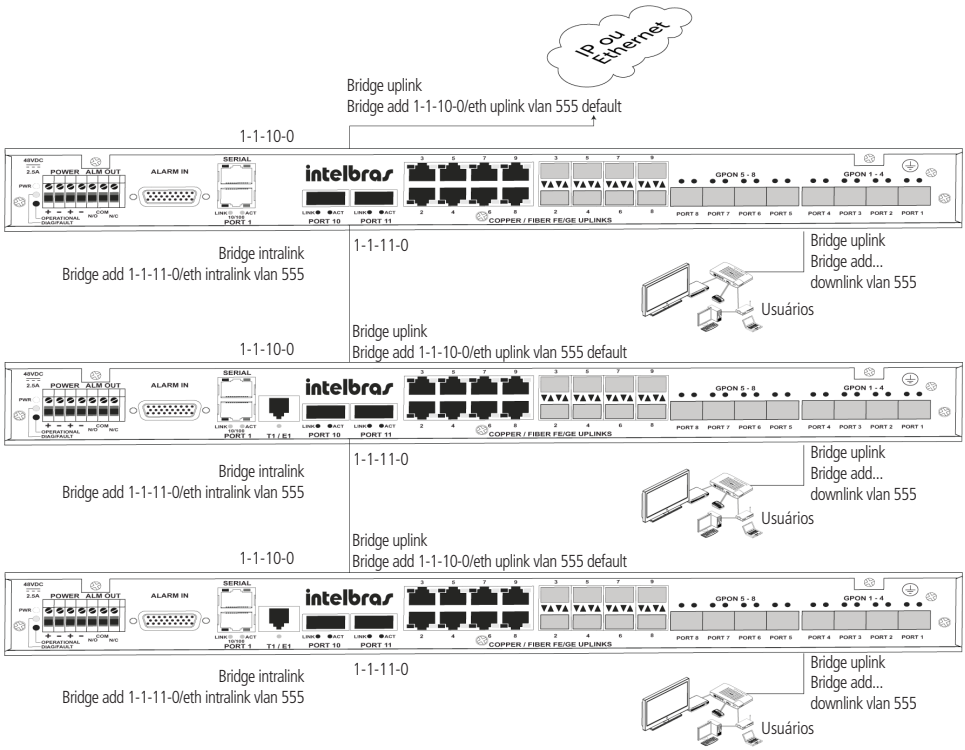
11.1. Bridging com topolgogia 10 Gigabit Ethernet linear

Dentro da topologia linear, o comportamento de bridging pode ser configurado para enviar tráfego com base em endereços MAC e VLAN ID para um IP ou rede externa. O nó conectado à rede contém uma bridge de uplink e uma bridge-path na primeira porta Ethernet de 10 Gigabit (*1-1-10-0/eth*) da OLT 8820 G para direcionar todo o tráfego de bridging para fora ou para a rede IP. Esse dispositivo também contém um intralink na segunda porta Ethernet 10 Gigabit (*1-1-11-0/eth*) para que o tráfego desconhecido seja enviado no sentido downstream, mesmo que o aprendizado de endereço não esteja ativada.

O segundo nó da topologia linear contém uma bridge de uplink na primeira porta Ethernet 10 Gigabit (*1-1-10-0/eth*) para direcionar todo o tráfego de bridging em trânsito para o nó de upstream. Esse nó também contém um intralink na segunda porta Ethernet 10 Gigabit (*1-1-11-0/eth*) para que o tráfego desconhecido seja enviado no sentido downstream a outra rede ou dispositivo Ethernet secundário, mesmo que o aprendizado de endereço não esteja ativada.

Nós adicionais podem ser adicionados à topologia linear da OLT repetindo esse padrão de conexões e bridging.

A imagem a seguir exibe o comportamento de bridging utilizando a configuração linear Ethernet 10 Gigabit na OLT 8820 G.



Bridge uplink
Bridge add 1-1-10-0/eth uplink vlan 555 default

Bridge intralink
Bridge add 1-1-11-0/eth intralink vlan 555

Bridge uplink
Bridge add...
downlink vlan 555

Bridge uplink
Bridge add 1-1-10-0/eth uplink vlan 555 default

Bridge intralink
Bridge add 1-1-11-0/eth intralink vlan 555

Bridge uplink
Bridge add...
downlink vlan 555

Bridge uplink
Bridge add 1-1-10-0/eth uplink vlan 555 default

Bridge intralink
Bridge add 1-1-11-0/eth intralink vlan 555

Bridge uplink
Bridge add...
downlink vlan 555

Bridging utilizando a configuração linear de Ethernet 10 Gigabit

Configurando o comportamento de bridging

1. Na OLT conectada à rede IP ou Ethernet:

a. Adicione uma bridge interface à primeira porta 10GE de uplink (essa é a porta conectada à rede externa):

```
iSH> bridge add 1-1-10-0/eth uplink vlan 555
Adding bridge on 1-1-10-0/eth
Created bridge-interface-record 1-1-10-0-eth-555/bridge
Bridge-path added successfully
```

b. Verifique a bridge de uplink.

```
iSH> bridge show
          Orig
Type VLAN/SLAN    VLAN/SLAN   Physical     Bridge                    St Table Data
upl             Tagged  555   1/1/10/eth   1-1-10-0-eth-555/bridge  DWN S VLAN 555 default
1 Bridge Interfaces displayed
```

Todo o tráfego será encaminhado por essa interface.

c. Adicione uma bridge interface intralink na segunda porta 10GE:

```
iSH> bridge add 1-1-11-0/eth intralink vlan 555
Adding bridge on 1-1-11-0/eth
Created bridge-interface-record 1-1-11-0-eth-555/bridge
Bridge-path added successfully
```

O tráfego desconhecido recebido nessa interface é enviado para a rede externa.

Essa interface é o intralink para a próxima OLT.

d. Adicione uma bridge de downlink ao assinante remoto:

```
iSH> bridge add 1-1-1-1/gpononu gem 501 gtp 1 downlink vlan 555
Adding bridge on 1-1-1-1/gpononu
Created bridge-interface-record 1-1-1-501-gponport/bridge
```

e. Verifique as interfaces de bridge.

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN      Physical           Bridge                   St Table Data
dwn             555           1/1/1/1/gpononu    1-1-1-901-gponport/bridge  UP
int             Tagged 555    1/1/11/0/eth       1-1-11-0-eth-555/bridge    DWN S VLAN 555 Intralink
upl             Tagged 555    01/01/2010/0/eth   1-1-10-0-eth-555/bridge    DWN S VLAN 555 default
3 Bridge Interfaces displayed
```

2. Na próxima OLT da topologia linear:

a. Adicione uma bridge interface uplink:

```
iSH> bridge add 1-1-10-0/eth uplink vlan 555
Adding bridge on 1-1-10-0/eth
Created bridge-interface-record 1-1-10-0-eth-555/bridge
Bridge-path added successfully
```

b. Adicione uma bridge interface intralink na segunda porta 10GE:

```
iSH> bridge add 1-1-11-0/eth intralink vlan 555
Adding bridge on 1-1-11-0/eth
Created bridge-interface-record 1-1-11-0-eth-555/bridge
Bridge-path added successfully
```

O tráfego desconhecido recebido nessa interface é enviado para a rede externa.

Essa interface é o intralink para a próxima OLT.

c. Adicione uma bridge de downlink ao assinante remoto:

```
iSH> bridge add 1-1-2-1/gpononu gem 901 gtp 1 downlink vlan 555
Adding bridge on 1-1-2-1/gpononu
Created bridge-interface-record 1-1-2-901-gponport/bridge
```

d. Visualize as interfaces de bridge.

```
iSH> bridge show
          Orig
Type VLAN/SLAN    VLAN/SLAN    Physical           Bridge                        St Table Data
dwn               555          1/1/2/1/gpononu    1-1-2-901-gponport/bridge     UP
int             Tagged 555     1/1/11/0/eth       1-1-11-0-eth-555/bridge       DWN S VLAN 555 Intralink
upl             Tagged 555     01/01/2010/0/eth   1-1-10-0-eth-555/bridge       DWN S VLAN 555 default
3 Bridge Interfaces displayed
```

3. Para a próxima OLT da topologia linear:

a. Adicione uma bridge interface à primeira porta 10GE de uplink (essa é a porta conectada a segunda OLT):

```
iSH> bridge add 1-1-10-0/eth uplink vlan 555
Adding bridge on 1-1-10-0/eth
Created bridge-interface-record 1-1-10-0-eth-555/bridge
Bridge-path added successfully
```

b. Verifique a bridge de uplink.

Todo o tráfego será encaminhado por essa interface.

```
iSH> bridge show
          Orig
Type VLAN/SLAN    VLAN/SLAN     Physical     Bridge                    St Table Data
upl             Tagged   555    1/1/10/eth   1-1-10-0-eth-555/bridge   DWN S VLAN 555 default
1 Bridge Interfaces displayed
```

c. Adicione uma bridge intralink na segunda porta 10GE:

```
iSH> bridge add 1-1-11-0/eth intralink vlan 555
Adding bridge on 1-1-11-0/eth
Created bridge-interface-record 1-1-11-0-eth-555/bridge
Bridge-path added successfully
```

O tráfego desconhecido recebido nessa interface é enviado para a rede externa.

Essa interface é o intralink para a próxima OLT.

d. Adicione uma bridge de downlink ao assinante remoto:

```
iSH> bridge add 1-1-3-2/gpononu gem 456 gtp 1 downlink vlan 555
Adding bridge on 1-1-3-2/gpononu
Created bridge-interface-record 1-1-3-456-gponport/bridge
```

e. Verifique as interfaces de bridge.

```
iSH> bridge show
       Orig
Type VLAN/SLAN  VLAN/SLAN   Physical           Bridge                        St Table Data
dwn                 555     1/1/3/2/gpononu    1-1-3-456-gponport/bridge     UP
int             Tagged 555  1/1/11/0/eth       1-1-11-0-eth-555/bridge       DWN S VLAN 555 Intralink
upl             Tagged 555  01/01/2010/0/eth   1-1-10-0-eth-555/bridge       DWN S VLAN 555 default
3 Bridge Interfaces displayed
```

4. Continue essa configuração para todos as OLTs da topologia linear.

12. Interfaces de assinantes GPON

12.1. Resumo

As interfaces GPON da OLT 8820 G fornecem uma interface GPON de alta velocidade baseada em padrões entre a OLT e as ONTs.

Esse capítulo fornece os procedimentos de configuração passo a passo para configuração de serviços de Dados, Voz e Vídeo na OLT para as ONTs.

12.2. Resumo OMCI

OMCI (ONT Management and Control Interface) é um protocolo definido pela norma ITU-T G.988 que habilita a OLT para controlar uma ONU/ONT. Esse protocolo possibilita a OLT:

- » Estabelecer e desconectar conexões na ONU.
- » Gerenciar as UNI Interfaces (Interfaces de Rede do usuário) na ONU.
- » Solicitar informações de configuração e estatísticas de desempenho.
- » Informar de modo autônomo ao operador de sistema sobre eventos como falhas de link.

O protocolo OMCI funciona através da conexão GEM entre a OLT e a ONU, estabelecida durante a inicialização da ONU.

O requisito de gerenciamento da ONU e da interface de controle são descrios pela norma ITU-T G.988. Essas recomendações são necessárias para gerenciar a ONU nas seguintes áreas:

- » Gerenciamento da configuração
- » Gerenciamento de falhas
- » Gerenciamento do desempenho
- » Gerenciamento da segurança

12.3. Provisionamento USP (Unified Service Provisioning)

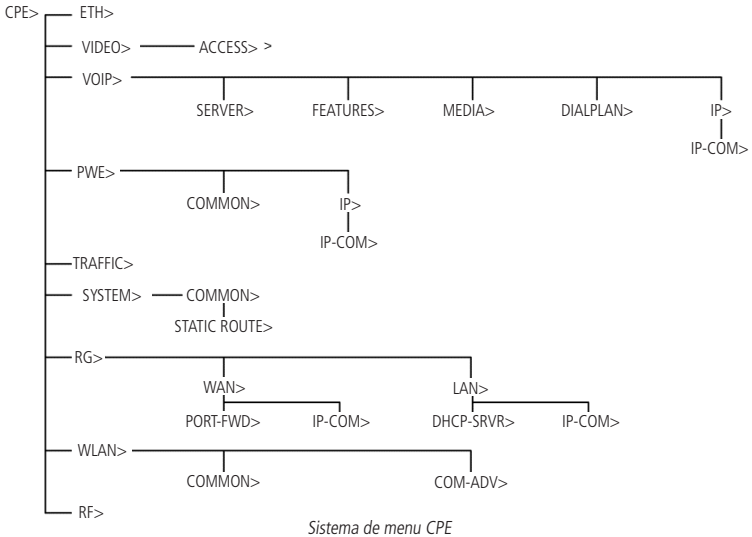
O provisionamento USP fornece um método único de provisionamento para ONT GPON da Intelbras, sua configuração é realizada via OLT 8820 G.

O Unified Service Provisioning (USP) acessa a todas as interfaces de gerenciamento, podendo trabalhar com características que estavam somente disponíveis através de SNMP ou pela interface web de usuário.

Obs.: *configurações realizadas na ONT através da OLT têm prioridade sobre as configurações realizadas localmente pelo usuário na ONT, ou seja, se o usuário modificar alguma configuração na ONT que foi realizada através da OLT, essa nova configuração permanecerá ativa até que seja feita a ressincronização através do comando "onu resync". Esse processo pode levar até 3 minutos após a ressincronização da ONT.*

Sistema de menu CPE

O sistema de menu CPE exibido na imagem a seguir é implementado no método de provisioanamento USP (Unified Service Provisioning).



Sistema de menu CPE

Usando o Shell de Comando CPE para provisonamento USP

Para provisionar e gerenciar serviços CPE nas ONTs, os usuários podem digitar um comando macro de perfil CPE com uma única linha, ou usar o shell de comando do CPE.

Os exemplos a seguir exibem como usar o shell de comando CLI.

1. Para entrar em um shell de comando:

```
iSH> ↵
iSH> cpe ↵
iSH> CPE> voip ↵
iSH> CPE > VOIP> server ↵
iSH> CPE > VOIP> SERVER>
```

Ou

```
iSH> cpe voip server ↵
iSH> CPE > VOIP> SERVER>
```

2. Para conhecer os comandos suportados no shell de comando corrente, pressione "?" e depois "Enter":

```
iSH> CPE> VOIP> SERVER> ? ↵
Error:    Invalid argument "?"
cpe voip server <add | delete | find | modify | show>
```

3. Para obter ajuda sobre os comandos suportados no shell de comando corrente, digite "help" e pressione "Enter":

```
iSH> CPE> VOIP> FEATURES> help ↵
cpe voip features add <profile-name>
          [ announcement-type < silence | reordertone | fastbusy | voice | na > ]
              specifies the treatment when a subscriber goes off hook but does
              not attempt a call
          [ cid-features < calling-number | calling-name | cid-block | cid-number |
                          cid-name | anonym-block | all | none > ]
              bit map of the caller ID features
          [ call-waiting-features < call-waiting | cid-announcement | all | none > ]
              bit map of the call waiting features
        [ call-progress-or-transfer-features < 3-way | call-transfer | call-hold | call-park |
                                    do-not-disturb | flash-on-emergency | emergency-hold |
```

```
                                                6-way | pbx-dialing | all | none > ]
                bit map of the call processing features
            [ call-presentation-features < msg-wait-splash-ring | msg-wait-special-dial-tone |
                                           msg-wait-visual | call-fwd | all | none > ]
                bit map of call presentation features

       To clear a bit map value, simply place a minus sign in from of the argument.
       Example:  "-calling-name" clears the calling-name value in the cid-features.

       To enable all features in a bit-map use the "all" keyword.

       To clear all features in a bit-map use the "none" keyword.

           [ hotline < disabled | hot | warm > ]
                 When the hotline is hot, the phone will immediately dial the hotline number.
              When the hotline is warm, the phone wait for the period specified in warmline-timer
                 in ms before automatically dial the hotline number.
           [ hotLine-number ] - hot line number to be given
         [ warmLine-Timer ]- timer to wait for the specified period before dialing hotLine-number
       This command creates a new profile.  The <profile-name> must be supplied
       and must be unique for profile type.  The profile index will be automatically
       generated

cpe voip features modify < index | profile-name > [ arguments ]
       Modify a profile using the profile's <index> or <profile-name>.
       See "add" command for available [ arguments ]

cpe voip features delete < index | profile-name >
       Delete a profile using the profile's <index> or <profile-name>

cpe voip features find < index | profile-name >
       Find all cpe-voip-subscriber profiles that reference the cpe-voip-features.
```

4. Para executar a auto completação no shell de comando corrente, insira o inicio do comando e pressione "Tab":

```
iSH> CPE> VOIP> SERVER> add metaswitch-sip primary-server 172.16.60.51 s<Tab>
secondary-server
signalling-dscp
signalling-protocol
sip-domain
sip-reg-exp-time
sip-reg-retry-time
sip-istrar
sip-rereg-head-start-time
softswitch
iSH> CPE> VOIP> SERVER> add metaswitch-sip primary-server 172.16.60.51 se<Tab>

iSH> CPE> VOIP> SERVER> add metaswitch-sip
primary-server 172.16.60.51 secondary-server
```

5. Para sair do shell de comando corrente, insira a palavra "exit":

```
iSH> CPE> VOIP> SERVER> exit ↵
iSH> CPE> VOIP>
```

Ou utilize a tecla de atalho x:

```
iSH> CPE> VOIP> SERVER> x ↵
iSH> CPE> VOIP>
```

6. Para sair do sistema de menu CPE:

```
iSH> CPE> VOIP> SERVER> quit ↵
iSH>
```

Ou utilize a tecla de atalho q:

```
iSH> CPE> VOIP> SERVER> q ↵
iSH>
```

Atribuição de GEM Ports com USP

Ao utilizar o serviço USP para provisioanemento, qualquer GEM Port ID no range de 257-3828 é permitido para ser associada com qualquer ONU, exceto os GEM Port IDs 5xx, onde xx deve ser o ID da ONU (varia de 1 a 64) na porta PON correspondente.

Os usuários podem especificar a GEM Port durante a execução do comando *bridge add* ou omitir esta informação e deixar que a OLT preencha esta informação de forma automática.

Atribuição automática de GEM Ports

O campo GEM Port ID não é obrigatório no comando bridge add.

O sistema irá escolher automaticamente os IDs das GEM Portsd disponíveis para ONUs. Neste exemplo, será adicionado serviços de dados para o modelo de serviço "TriplePlay", sem especificar uma GEM Port.

```
zSH> bridge add tripleplay gtp 10240 downlink vlan 102 tagged rg-brouted eth [1-2]
Adding bridge on tripleplay
Created bridge-interface-record 1-0-0-257-gponport-102/bridge GEM port 257 has been assigned automatically
CPE Connection 1-0-0-257/gponport/1/1/0/0 has been created
CPE Connection 1-0-0-257/gponport/1/2/0/0 has been created
```

Atribuição arbitrário de GEM Ports

Ao criar uma GEM Port com o comando bridge add, deve-se especificar a interface da ONU (ONU ID) e o GEM Port ID. Observe que cada um destes GEM Port IDs deve ser único para cada porta PON da OLT.

```
zSH> bridge add 1-1-3-1/gpononu gem 610 gtp 1 downlink vlan 1001 tagged eth 1
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record 1-1-3-610-gponport-1001/bridge
CPE Connection 1-1-3-610/gponport/1/1/0/0 has been created
```

Se o especificado GEM Port ID está livre, então ele será atribuido a ONU.

Se o GEM Port ID já esteja atribuido e utilizado pela mesma ONU, ele será reutilizado.

Se o GEM Port ID esteja atribuido para uma ONU diferente, uma mensagem de erro será exibida e o comando falhará.

Para visualizar quais GEM Port IDs estão sendo utilizadas na ONU, pode-se utilizar o comando *gpononu gemports.*

O comando *gpononu gemports* permite as opções de escolha por slot, OLT ou ONU. Ao executar o comando sem definir o slot/OLT/ONU o comando verificará a informação em cada porta da OLT, o que pode levar um tempo maior para a conclusão do comando.

O exemplo do comando bridge add também define qual VLAN é correspondente a GEM Port. Dependendo de sua implementação, os usuários podem especificar uma VLAN para um serviço e atribuir a mesma VLAN para GEM Ports diferentes.

Atribuição do GTP (GPON Traffic Profile) com USP

Os usuários podem especificar o GTP (GPON Traffic Profile) durante a execução do comando bridge add ou omitir esta informação e deixar que a OLT preencha esta informação com um valor default.

Atribuição automática do GTP

O campo GTP é ignorado no comando bridge add, o sistema irá atribuir automaticamente um perfil GTP baseado nos seguintes tipos de serviços:

» **Para serviços de dados, o GTP padrão é *1100000000*:**

```
iSH> get gpon-traffic-profile 1100000000
gpon-traffic-profile 1100000000
guaranteed-upstream-bw: -----> {0}
traffic-class: ---------------> {ubr}
compensated: -----------------> {false}
shared: ----------------------> {false}
dba-enabled: -----------------> {true}
dba-fixed-us-ubr-bw: ---------> {128}
dba-fixed-us-cbr-bw: ---------> {0}
dba-assured-us-bw: -----------> {0}
dba-max-us-bw: ---------------> {1000000}
dba-extra-us-bw-type: -------> {nonassured}
```

» **Para serviços de voz com 2 portas FXS, o GTP padrão é *1100000001*:**

```
iSH> get gpon-traffic-profile 1100000001
gpon-traffic-profile 1100000001
guaranteed-upstream-bw: -----> {0}
traffic-class: ---------------> {ubr}
compensated: -----------------> {false}
shared: ----------------------> {false}
dba-enabled: -----------------> {true}
dba-fixed-us-ubr-bw: ---------> {128}
dba-fixed-us-cbr-bw: ---------> {0}
dba-assured-us-bw: -----------> {256}
dba-max-us-bw: ---------------> {384}
dba-extra-us-bw-type: -------> {nonassured}
```

» **Para serviços de voz com 4 portas FXS, o GTP padrão é *1100000002*:**

```
iSH> get gpon-traffic-profile 1100000002
gpon-traffic-profile 1100000002
guaranteed-upstream-bw: -----> {0}
traffic-class: ---------------> {ubr}
compensated: -----------------> {false}
shared: ----------------------> {false}
dba-enabled: -----------------> {true}
dba-fixed-us-ubr-bw: ---------> {128}
dba-fixed-us-cbr-bw: ---------> {0}
dba-assured-us-bw: -----------> {384}
dba-max-us-bw: ---------------> {1000000}
dba-extra-us-bw-type: -------> {nonassured}
```

» **Para serviços de voz com 8 portas FXS, o GTP padrão é *1100000003*:**

```
iSH> get gpon-traffic-profile 1100000003
gpon-traffic-profile 1100000003
guaranteed-upstream-bw: --------> {0}
traffic-class: -----------------> {ubr}
compensated: -------------------> {false}
shared: ------------------------> {false}
dba-enabled: -------------------> {true}
dba-fixed-us-ubr-bw: -----------> {128}
```

```
dba-fixed-us-cbr-bw: ------------>     {0}
dba-assured-us-bw: ------------->     {896}
dba-max-us-bw: ----------------->     {1000000}
dba-extra-us-bw-type: ---------->     {nonassured}
```

» **Para serviços de voz com 24 portas FXS, o GTP padrão é *1100000004*:**

```
iSH> get gpon-traffic-profile 1100000004
gpon-traffic-profile 1100000004
guaranteed-upstream-bw: ------->     {0}
traffic-class: ----------------->     {ubr}
compensated: ------------------->     {false}
shared: ------------------------>     {false}
dba-enabled: ------------------->     {true}
dba-fixed-us-ubr-bw: ------------>     {128}
dba-fixed-us-cbr-bw: ------------>     {0}
dba-assured-us-bw: ------------->     {2944}
dba-max-us-bw: ----------------->     {1000000}
dba-extra-us-bw-type: ---------->     {nonassured}
```

» **Para serviços com 2 portas PWE, o GTP padrão é *1100000005*:**

```
iSH> get gpon-traffic-profile 1100000005
gpon-traffic-profile 1100000005
guaranteed-upstream-bw: ---------->     {0}
traffic-class: -------------------->     {ubr}
compensated: ---------------------->     {false}
shared: ------------------------->     {false}
dba-enabled: ---------------------->     {true}
dba-fixed-us-ubr-bw: ------------->     {0}
dba-fixed-us-cbr-bw: ------------->     {6016}
dba-assured-us-bw: --------------->     {0}
dba-max-us-bw: ------------------->     {1000000}
dba-extra-us-bw-type: ------------>     {nonassured}
```

» **Para serviços com 4 portas PWE, o GTP padrão é *1100000006*:**

```
iSH> get gpon-traffic-profile 1100000006
gpon-traffic-profile 1100000006
guaranteed-upstream-bw: ------->     {0}
traffic-class: ----------------->       {ubr}
compensated: ------------------->     {false}
shared: ------------------------>     {false}
dba-enabled: ------------------->     {true}
dba-fixed-us-ubr-bw: ------------>     {0}
dba-fixed-us-cbr-bw: ------------>     {12032}
dba-assured-us-bw: ------------->     {0}
dba-max-us-bw: ----------------->     {1000000}
dba-extra-us-bw-type: ---------->     {nonassured}
```

» **Para serviços com 8 portas PWE, o GTP padrão é *1100000007*:**

```
iSH> get gpon-traffic-profile 1100000007
gpon-traffic-profile 1100000007
guaranteed-upstream-bw: ------->     {0}
traffic-class: ----------------->     {ubr}
compensated: ------------------->     {false}
shared: ------------------------>     {false}
dba-enabled: ------------------->     {true}
dba-fixed-us-ubr-bw: ------------>     {0}
```

```
dba-fixed-us-cbr-bw: ----------->     {24000}
dba-assured-us-bw: ------------>      {0}
dba-max-us-bw: ----------------->     {1000000}
dba-extra-us-bw-type: --------->      {nonassured}
```

» **Para serviços com 24 portas PWE, o GTP padrão é *1100000008*:**

```
iSH> get gpon-traffic-profile 1100000008
gpon-traffic-profile 1100000008
guaranteed-upstream-bw: ------->      {0}
traffic-class: ----------------->     {ubr}
compensated: ------------------->     {false}
shared: ------------------------->    {false}
dba-enabled: ------------------->     {true}
dba-fixed-us-ubr-bw: ----------->     {0}
dba-fixed-us-cbr-bw: ----------->     {72000}
dba-assured-us-bw: ------------>      {0}
dba-max-us-bw: ----------------->     {1000000}
dba-extra-us-bw-type: --------->      {nonassured}
```

Neste exemplo, serão adicionados serviços de video para o modelo de serviço *TriplePlay* sem especificar a GEM Port e o GTP.

```
iSH> bridge add tripleplay downlink vlan 203 tagged rg-bridged eth 3 video 0/10
Adding bridge on tripleplay
Created bridge-interface-record 1-0-0-258-gponport-203/bridge GEM 258 is auto-assigned
CPE Connection 1-0-0-258/gponport/12/3/0/0 has been created
```

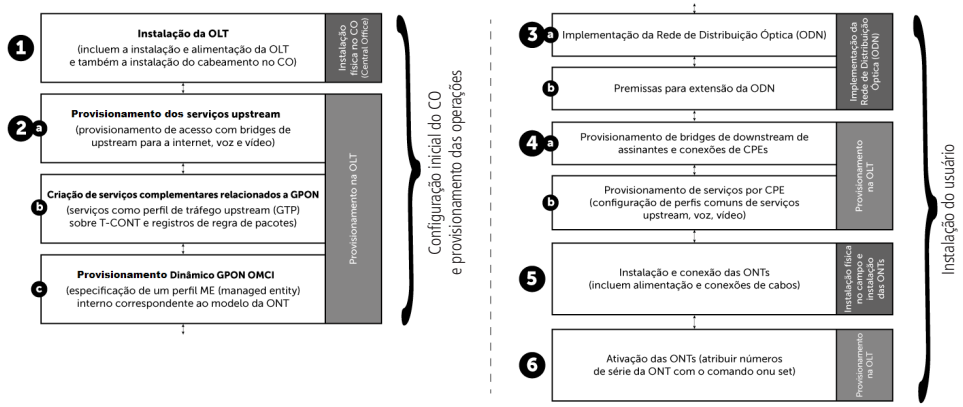
Atribuição manual do GTP

Neste exemplo é criado um serviço de vídeo em bridge de downlink para a ONU 1/1/1 e atribuido o GTP 2 com GEM Port 403.

```
iSH> bridge add 1-1-1-1/gpononu gem 403 gtp 2 downlink vlan 200 tagged video 0/4 eth 2 rg-bridged
Adding bridge on 1-1-1-1/gpononu
Created bridge-interface-record 1-1-1-403-gponport-200/bridge
CPE Connection 1-1-1-403/gponport/12/2/0/0 has been created
```

Provisionamento com OMCI dinâmico (Dynamic OMCI)

A imagem a seguir exibe o fluxograma geral do procedimento de instalação.

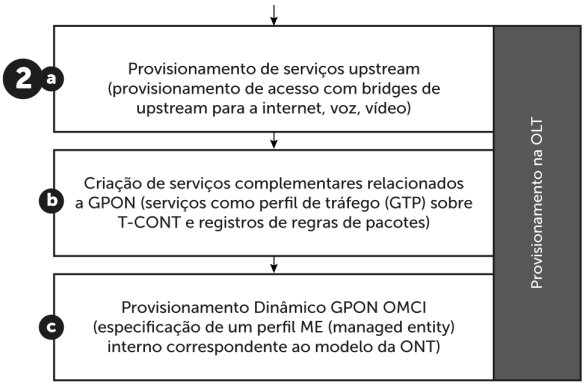


Procedimento de instalação para ONUs com OMCI Dinâmico

Resumo da configuração OMCI dinâmico

Com OMCI Dinâmico é possível utilizar um único comando macro para o provisionamento de bridges e com funções de CPE ao mesmo tempo. Os serviços de voz, vídeo e dados são configurados na OLT e fluem através das ONTs (CPEs).

Perfis ME internos



Perfil ME interno com OMCI Dinâmico

A Intelbras fornece perfis ME internos para as ONTs suportadas. O formato de um perfil interno é *intelbras-modelo-da-ont*.

Como exibido no passo 2c do fluxograma, ao especificar o nome de um perfil ME interno na configuração inicial (utilize o comando *onu set OnuInterface meprof InternalMEProfileName*) em uma ONU, a OLT conhece o modelo dessa ONU e provisionará essa ONU com OMCI Dinâmico. Por exemplo, o perfil ME interno intelbras-1420g define que há 4 portas Ethernet, 2 portas FXS na ONT Intelbras.

Exibindo os perfis ME interno suportados pela OLT 8820 G.

```
iSH> gpononu profile show internal-me
intelbras-110g     1 GE
intelbras-1420g    4 GE + 2 POTS
intelbras-142ng    4 GE + 2 POTS + 1 WiFi(wlan1-wlan4) + 1 USB
```

Os dois procedimentos a seguir exibem como associar ou remover perfis ME interno para uma ONU indivídual ou para um intervalo de ONUs.

Pode utilizar o comando *onu set meprof* para configurar os perfis ME internos da ONT. Depois disso, os atributos suportados pela OMCI são associados à ONT.

```
iSH> onu set 1/1/5 meprof intelbras-1420g

 iSH> onu show 1/1/5
ONU     Name        Enabled    Model #   Number       OMCI files and profiles
5       1-1-1-5     No                               ME        intelbras-1420g
Note: NULL Model String indicates not able to get model ID
```

Para remover o perfil ME interno dessa ONT, utilize o comando *onu set noomci*. Esse comando pode ser utilizado quando não há um intervalo de ONUs atribuído.

```
iSH> onu set 1/1/5 noomci

 iSH> onu show 1/1/5
ONU     Name        Enabled    Model #   Serial Number    OMCI files and profiles
5       1-1-1-5     No                                    (none)
Note : NULL Model String indicates not able to get model ID
```

Intervalos podem ser utilizadas nos comandos *onu set* para configurar ou remover perfis me:

Esse exemplo associa todas as ONUs da porta PON 3 da OLT com o perfil ME intelbras-110.

```
iSH> onu set 1/3 meprof intelbras-110g
iSH> onu set 1/3 noomci
```

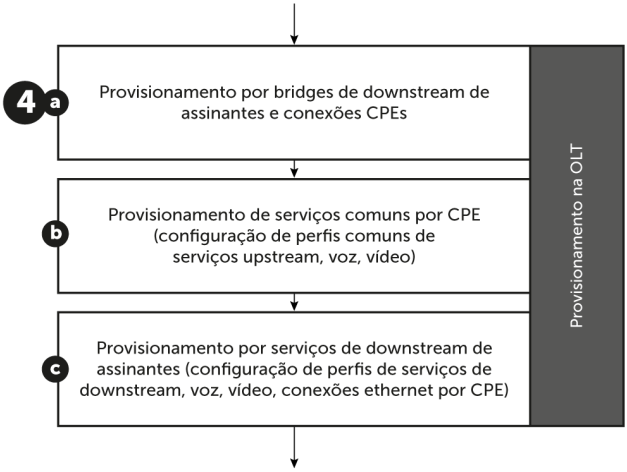
Esse exemplo associa as ONUs que estão na posição 1 a 10 na porta PON 3 com o perfil ME intelbras-142ng.

```
iSH> onu set 1/3/[1-10] meprof intelbras-142ng
iSH> onu set 1/3/[1-10] noomci
```

```
iSH> onu showall 1/3
Processing list of 64
This command may take several minutes to complete.
Do you want to continue? (yes or no) [no] yes
```

ONU	Name	Enabled	Model #	Serial Number	OMCI files and profiles
1	1-1-3-1	No			(none)
2	1-1-3-2	No			(none)
3	1-1-3-3	No			(none)
4	1-1-3-4	No			(none)
5	1-1-3-5	No			(none)
6	1-1-3-6	No			(none)
7	1-1-3-7	No			(none)
8	1-1-3-8	No			(none)
9	1-1-3-9	No			(none)
10	1-1-3-10	No			(none)

Comando bridge add com OMCI dinâmico

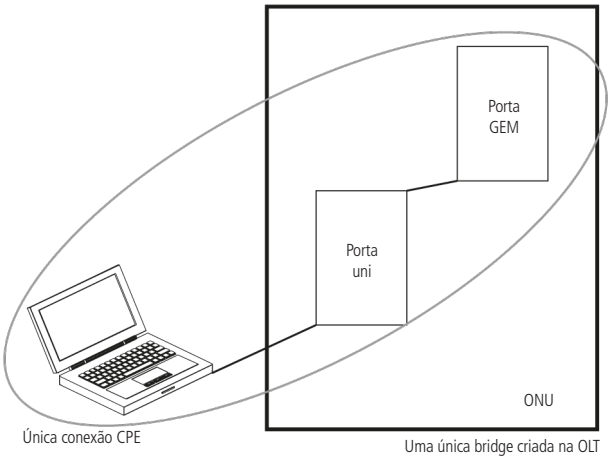


Bridging dinâmica com OMCI Dinâmico

A bridging dinâmica é utilizada no passo 4a do fluxograma. Ele utiliza um único comando macro *bridge add* para criar a bridge na OLT e suas conexões CPE, bem como as definições relativas aos tipos de serviços da bridge.

No OMCI Dinâmico, a bridge da OLT 8820 G e a conexão CPE podem ter mapeamentos um-para-um.

Conforme exibido na imagem a seguir, o mapeamento um-para-um é uma bridge criada em uma GEM Port que é mapeada para uma conexão CPE criada para uma porta da ONU.



O mapeamento um-para-um entre bridges da OLT e Conexões CPE

Criando mapeamento um-para-um entre OLT e conexões CPE

O exemplo a seguir cria um mapeamento um-para-um de uma bridge na OLT com uma conexão CPE.

1. Crie uma bridge da OLT com uma conexão CPE:

```
iSH> bridge add 1-1-1-5/gpononu gem 505 gtp 1 tm 1 downlink vlan 100 tagged eth 1 uni-vlan 100
Adding bridge on 1-1-1-5/gpononu
Created bridge-interface-record 1-1-1-505-gponport-100/bridge
CPE Connection 1-1-1-505/gponport/1/1/100/0 has been created
```

A primeira parte desse comando "bridge add 1-1-1-5/gpononu gem 505 gtp 1 tm 1 downlink vlan 100 tagged" cria uma nova bridge na OLT. A segunda parte desse comando "eth 1 uni-vlan 100" cria uma conexão CPE com essa bridge da OLT. Neste exemplo, os quadros ao sair da porta LAN 1 da ONU serão marcados (tagged).

2. Exiba a bridge da OLT 8820 G e a conexão CPE.

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN    Physical          Bridge                          St Table Data
dwn             Tagged 100   1/1/1/5/gpononu   1-1-1-505-gponport-100/bridge   DWN
upl             Tagged 100   1/1/9/0/eth       1-1-9-0-eth-100/bridge          UP S VLAN 100 default
2 Bridge Interfaces displayed

iSH> bridge show onu
 GEM  ONU      DSCP    ONU UNI       OLT                                  OLT
ONU Port    UNI      to COS VLAN/SLAN  VLAN/SLAN  G-VLAN  MVR  Service Rg-Mode OLT Bridge      ST
1/1/5 505  eth 1  ---   100/----   Tagged  100 ----  ---   data    -----   1-1-1-505-gponport-100/bridge  DWN
1 Bridge Interfaces displayed
1 GPON ONU Connections displayed
```

A tabela a seguir fornece um resumo sobre como adicionar bridges para serviço suportados.

Como exibido na tabela, para serviços VoIP, ao invés da *keyword + UNIport index*, o comando bridge *add* especifica somente a *keyword*, fato que indica que a conexão CPE é criada em todas as portas UNI da ONU relacionadas ao serviço.

Serviços	Bridges	keyword de serviços	Exemplos de comando
Dados	Um comando bridge add por conexão CPE	N/A (Quando nenhuma palavra-chave de serviço for especificada, fica implícito que o serviços é de dados)	bridge add 1-1-1-5/gpononu gem 301 gtp 1 downlink vlan 100 tagged eth 1 (cria serviço de dados na porta ethernet 1 da ONU)
Vídeo	Um comando bridge add por conexão CPE	vídeo	bridge add 1-1-1-5/gpononu gem 401 gtp 1 video 0/4 downlink vlan 999 tagged eth 2 (cria serviço de vídeo na porta ethernet 2 da ONU)
VoIP	Um comando bridge add por ONU	sip	bridge add 1-1-1-5/gpononu gem 702 gtp 1 downlink vlan 300 tagged sip (cria serviço SIP VoIP em todas as portas FXS na ONU)

Bridging dinâmica para serviços

Todos os exemplos de comando exibidos na tabela anterior adicionam uma VLAN a tráfegos sem marcação (untagged) nas portas ethernet da ONU.

Removendo a bridges da OLT 8820 G e as conexões CPE associadas

O exemplo a seguir remove o mapeamento um-para-um da bridge da OLT com a conexão CPE.

Para remover a bridge da OLT e a conexão CPE associada ao mesmo tempo execute:

```
iSH> bridge delete 1-1-1-505-gponport-100/bridge
CPE Connection 1-1-1-505/gponport/1/1/100/0 has been deleted
1-1-1-505-gponport-100/bridge delete complete
```

Instalação de serviços serviços TriplePlay com OMCI dinâmico

» **Criar acesso de banda larga em bridges de uplink e downlink com OMCI dinâmico**

Somente é necessário especificar o perfil ME interno uma única vez para cada ONU.

Somente é necessário ativar a ONU uma única vez.

Nesse exemplo, para serviços de dados, iremos criar bridges de uplink/downlink com VLAN 1001.

Para criar um serviço de dados nas portas Ethernet da ONU, utilize os passos a seguir:

» **Criando um perfil de tráfego GPON**

Os perfis de tráfego GPON são um modelo para definir como o tráfego será gerenciado na bridge e a qual GTP está associado. Um GTP pode estar associado a várias bridges diferentes. O GTP desse procedimento criará uma configuração de banda larga de alta velocidade.

O modelo a seguir é recomendado para configurações de dados em alta velocidade.

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile 1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------>      {0}: 2048 em Kbps
traffic-class: ---------------->      {ubr}: ubr é o valor padrão
compensated: ----------------->      {false}:
shared: ---------------------->      {false}:
dba-enabled: ----------------->      {false}:
dba-fixed-us-ubr-bw: ---------->      {0}:
dba-fixed-us-cbr-bw: ---------->      {0}:
dba-assured-us-bw: ----------->      {0}:
dba-max-us-bw: ---------------->      {0}:
dba-extra-us-bw-type: -------->      {nonassured}:
.................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Especificando o perfil ME interno para a ONU

Com base no modelo da ONU, atribua o perfil ME interno correspondente a ONU. Isso é um modo de indicar que essa ONU é provisionada por OMCI dinâmico.

1. Liste os perfis ME internos atualmente válidos;

```
iSH> gpononu profile show internal-me
intelbras-110g     1 GE
intelbras-1420g    4 GE + 2 POTS
intelbras-142ng    4 GE + 2 POTS + 1 WiFi(wlan1-wlan4) + 1 USB
```

2. Especifique um perfil ME interno para a ONU.

Depois de especificar o perfil ME interno intelbras-1420g para a ONU 1/1/1, o suporte a OMCI Dinâmico é associado a ONU.

```
iSH> onu set 1/1/1 meprof intelbras-1420g
```

Criando bridges de uplink/downlink na OLT e conexões CPE

Essa seção criará bridges de uplink e downlink para VLAN 1001 na OLT, e criará conexões CPE para a mesma VLAN em duas portas Ethernet da ONU:

1. Crie uma bridge interface uplink na OLT;

```
iSH> bridge add 1-1-8-0/eth uplink vlan 1001
Adding bridge on 1-1-8-0/eth
Created bridge-interface-record ethernet8-1001/bridge
bridge-path added successfully
```

2. Crie bridges de downlink na OLT e conexões CPE nas portas Ethernet da ONU;

Esse exemplo exibe o mapa da porta Ethernet 1 da ONU mapeada para a GEM Port 610 na VLAN 1001.

Crie uma bridge na GEM Port 610 e uma conexão CPE na porta Ethernet 1 da ONU. Associe o GTP 1 com a GEM Port 610. Tanto a conexão CPE como a GEM Port estão na mesma VLAN 1001.

```
iSH> bridge add 1-1-1-1/gpononu gem 610 gtp 1 downlink vlan 1001 tagged eth 1 uni-vlan 1001
Adding bridge on 1-1-1-1/gpononu
Created bridge-interface-record 1-1-1-610-gponport-1001/bridge
CPE Connection 1-1-1-610/gponport/1/1/1001/0 has been created
```

3. Visualize as bridges da OLT 8820 G;

```
iSH> bridge show
          Orig
Type VLAN/SLAN     VLAN/SLAN Physical         Bridge                          St Table Data
dwn                Tagged 1001   1/1/1/1/gpononu   1-1-3-610-gponport-100/bridge   UP
upl                Tagged 1001   1/1/8/0/eth       1-1-8-0-eth-1001/bridge         UP S VLAN 1001 default
1001 default
2 Bridge Interfaces displayed
```

4. Visualize as conexões CPE.

```
iSH> bridge show onu
GEM  ONU     DSCP   ONU UNI      OLT                              OLT
ONU Port   UNI     to COS VLAN/SLAN   VLAN/SLAN     G-VLAN  MVR  Service Rg-Mode  OLT Bridge            ST
1/3/1 610  eth 1  -----  1001/----  Tagged  1001  ----  ----  data  -------  1-1-1-610-gponport-1001/bridge  DWN
1 Bridge Interfaces displayed
1 GPON ONU Connections displayed
```

Ativando a ONT

Ative a ONT para adicioná-la ao sistema. Ao utilizar OMCI Dinâmico e alterar as configurações de serviço em uma ONU ativada, as configurações serão atualizadas automaticamente.

1. Para ativar uma ONT, primeiro execute o comando *onu show* para exibir as ONT presentes na OLT e descobrir os números de série disponíveis;

O comando *onu show* possui opções para selecionar uma porta PON específica da OLT. Ao executar o comando sem definir a porta PON, o comando buscará por ONTs em cada porta PON, podendo levar um certo tempo para a finalização do comando.

```
iSH> onu show 1/3
Free ONUs for slot 1 olt 3:
1     2     3     4     5     6     7     8     9     10    11    12
13    14    15    16    17    18    19    20    21    22    23    24
25    26    27    28    29    30    31    32    33    34    35    36
37    38    39    40    41    42    43    44    45    46    47    48
49    50    51    52    53    54    55    56    57    58    59    60
61    62    63    64
Discovered serial numbers for slot 1 olt 3:
sernoID     Vendor      Serial Number     Model       Time discovered
1           ZNTS        035C13CE          110g        MAR 23 22:28:45 2015
2           ZNTS        035C7533          1420g       MAR 23 22:28:50 2015
3           ZNTS        035C779F          142ng       MAR 23 22:29:20 2015
```

2. Execute o comando onu set para associar um ONU port ID a um número de série de uma ONT desejada:

```
iSH> onu set 1/3/1 1
Onu 1 successfully enabled with serial number ZNTS 93425008
```

3. Execute o comando *onu show* para verificar se a ONT está ativada, e se o suporte OMCI foi adicionado à ONT (o perfil ME interno associado poderá ser exibido);

```
iSH> onu show 1/3/1
ONU     Name        Enabled    Model #   Serial Number   OMCI files and profiles
1       1-1-3-1     Yes        110G      ZNTS 035C13CE   ME  intelbras-110g
Observação: NULL Model String indicates not able to get model ID
```

4. Execute o comando *onu status* para verificar se o status de configuração OMCI está ativo.

```
iSH> onu status 1/3/1
ID      Onu     OperStatus  ConfigState  Download State  OLT Rx Power  ONT Rx Power  Distance (km)  GPON OnuStatus
1     1-1-3-1       Up         Active      NoUpgrade     -19.2 dBm     -20.0 dBm       18          Active
```

Criação de bridges de uplink e downlink para serviços de vídeo com OMCI dinâmico

A bridging de vídeo é similar a bridging de dados, que utiliza bridges de uplink e downlink, mas as GEM Ports, GTP e VLAN são diferentes. Durante a configuração dos serviços de dados, o nome do perfil ME interno já está especificado na ONU, portanto se o serviço de vídeo for configurado na mesma ONU, não é preciso especificar novamente o nome do perfil ME interno.

Para criar um serviço de vídeo nas portas Ethernet da mesma ONU, utilize os passos a seguir:

Criando um perfil de tráfego GPON

Adicione o perfil de tráfego GPON.

O perfil de tráfego GPON a seguir é recomendado para vídeo:

```
iSH> new gpon-traffic-profile 2
gpon-traffic-profile 2
Please provide the following: [q]uit.
guaranteed-upstream-bw: ----->       {0}: 512
traffic-class: --------------->         {ubr}:
compensated: ----------------->         {false}:
shared: ---------------------->         {false}:
dba-enabled: ----------------->         {false}:
dba-fixed-us-ubr-bw: --------->         {0}:
dba-fixed-us-cbr-bw: --------->         {0}:
dba-assured-us-bw: ----------->         {0}:
dba-max-us-bw: --------------->         {0}:
dba-extra-us-bw-type: ------->       {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Criando bridges de Uplink/Downlink e conexões CPE

Essa etapa será criada uma bridge de uplink e downlink para VLAN 999:

1. Crie uma bridge interface de uplink:
   a. Crie a bridge interface de uplink.

      O exemplo a seguir cria uma bridge de vídeo de uplink e ativa o IGMP Proxy com IGMP snooping.

```
iSH> bridge add 1-1-4-0/eth uplink vlan 999 tagged igmpproxy
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record 1-1-4-0-eth-999/ bridge
Bridge-path added successfully
```

   b. Modifique A bridge-path da bridge de uplink com 30 segundos de intervalo de pesquisa IGMP.

```
iSH> bridge-path modify 1-1-4-0-eth-999/bridge vlan 999 default igmptimer 30
```

2. Criar as bridges interfaces de downlink e conexões CPE nas portas Ethernet da ONU;

Crie bridges de downlink em uma GEM Port e ONU com VLAN ID e GTP.

Também pode especificar *video m/n. m* indica a lista de controle multicast na bridge da OLT, e *n* indica o número máximo de streaming de vídeo permitido na bridge. O streaming máximo de vídeo é um campo obrigatório ao criar uma bridge de downlink para serviços de vídeo, caso contrário a bridge falhará na transmissão do tráfego multicast de vídeo. Especificando *video 0/4* conforme exemplo,será possível até quatro streamings de vídeo na bridge interface da OLT sem verificação de lista de controle.

Esse exemplo adiciona VLAN 999 ao tráfego de vídeo sem marcação.

```
iSH> bridge add 1-1-3-1/gpononu gem 650 gtp 2 downlink vlan 999 tagged video 0/4 eth 3
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record 1-1-3-650-gponport-999/bridge
CPE Connection 1-1-3-650/gponport/12/3/0/0 has been created
```

3. Visualize as bridges da OLT;

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN      Physical          Bridge                              St Table Data
dwn              Tagged 999    1/1/3/1/gpononu   1-1-3-650-gponport-999/bridge       UP
dwn              Tagged 1001   1/1/3/1/gpononu   1-1-3-610-gponport-1001/bridge      UP
upl              Tagged 999    1/1/4/0/eth       ethernet4-999/bridge                UP S VLAN 999 default
upl             Tagged 1001    1/1/8/0/eth       ethernet5-1001/bridge               UP S VLAN 1001 default
4 Bridge Interfaces displayed
```

4. Visualize as conexões CPE;

```
iSH> bridge show onu
       GEM   ONU     DSCP    ONU UNI OLT            OLT
ONU    Port  UNI     to COS VLAN/SLAN VLAN/SLAN     MVR  Service OLT Bridge                    ST
1/3/1  610   eth 1          1001/     Tagged 1001   data      1-1-3-610-gponport-1001/bridge  UP
1/3/1  650   eth 3                    Tagged 999    iptv      1-1-3-650-gponport-999/bridge   UP
2 Bridge Interfaces displayed
1 GPON ONU Connections displayed
```

5. Visualize os serviços CPE na ONT desejada.

```
iSH> CPE show 1/3/1

CPE 1/3/1
Service: DATA
GEM    UNI      UNI VLAN/SLAN    OLT VLAN/SLAN    Admin Oper   Rg-Mode
610    eth 1    1001/----        Tagged 1001      up           down

Service: IPTV
GEM    UNI      UNI VLAN/SLAN    OLT VLAN/SLAN    Admin Oper   Video Prof
650    eth 3                     Tagged 6, 999    up           down      1 6 is the Video CoS value
```

Criando um perfil CPE de controle de acesso a vídeo (opcional)

O perfil de controle de acesso a vídeo cria uma lista de controle de acesso, que define quais endereços multicast de vídeo podem ser acessados pelo dispositivo final. Essa lista de controle de acesso pode ser especificada posteriormente no perfil de vídeo. Se não há perfis de controle de acesso a vídeo especificados, nenhum controle de endereço multicast será realizado.

> **Observação:** o perfil de controle de acesso a vídeo não poderá ser removido se esse perfil estiver associada a uma bridge de vídeo

Para criar um novo perfil de acesso a vídeo, utilize o comando a seguir:

cpe video access add *<list-name>*
[src-ip *<IPAddress>***]**
[st-ip-start *<IPAddress>***]**
[dst-ip-end *<IPAddress>* **]**
[imputed-group-bw *<value in bytes/sec>***]**

A tabela a seguir fornece a descrição das opções do comando cpe video access add.

Opção	Descrição
list-name	Nome do perfil de controle de acesso a vídeo.
src-ip IPAddress	Endereço IP de origem. O valor padrão é *0.0.0.0*, fato que indica que o endereço IP de origem deve ser ignorado.
dst-ip-start IPAddress	Endereço IP de destino inicial da faixa de endereços multicast bloqueado.
dst-ip-end IPAddress	Endereço IP de destino final da faixa de endereços multicast bloqueado.
imputed-group-bw value	Largura de banda (bytes/segundos) de entrada ao grupo multicast. A largura de banda de entrada é utilizada para decidir se acatar ou não uma solicitação de Join na presença de um limite máximo de largura de banda multicast. O valor padrão *0* possibilita efetivamente a entrada na tabela, afim de evitar limitações máximo de largura de banda.

Descrição das opções do comando cpe video acess add

Esse exemplo cria dois perfis de controle de acesso a vídeo, cada perfil é um registro de uma lista de controle de acesso a vídeo:

1. Crie um perfil de controle de acesso a vídeo;

```
iSH> CPE> VIDEO> ACCESS> add basic-plan dst-ip-start
224.10.10.1 dst-ip-end 224.10.10.15 imputed-group-bw
4000
Profile has been created with index 1/1
```

O primeiro perfil de controle de acesso a vídeo no sistema é criado automaticamente com list-index 1/list-entry 1.

2. Crie o segundo perfil de controle de acesso a vídeo na mesma lista (1/2):

```
iSH> CPE> VIDEO> ACCESS> add basic-plan dst-ip-start
224.11.10.1 dst-ip-end 224.11.10.4 imputed-group-bw
4000
Profile has been created with index 1/2
```

3. Visualize os dois perfis cpe-video-access-control presentes na mesma lista;
   Pode especificar list-name ou list-index.

```
iSH> CPE> VIDEO> ACCESS> show 1
List/Entry Index     Profile Name      dstIpStart                  dstIpEnd       imputedGroupBw
1/1                                    basic-plan 224.10.10.1 224.10.10.15        4000
1/2                                    basic-plan 224.11.10.1 224.11.10.4         4000
2 entries found.
```

4. Se os usuários desejam eliminar um perfil cpe-video-access-control, utilize o comando *cpe video access delete <list-name | list-index> / <entry-index>;*

```
iSH> CPE> VIDEO> ACCESS> delete 1/1
Profile has been deleted.
```

Criação de bridges de uplink e downlink para serviços de voz com OMCI Dinâmico

Para serviços VoIP, recomendamos a utilização de bridges de uplink e de downlink.

> **Observação:** uma ONU somente pode ter um tipo de sinalização VoIP. Por exemplo, ao configurar a porta FXS 1 com uma configuração SIP, a outra porta FXS utilizará a mesma configuração SIP

Para criar um serviço de voz nas portas FXS, utilize os passos a seguir:

Criando um perfil de tráfego GPON

Adicione o perfil de tráfego GPON.

O perfil de tráfego GPON a seguir é recomendado para até quatro telefones VoIP ou quatro portas FXS.

```
iSH> new gpon-traffic-profile 3

gpon-traffic-profile  3
Please provide the following:[q]uit.
guaranteed-upstream-bw: ------->      {0}: 512
traffic-class: ----------------->      {ubr}:
compensated: ------------------->      {false}:
shared: ------------------------>      {false}:
dba-enabled: ------------------->      {false}:
dba-fixed-us-ubr-bw: ------------>     {0}:
dba-fixed-us-cbr-bw: ------------>     {0}:
dba-assured-us-bw: ------------->      {0}:
dba-max-us-bw: ----------------->      {0}:
dba-extra-us-bw-type: ---------->      {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Criando bridges de Uplink/Downlink e conexões CPE

Esta etapa irá criar uma bridge de uplink e uma de downlink na OLT, e criará uma conexão CPE na ONU para serviços SIP:

1. Crie uma bridge de uplink na interface de uplink;

```
iSH> bridge add 1-1-4-0/eth uplink vlan 300 tagged
Adding bridge on 1-1-4-0/eth
Created bridge-interface-record ethernet4-300/bridge
Bridge-path added successfully
```

2. Crie uma bridge de downlink na interface de downlink e crie uma conexão CPE para todas as portas FXS da ONU;

Esse exemplo cria uma bridge de downlink com GEM Port 710, cria um serviço SIP para todas as portas FXS da ONU 1/3/1 na VLAN 300.

```
iSH> bridge add 1-1-3-1/gpononu gem 710 gtp 3 downlink vlan 300 tagged sip
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record 1-1-3-710-gponport-300/bridge
CPE Connection 1-1-3-710/gponport/14/0/0/0 has been created
```

3. Na OLT, execute o comando bridge *show* para visualizar as bridges configuradas na OLT;

```
iSH> bridge show
          Orig
Type VLAN/SLAN VLAN/SLAN      Physical          Bridge                          St Table Data
dwn            Tagged 300     1/1/3/1/gpononu   1-1-3-710-gponport-300/bridge   UP
dwn            Tagged 999     1/1/3/1/gpononu   1-1-3-650-gponport-999/bridge   UP
dwn            Tagged 1001    1/1/3/1/gpononu   1-1-3-610-gponport-1001/bridge  UP
upl            Tagged 300     1/1/4/0/eth       ethernet4-300/bridge            UP
upl            Tagged 999     1/1/4/0/eth       ethernet4-999/bridge            UP S VLAN 999 default
upl            Tagged 1001    1/1/8/0/eth       ethernet8/bridge                UP S VLAN 1001 default
6 Bridge Interfaces displayed
```

4. Visualize as conexões CPE.

```
iSH> bridge show onu
        GEM    ONU      DSCP    ONU UNI OLT             OLT
ONU     Port   UNI      to COS VLAN/SLAN VLAN/SLAN     MVR  Service OLT Bridge                 ST
1/3/1   610    eth 1           1001/    Tagged 1001    data 1-1-3-610-gponport-1001/bridge    UP
1/3/1   650    eth 3                    Tagged 999     iptv 1-1-3-650-gponport-999/bridge     UP
1/3/1   710    pots                     Tagged 300     sip  1-1-3-710-gponport-300/bridge     UP
3 Bridge Interfaces displayed
3 GPON ONU Connections displayed
```

Criando um perfil CPE IP-COM para voz (opcional)

O perfil CPE IP-COM padrão especifica um cliente DHCP como opção no campo *host IP option*. Isso indica que a ONU obterá o endereço IP automaticamente de um servidor DHCP.

Observação: o perfil IP-COM somente poderá ser removido quando não estiver associado a nenhum perfil CPE IP

Comando:

```
cpe <voip> ip ip-com add <profile-name>
[ host-ip-option < dhcp | static | unconfigured > ]
[ netmask < value > ]
[ gateway < IP address > ]
[ primary-dns < IP address > ]
[ secondary-dns < IP address > ]
[ mtu < value > ]
[ default-iface < true | false > ]
[ dns-src < true | false > ]
[ dns-type < default | static | proxy > ]
```

Opção	Descrição
profilename	Especifica um nome exclusivo do perfil IP-COM.
host-ip-option <dhcp| static >	Selecione a forma de obtenção do endereço IP, dhcp ou static. DHCP é a opção padrão, isto informa que a ONT obterá o endereço IP automaticamente do servidor DHCP, caso for static, deverá ser inserido um endereço IP manualmente.
netmask <value>	Especifica a máscara de sub-rede utilizada pelo serviço de voz.
gateway <IP address>	Especifica o endereço do gateway padrão utilizado para serviços de voz. Esse atributo possui o valor padrão *0.0.0.0*.
primary-dns <IP address>	Especifica o endereço IP de DNS primário. Se o valor é 0.0.0.0, não há um SIP DNS primário definido. O valor padrão é *0.0.0.0*.
secondary-dns <IP address>	Especifica o endereço IP DNS secundário. Se o valor é 0.0.0.0, não há um SIP DNS secundário definido. O valor padrão é *0.0.0.0*.
mtu < value >	MTU (Maximum Transmission Unit). Esta opção permite que a OLT defina o tamanho máximo do pacote IP (em bytes) que pode ser transmitido sem fragmentação. Valores: 0 para 1540 Padrão: *1500*.
default-iface < true | false >	Quando verdadeiro, um pacote gerado internamente (por exemplo, traps SNMP, SNTP, etc) é enviado através desta interface se o endereço IP de destino não está definido na tabela de roteamento. Padrão: *false*.
dns-src < true | false >	Quando verdadeiro, a interface é utilizada pelo cliente DHCP para obtenção das informações de DNS.
dns-type < default | static | proxy >	Default - Obtem as informações de DNS a partir da interface WAN. Static - As informações de DNS será configurada estaticamente. Proxy - Habilita a interface para agir como um proxy para pedidos de DNS. Padrão: *default*.

Opções e descrição do comando cpe ip-com add

O exemplo a seguir cria um perfil IP-COM para serviços de voz:

1. Crie um perfil IP-COM. O índice do perfil será gerado automaticamente;

```
iSH> CPE> VOIP> IP> IP-COM> add IPserver host-ip-option static netmask
255.255.255.0 gateway 172.168.3.254 primary-dns 172.168.19.1

Profile "IPserver" has been created with index 2
```

2. Exiba os perfis IP-COM padrão e os perfis IP-COM criados manualmente;

```
iSH> CPE> VOIP> IP> IP-COM> show all

                                host IP                    igmp          secure  default
Index  Profile Name              option   gateway           fn     nat     fwd    iface    dns  src  dns  type
1      Default_Cpe_Ip_Server      dhcp          0.0.0.0     none   nat    disabl  false          false     default
2      IPserver                 static    172.168.3.254    none   nat    disabl  false          false     default
```

3. Para remover um perfil IP-COM, utilize o comando delete juntamente com o índice ou nome do perfil IP-COM desejado.

```
iSH> CPE> IP> IP-COM> delete IPserver
Profile has been deleted.
```

Criando um perfil CPE IP para serviços VoIP e associando a um perfil IP-COM (opcional)

Crie um perfil IP para o serviço VoIP e associe-o a um perfil IP-COM. Caso nenhum perfil IP-COM seja especificado, será utilizado o perfil IP-COM padrão.

Comando:

cpe voip ip add *<interface>*
[host-ip *< IP address >]*
[ip-com *< index | profile-name >]*

Opção de comando	Descrição
Interface	Especifica a ONU (ONU interface ID).
host-ip <IP address>	Especifica o endereço IP utilizado pelo servico. O endereço padrão é *0.0.0.0*.
ip-com <index| profile-name>	Associa um perfil IP-COM a esse host IP. Se o campo não for especificado, será utilizado o perfil IP-COM padrão com índice 1 (que possui a opção DHCP cliente ativado).

Opções e descrições do comando cpe ip add

1. Crie um perfil IP para o serviço VoIP;

```
iSH> CPE> VOIP> IP> add 1/3/1
Service has been created
```

Será utilizado o perfil IP-COM padrão.

2. Exiba os perfis CPE IP;

```
iSH> CPE> VOIP> IP> show all

CPE     Service       host IP      IP Com Profile
1/3/1   VOIP          0.0.0.0            1
1 services displayed
```

3. Remova o perfil IP configurado.

```
iSH> CPE> VOIP> IP> delete 1/3/1
Service has been deleted.
```

Criando um perfil CPE VOIP SERVER com parâmetros do servidor VoIP

Esta etapa criará um perfil voip server com informações do servidor VoIP. Cada perfil voip server configurado, especifica os endereços IP ou nomes dos servidores VoIP primários e secundários, assim como o protocolo de sinalização VoIP utilizado.

Observação: o perfil voip server somente poderá ser removido quando não estiver associada a nenhum perfil de assinante

Comando:

cpe voip server add *<profile-name>*
[primary-server *< 64 byte character string >]*
[secondary-server *< 64 byte character string >]*
[signalling-protocol < sip | siplar | h248 >]
[sip-domain *< linha de caracteres de 64 byte>]*

[sip-registrar *< linha de caracteres de 64 byte>]*

[mgc-termination-id-base *< linha de caracteres de 25 byte>]*

[oob-dtmf-events < enabled | disabled >]

[oob-cas-events < enabled | disabled >]

[softswitch *< código de vendedor de 4 byte>]*

[outbound-server *< linha de caracteres de 255 byte>]*

[port-id *< 2 byte, padrão -1 >*

[dtmf-events-passing-method <rfc4733 | sipinfo >]

[cas-events-passing-method <rfc4733 | sipinfo >]

[rtp-dscp < 0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef >][signalling-dscp < 0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef >][sip-reg-exp-time][sip-rereg-head-start-time] [sip-reg--retry-time] [release-timer][roh-timer][mgcp-client-address-mode <ip | ipbracket | domainname>]

[mgcp-persistent-notify<enabled | disabled>][pbx-number *<0-9>***]**

A tabela a seguir fornece a descrição das opções do comando comando *cpe voip server add.*

Opção	Descrição
profilename	Especifica um nome exclusivo para o perfil voip server
primary-server value	Contém o nome (endereço IP ou nome resolvido) do servidor proxy SIP primário que controla as mensagens de sinalização
secondary-server value	Contém o nome (endereço IP ou nome resolvido) do servidor proxy SIP secundário que controla as mensagens de sinalização
signalling-protocol < sip |siplar | h248 >	Especifica o protocolo de sinalização VoIP. Por padrão, é *h248*
sip-domain < 64 byte character string	Contém o nome (endereço IP ou nome resolvido) do servidor SIP de registro para os usuários conectados a essa ONT
sip-registrar < 64 byte character string >	Contém o nome (endereço IP ou nome resolvido) do servidor de registro para mensagens de sinalização SIP
mgc-termination-id-base < 25 byte character string	Especifica a string de base para o id de terminação física H.248 dessa ONT. Essa string está destinada somente para identificar uma ONT. Os identificadores de terminação específica dos fabricantes são adicionados opcionalmente a essa string para identificar a terminação de uma ONT específica
oob-dtmf-events < enabled | disabled >	Quando oob-dtmf-events está em habilitado, sinais DTMF (Dual-Tone Multi-Frequency) são transmitidos via RTP ou pelo protocolo de sinalização associado. Quando está desabilitado, o tom DTMF é transmitidos por fluxos PCM, e as configurações de dtmf-events-passing-method são ignoradas. *Disabled* é o valor padrão
oob-cas-events < enabled | disabled >	Quando oob-dtmf-events está em habilitado, sinais DTMF (Dual-Tone Multi-Frequency) são transmitidos via RTP ou pelo protocolo de sinalização associado. Quando está desabilitado, o tom DTMF é transmitidos por fluxos PCM, e as configurações de dtmf-events-passing-method são ignoradas. *Disabled* é o valor padrão
softswitch < 4 byte vendor code >	Define o fabricante do SoftSwitch (gateway SIP). O formato é de quatro caracteres alfabéticos de codificação ASCII [A..Z]. Por padrão é utilizado o *metaswitch.* A seguir temos a lista dos códigos SoftSwitch de 4 caracteres suportados. AX2K: Axtel CS2K BSFT: Broadsoft CRPK: Cirpack CCOM : CopperCom ERIC: Ericsson GBND: GenBand G6 HWEI: Huawei SoftX3000 META: Metaswitch NSHQ: Nokia Siemans HiQ NTEL: Nortel CS1500 / GenBandC15, Nortel CS2K / GenBandCS20 NTWK: Network Only OSER: OpenSer TRUA: TaquaT7000 UTSI: UT StarCom URAL: Huawei IMS VXTL: VixTel
outbound-server < 4255 byte character string>	Contém o nome (endereço IP ou nome resolvido) do servidor proxy de saída para mensagens de sinalização SIP

port-id < 2 bytes, default -1>	Esse atributo especifica o número da porta TCP/UDP do protocolo VoIP. O valor padrão *-1* seleciona o número de porta padrão para o protocolo VoIP. É 2944 para H.248 e 5060 para SIP
dtmf-events-passing-met hod <rfc4733 | sipinfo>	Se dtmf-events-passing-method = rfc4733, os dígitos DTMF são transportados no payload RTP. *rfc4733* é o valor padrão. Se dtmf-events-passing-method = sipinfo, os dígitos DTMF são transportados ao longo do caminho de sinalização nas mensagens INFO
cas-events-passing-meth od <rfc4733 | sipinfo>	Se cas-events-passing-method = rfc4733, os dígitos Channel-Associated Signaling (CAS) são transportados no payload RTP. *rfc4733* é o valor padrão. Se cas-events-passing-method = sipinfo, os dígitos CAS são transportados ao longo do caminho de sinalização nas mensagens INFO
rtp-dscp <0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef>	Define o valor DSCP para streams RTP associados ao Servidor Voip
signalling-dscp <0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef>	Define o valor DSCP para mensagens de sinalização sip associadas ao servidor VoIP
sip-reg-exp-time	Tempo em segundos para encerramento do registro SIP. Se o valor é 0, não há encerramento nem nova tentativa de registro. O padrão é *3600*
sip-rereg-head-start-time	Tempo em segundos antes do encerramento de sessão que faz que o agente SIP comece iniciar o processo de re-registro. O padrão é *360*
sip-reg-retry-time	Tempo para nova tentativa de registro SIP em segundos. O padrão é *60*
release-timer	Tempo de liberação em segundos. O valor 0 especifica que a ONT deve utilizar temporizador padrão interno. O padrão é *10* segundos
roh-timer	Esse atributo define o tempo em segundos para a condição de recepção off hook antes que o tom ROH seja aplicado. O valor 0 desativa a cronometragem ROH. O valor padrão é *15 segundos*
mgcp-client-address-mo de <ip | ipbracket | domainname>	Ip e ipbracket fará com que o nome do cliente MGCP seja o endereço IP do host de voz. domainname permitirá ao usuário inserir qualquer linha de texto, normalmente um nome de domínio. Valor padrão: *IP*
mgcp-persistent-notify<enabled | disabled>	Quando habilitado, todos os eventos switchhook serão encaminhados ao switch sem importar qual switch foi solicitado. Quando desabilitado, apenas o evento solicitado pelo switch será encaminhado

Opções e descrições do comando cpe voip server add

Para criar perfis de voip server, utilize o comando *cpe voip server add*.

1. Esse exemplo cria um perfil voip server para um servidor VoIP SIP;

```
iSH> CPE> VOIP> SERVER> add metaswitch-sip primary-server 172.16.60.51
signalling-protocol sip sip-registrar 172.16.60.51
Profile "metaswitch-sip" has been created with index 1
```

2. Ative oob-dtmf-events, e coloque dtmf-events-passing-method em sipinfo;

```
iSH> CPE> VOIP> SERVER> modify 1 oob-dtmf-events enabled dtmf-events-
passing-method sipinfo
Profile has been modified.
```

3. Ative oob-cas-events, e coloque cas-events-passing-method em sipinfo;

```
iSH> CPE> VOIP> SERVER> modify 1 oob-cas-events enabled cas-events-passing-method sipinfo
Profile has been modified.
```

4. Exiba o perfil de servidor VoIP.

```
iSH> CPE> VOIP> SERVER> show metaswitch-sip
                    Signalling   Oob Dtmf   Oob Cas     Dtmf Events       Cas Events
Index   Profile Name    Protocol    Events     Events     Passing Method    Passing Method
1      metaswitch-sip   sip       enabled    disabled       sipinfo        rfc4733
Primary Server          : 172.16.60.51
Secondary Server        : 0.0.0.0
Sip Domain              :
Sip Registrar           : 172.16.60.51
Mgc Termination Id Base :
Softswitch              :
OutBound Server         :
Port Id                 : -1
Rtp Dscp                : 0
Signalling Dscp         : 0
Sip Reg Exp Time        : 3600
Rereg Head Start Time   : 360
Sip Reg Retry Time      : 60
Release Timer           : 10
Roh Timer               : 15
MGCP Address Mode       : ip
MGCP Persistent Notify  : disabled
PBX Number              : 9
1 entries found.
```

Criando um perfil CPE DIALPLAN para um servidor VOIP (opcional)

Os planos de discagem são utilizado apenas para serviços SIP. É possível criar até 30 planos de discagem para cada servidor VoIP.

Comando:

cpe voip dialplan add < server-index | server-profile-name >
[dial-plan-format < h248 | nsc | vendor-specific >]
[**dial-plan** < 25 character string >]

Opção	Descrição
profilename	Especifica um nome exclusivo de perfil dialplan.
dial-plan-format <h248| nsc | vendor-specific >	Define o formato padrão do plano de discagem suportado na ONT para o serviço VoIP. pode ser h248, nsc ou vendor-specific. O valor padrão é *h248*.
dial-plan < 25 character string >	Define o plano de discagem utilizado pelo serviço VoIP.

Opções e descrições do comando cpe sip dialplan add

1. Crie o primeiro perfil de plano de discagem SIP para o servidor SIP VoIP 1;

```
iSH> CPE> VOIP> DIALPLAN> add 1 dial-plan 1xx|[2-7]xxxxxx
Profile has been created with index 1/1
```

2. Crie o segundo perfil de plano de discagem SIP para o mesmo servidor SIP VoIP 1;

```
iSH> CPE> VOIP> DIALPLAN> add 1 dial-plan xx.T|*xx.T
Profile has been created with index 1/2
```

3. Exiba todos os planos de discagem SIP.

```
iSH> CPE> VOIP> DIALPLAN> show all
Index             dial-plan-format     dial-plan
1/1               h248                 1xx|[2-7]xxxxxx
1/2               h248                 xx.T|*xx.T
2 entries found.
```

Criando um perfil CPE FEATURES para um servidor SIP

Crie um perfil de features (funções) para o serviço VoIP. Os perfis de funções VoIP utilizam o formato bitmap.

> **Observação:** o perfil de funções somente é aplicável para um servidor VoIP SIP

> **Observação:** o perfil de funções somente poderá ser removido quando não estiver associado a nenhum perfil de assinante VoIP

Comando:

cpe voip features add *<profile-name>*

[announcement-type *<silence | reordertone | fastbusy | voice | na >***]**

[cid-features < calling-number | calling-name | cid-block | cid-number | cid-name | anonym-block | all | none >][call-waiting-features < calling-waiting | cid-announcement | all | none >][call-progress-or-transfer-features < 3-way | call-transfer | call-hold | call-park | do-not-disturb | flash-on-emergency | emgergency-hold | 6-way | all | none>][call-presentation-features < msg-wait-splash-ring | msg-wait-special-dial-tone | msg-wait-visual | call-fwd | all | none>][hotline < disabled | hot | warm>] [hotline-number <*PhoneNumber***>]**

[warmline-timer <*Timer***>]**

Opção	Descrição
profilename	Especifica um nome para o perfil voip features.
announcement-type < silence | reordertone| fastbusy | voice| na>	Especifica o tratamento quando um assinante tira o telefone do gancho, mas não faz uma ligação. Padrão: *reordertone*
cid-features <calling-number| calling-name| cid-blocking| cid-number | cid-name | anonym-block | all | none>	Especifica o bit map das características da identificação de chamadas. Padrão: *Todos os itens são habilitados*
call-waiting-features < call-waiting | cid-announcement | all | none >	Especifica o bit map das características de chamada em espera. Padrão: *Todos os itens são habilitados*
call-progress-or-transfer-features < 3-way | call-transfer | call-hold | call-park |do-not-disturb | flash-on-emergency | emergency-hold | 6-way | all | none >	Especifica o bit map das características de processamento de chamadas. Padrão: *Todos os itens são habilitados*
call-presentation-features < msg-wait-splash-ring | msg-wait-special-dial-tone | msg-wait-visual | call-fwd | all | none >	Especifica o bit map das características de apresentação de chamada. Padrão: *Todos os itens são habilitados*
hotline < disabled | hot | warm >	Quando a hotline está ativa, o telefone discará imediatamente o número de telefone da hotline. Quando a hotline estiver ociosa, o telefone esperará pelo período especificado no warmline-timer em ms antes de discar automaticamente o número da hotline. Padrão: *disabled*
hotline-number <PhoneNumber>	O número discado automaticamente por esse telefone se a função hotline ou warmline está ativada.
warmline-timer <Timer >	O período de espera antes da warmline discar automaticamente o número de telefone. A unidade de medição é milissegundos. Padrão: *200*

Opções e descrições do comando cpe voip features add

1. Adicione um perfil de funções VoIP. Especificando somente o campo profile-name, o perfil será criado com todas as configurações padrão;

```
iSH> CPE> VOIP> FEATURES> add featureslist1
Profile "featurelist1" has been created with index 2
```

2. Exiba todos os perfis de funções VoIP, incluindo os perfis padrão e os perfis criados pelo usuário;

```
iSH> CPE> VOIP> FEATURES> show all
```

cpe-voip-features 1	Name: Default_Cpe_Voip_Features		Type: reordertone
Caller ID Features	Call Waiting Features	Call Progress or Transfer Features	Call Presentation Features
calling-number	call-waiting	3-way	msg-wait-splash-ring
calling-name	cid-announcement	call-transfer	msg-wait-special-dial-tone
cid-blocking		call-hold	msg-wait-visual
cid-number		call-park	call-fwd
cid-name		do-not-disturb	
anonym-block		flash-on-emergency	
		emergency-hold	
		6-way	

cpe-voip-features 2	Name: featurelist1		Type: reordertone
Caller ID Features	Call Waiting Features	Call Progress or Transfer Features	Call Presentation Features
calling-number	call-waiting	3-way	msg-wait-splash-ring
calling-name	cid-announcement	call-transfer	msg-wait-special-dial-tone
cid-blocking		call-hold	msg-wait-visual
cid-number		call-park	call-fwd
cid-name		do-not-disturb	
anonym-block		flash-on-emergency	
		emergency-hold	
		6-way	

3. Modifique o perfil de funções VoIP;

» Para remover um valor bit map, coloque um símbolo de subtração antes do argumento. Por exemplo: "-calling-name" remove os valores calling-name em cid-features.

» Para remover todas as funções de um bit-map, utilize a palavra-chave "none".

» Para ativar todas as funções de um bit-map, utilize a palavra-chave "all".

```
iSH> CPE> VOIP> FEATURES> modify featurelist1 cid-features -calling-name
call-waiting-features none call-progress-or-transfer-features all
call-presentation-features -call-fwd hotline warm hotline-number 7777437
warmline-timer 3000
Profile has been modified.
```

4. Exiba o perfil de funções CPE VoIP.

```
iSH> CPE> VOIP> FEATURES> show featurelist1
```

cpe-voip-features 2	Name: featurelist1		Type: reordertone
hotLine: warm	hotline-number: 7777437		warmline-timer: 3000
Caller ID Features	Call Waiting Features	Call Progress or Transfer Features	Call Presentation Features
calling-number		3-way	msg-wait-splash-ring
cid-blocking		call-transfer	msg-wait-special-dial-tone
cid-number		call-hold	msg-wait-visual
cid-name		call-park	
anonym-block		do-not-disturb	
		flash-on-emergency	
		emergency-hold	
		6-way	

```
1 entries found.
```

Criando um perfil CPE MEDIA para serviços VoIP

Crie o perfil media (mídia) para o serviço VoIP.

> **Observação:** o perfil de mídia somente poderá ser removido quando não estiver associado a nenhum perfil de assinante

Comando:

```
cpe voip media add <profile-name>
[ echo-cancel < enabled | disabled > ] [ fax-mode < pass-through | t38 > ]
[ codec-selection-first-order < pcmu | gsm | g723 | dvi4-8 |
dvi4-16 | lpc | pcma | g722 | l16.2 | l16.1 |
qcelp | cn | mpa | gy28 | dvi4-22 | g729 > ]
[ packet-period-selection-first-order < 10 .. 30 > ]
[ silence-suppression-first-order < enabled | disabled > ]
[ codec-selection-second-order < pcmu | gsm | g723 | dvi4-8 |
dvi4-16 | lpc | pcma | g722 | l16.2 | l16.1 |
qcelp | cn | mpa | gy28 | dvi4-22 | g729 > ]
[ packet-period-selection-second-order < 10 .. 30 > ]
[ silence-suppression-second-order < enabled | disabled > ]
[ codec-selection-third-order < pcmu | gsm | g723 | dvi4-8 |
dvi4-16 | lpc | pcma | g722 | l16.2 | l16.1 |
qcelp | cn | mpa | gy28 | dvi4-22 | g729 > ]
[ packet-period-selection-third-order < 10 .. 30 > ]
[ silence-suppression-third-order < enabled | disabled > ]
[ codec-selection-fourth-order < pcmu | gsm | g723 | dvi4-8 |
dvi4-16 | lpc | pcma | g722 | l16.2 | l16.1 |
qcelp | cn | mpa | gy28 | dvi4-22 | g729 > ]
[ packet-period-selection-fourth-order < 10 .. 30 > ]
[ silence-suppression-fourth-order < enabled | disabled > ]
```

Esse comando cria um novo perfi de mídia. O nome do perfil deve ser fornecido e exclusivo para o tipo de perfil. O índice de perfil será gerado automaticamente.

Opção	Descrição
profilename	Especifica um nome exclusivo para o perfil de mídias.
echo-cancel < enabled | disabled >	Ativa ou desativa o cancelamento de eco.
fax-mode < pass-through | t38 >	Seleciona o modo fax.
codec-selection-n < pcmu | gsm | g723 | dvi4-8 | dvi4-16 |lpc | pcma | g722 | l16.2 | l16.1 | qcelp | cn | mpa |gy28 | dvi4-22 | g729 >	Especifica a seleção de codecs conforme definida na RFC 3551. n é o índice de seleção prioridade (varia de 1 a 4).
packet-period-selection-n < 10 .. 30 >	Intervalo do período de seleção de pacotes em milissegundos. n é o índice de seleção prioridade (varia de 1 a 4).
silence-suppression-n < enabled | disabled >	Especifica se a supressão de silêncio está ativada ou desativada. n é o índice de seleção prioridade (varia de 1 a 4).

Opões e descrições do comando cpe voip media add

1. Crie um perfil de mídia;

```
iSH> CPE> VOIP> MEDIA> add T38fax fax-mode t38
Profile "T38fax" has been created with index 2
```

2. Exiba os perfis de mídia CPE VoIP.

```
iSH> CPE> VOIP> MEDIA> show all
                                 echo                          codec       Packet-period  Silence
Index    Profile Name            cancel    fax mode            Selection   Selection      suppression
1        Default_Cpe_Voip_Media  enabled   passThrough         PCMU (1st)  10 (1st)       disabled (1st)
                                                               PCMU (2nd)  10 (2nd)       disabled (2nd)
                                                               PCMU (3rd)  10 (3rd)       disabled (3rd)
                                                               PCMU (4th)  10 (4th)       disabled (4th)
2        T38fax                  enabled                       PCMU (1st)  10 (1st)       disabled (1st)
                                 T38
                                                               PCMU (2nd)  10 (2nd)       disabled (2nd)
                                                               PCMU (3rd)  10 (3rd)       disabled (3rd)
                                                               PCMU (4th)  10 (4th)       disabled (4th)
2 entries found.
```

Criando um perfil CPE SUBSCRIBER (assinante) VoIP e associando-o a um perfil de servidor VoIP, a um perfil de funções VoIP e a um perfil de mídia VoIP

Para criar um perfil de assinante VoIP nas portas FXS da ONU, utilize o comando *cpe voip add*. Ao criar um perfil de assinante VoIP, o usuário deve especificar um perfil de servidor VoIP e associar as informações do servidor VoIP à porta FXS. Não existe um perfil de servidor VoIP padrão. Um perfil de funções VoIP e um perfil de mídia VoIP também são necessários ao criar o perfil de assinante VoIP, caso esses perfis não sejam especificados, serão utilizado os perfis padrão.

Depois de criar um perfil de assinante VoIP, caso seja necessário alterar as configurações desse perfil, pode ser utilizado o comando *cpe voip modify*, que possui a mesma sintaxe de comando que *cpe voip add*.

Comando:

```
cpe voip add <interface>[/<port number>]
[ admin-state < up | down >]
[ dial-number < 36 byte character string > ]
[ username < 25 byte unique character string > ]
[ password < 25 byte character string > ]
[ rx-gain < -12db - 6db > ]
[ tx-gain < -12db - 6db > ]
[ voip-server-profile <index | profile-name>]
[ voip-features-profile <index | profile-name>]
[ voip-media-profile <index | profile-name>]
```

Opção	Descrição
interface/port number	ID da ONU e ID da porta FXS das interfaces físicas.
admin-state < up | down>	Ativa ou desativa as funções executadas pela porta FXS para esse assinante. Padrão: *up*
[dial-number < 36 byte character string >]	Especifica o dial-number do assinante. Observação: o campo dial-number somente é utilizado com SIP.
username < 25 byte unique character string >	Define o ID de cliente usado para exibição das mensagens SIP. Observação: o campo username somente é utilizado com SIP.
password < 25 byte character string >	Define a senha da conta SIP para autenticação. Observação: o campo password somente é utilizado com SIP.
rx-gain < -12db - 6db >	Especifica um valor de ganho para o sinal recebido. Os valores válidos são de -12 (-12.0 dB) até 6 (+6.0 dB).
tx-gain < -12db - 6db >	Especifica um valor de ganho para o sinal transmitido. Os valores válidos são de -12 (-12.0 dB) até 6 (+6.0 dB).
voip-server-profile <index | profile-name>	Perfil cpe-voip-server associado.

voip-features-profile <index | profile-name>	Perfil cpe-voip-features associado. Se este campo for omitido, é utilizado um perfil padrão. Observação: o campo voip-features-profile somente é utilizado com SIP.
voip-media-profile <index | profile-name>	Perfil cpe-voip-media associado. Se este campo for omitido, é utilizado um perfil padrão.

Opções e descrições do comando cpe voip add

Para criar um perfil de assinante VoIP em uma ONU utilize o comando *cpe voip add*

1. Crie serviços SIP na porta FXS 1 da ONU 1/3/1, e associe o perfil do servidor VoIP 1, o perfil de funções padrão VoIP e o perfil de mídia padrão VoIP a eles;

```
iSH> CPE> VOIP> add 1/3/1/1 dial-number 2012020013
username 2012020013 password 123456
voip-server-profile 1
Service has been created
```

2. Crie serviços SIP na FXS 2 da ONU 1/3/1, e associe o perfil do servidor VoIP 1, o perfil de funções VoIP featurelist1 e o perfil de mídia VoIP T38fax a eles;

```
iSH> CPE> VOIP> add 1/3/1/2 dial-number 2012020014
username 2012020014 password 123456
voip-server-profile 1 voip-features-profile
featurelist1 voip-media-profile T38fax
Service has been created
```

3. Exiba todos os perfis de subscrição VoIP.

```
iSH> CPE> VOIP> show all
          Port     Admin                              Voip Server    Voip Features    Voip Media
CPE       Number           State    Rx Gain  Tx Gain  Profile Index  Profile Index    Profile Index
1/3/1     1                up       0        0        1              1                1
Dial Number : 2012020013
Username : 2012020013

          Port     Admin                              Voip Server    Voip Features    Voip Media
CPE       Number           State    Rx Gain  Tx Gain  Profile Index  Profile Index    Profile Index
1/3/1     2                up       0        0        1              2                2
Dial Number : 2012020014
Username : 2012020014
2 services displayed
```

Remoção de perfis CPE e conexões CPE associadas a uma ONU

O comando *cpe delete slot[/olt[/onu]]* remove:

1. Todos os perfis de assinante criados em uma ONU;
2. Outros perfis CPE associados a uma ONU, como o perfil de sistema CPE se foi configurado no provisionamento RG;

Perceba que se deseja eliminar todas as configurações de uma ONU, utilize o comando *onu delete slot[/olt[/onu]]*.

3. Exiba os perfis CPE e as conexões CPE na ONU 1/3/1;

```
iSH> cpe show 1/3/1
CPE 1/3/1
Service: DATA
GEM       UNI      UNI-VLAN/SLAN     VLAN/SLAN      G-VLAN   Admin     Oper    Rg-Mode
303       eth 1                      Tagged 100     0        up        down    B-Routed
Service: IPTV
GEM       UNI      UNI-VLAN/SLAN     OLT VLAN/SLAN  G-VLAN   Admin     Oper    Video Prof Rg-Mode
403       eth 2                      Tagged 200     0        up        down    Bridged
Service: IPTV
GEM       UNI      UNI-VLAN/SLAN     OLT VLAN/SLAN  G-VLAN   Host IP   IP Srvr Prof
501       pots                       Tagged 300     0                                1
cpe-system-common profile used: 1
```

4. Utilize *cpe delete* na ONU 1/3/1;

```
iSH> cpe delete 1/3/1
Ok to delete ALL CPE profiles for ONU 1/3/1? [yes] or [no]: yes
Do you want to exit from this request? [yes] or [no]: no
Are you sure? [yes] or [no]: yes
Operation completed
3 cpe-connection profiles deleted
1 Ethernet service deleted
1 SIP service deleted
1 Video service deleted
```

5. Verifique se os perfis de assinante CPE e os perfis de sistema CPE foram removidos dessa ONU;

```
iSH> CPE> ETH> show 1/3/1
No services found.

iSH> CPE> VOIP> show 1/3/1
No services found.

iSH> CPE> SYSTEM> show 1/3/1
No profiles found.
```

6. Verifique se todas as conexões CPE e configurações especificadas nos perfis de assinante CPE foram removidas dessa ONU.

```
iSH> CPE show 1/3/1
No connections found for 1-1-3-1/gpononu
```

Provisionamento com RG (Residential Gateway)

Existem algumas ONT GPON onde as funções ONU e RG estão fisicamente integradas no mesmo dispositivo - essas ONT são denominadas ONT com Gerenciamento Compartilhado. Dois Modos de Configuração (ex. Modo de Configuração ONT-Only e Modo de Configuração ONT+RG) existem para facilitar o provisionamento das ONT com Gerenciamento Compartilhado sob a alçada do provisionamento USP (Unified Service Provisioning).

Características do provisionamento RG (Residential Gateway)

Modos de configuração

As ONT GPON com Gerenciamento Compartilhado podem ser provisionados com o Modo de Configuração ONT-Only ou o Modo de Configuração ONT+RG. Com o modo ONT-Only, a ONT é gerenciada apenas via OMCI (OMCI Dinâmico) e isso é útil quando os serviços estão limitados a dados L2, vídeo e ou VoIP em casos simples de bridging. A grande maioria das ONTs GPON são fornecidas com essa cofiguração, pois o OMCI é utilizado exclusivamente para configuração e controle. Os requisitos de provisionamento para esse modo operacional são definidos pelo padrão ITU-T G.988.

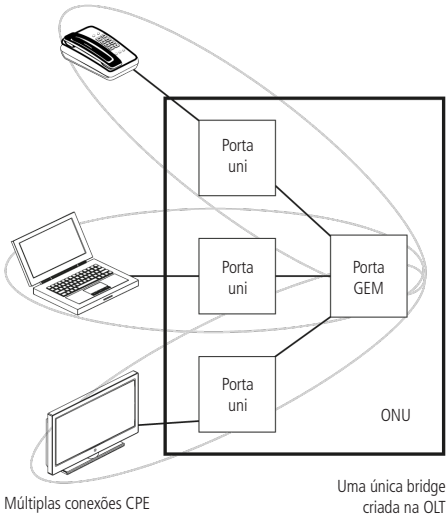
No entanto, as capacidades de provisionamento RG para ONT GPON com Gerenciamento Compartilhado exigem o Modo de Configuração ONT+RG. Com esse modo, uma conexão ONT+RG é gerenciada através de uma combinação de OMCI e SNMP. (Perceba que os usuários não precisam saber quais protocolos de gerenciamento são utilizados quando executa o provisionamento das ONT). Aqui, o SNMP complementa o OMCI, sendo responsável pelas configurações e pelo gerenciamento das funções RG.

Ambos os modos de configuração possibilitam o provisionamento prévio, e as ONTs GPON serão configuradas automaticamente após serem conectadas a porta PON e estarem ativadas.

Comando bridge add e modos RG no provisionamento RG

No provisionamento RG, a bridge da OLT 8820 G e a conexão CPE podem ter mapeamento um-para-um ou um-para-muitos.

O mapeamento um-para-um é exibido na seção "Provisionamento com OMCI dinâmico". O mapeamento um-para-muitos é exibido na imagem a seguir e mostra uma única bridge criada na OLT, que possui sua GEM Port mapeada para várias conexões CPE criadas para as múltiplas portas ethernet (UNI) da ONT.



Mapeamento um-para-muitos entre bridges da OLT 8820 G e conexões CPE

O comando *bridge add* com a palavra-chave *rg-operatingmode* cria uma bridge interface na OLT e uma conexão ONT+ RG entre uma GEM Port e as UNI Port (porta ethernet) da ONT.

A palavra-chave *rg-operatingmode* especifica o modo de funcionamento de uma VLAN no modo RG. Os modos operação RG VLAN incluem:

» **rg-bridged**

As interfaces do lado LAN e as interfaces da LAN Sem Fio podem ser integrantes da mesma bridge VLAN configurada para a interface WAN da ONT. Uma bridge VLAN pode ter um endereço IP opcional atribuído com o objetivo de possibilitar o gerenciamento, ou suportar clientes VoIP.

Uma bridge no modo RG é criada se o modo *rg-bridged* é especificado no comando *bridge add*.

» **rg-brouted**

O modo rg-brouted opera como uma Bridge VLAN para todas as interfaces LAN, e como uma VLAN routed para a interface WAN.

No modo rg-brouted, existem somente duas interfaces IP: uma para a itnerface WAN e outra para as interfaces LAN.

Uma VLAN Brouted pode ter várias portas LAN como integrantes da VLAN, e todas as portas utilizarão a mesma sub-rede IP, portanto também os mesmo servidores DHCP e IP.

» **rg-bpppoe**

PPPoE/Bridge VLAN são similares a VLAN brouted, mas a interface WAN é um cliente PPPoE que estabelece um túnel PPPoE para um BRAS no sentido upstream. No lado LAN de um PPPoE/Bridge VLAN, todas as portas serão integrantes da mesma sub-rede IP.

O comando *bridge add* é um comando poderoso. Se não houver uma conexão PPPoE, depois de executar o comando *bridge add*, a ONT estará pronta para fornecer serviços. Para o PPPoE, os usuários também precisam de um nome de usuário e senha.

A tabela a seguir fornece um resumo sobre como adicionar bridges dos serviços suportados em diferentes modos operacionais RG.

Serviços	Modos operacionais RG	Palavras-chave dos serviços	Exemplos de comando "bridge add"
Dados	rg-brouted (modo preferencial para dados)	N/A Observação: quando nenhuma palavra-chave de serviço for especificada, isso implica em serviços de dados	bridge add 1-4-1-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged eth 1 rg-brouted
	rg-bridged	N/A	bridge add 1-4-1-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged eth 1 rg-bridged
	rg-bpppoe	N/A	bridge add 1-4-1-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged eth 1 rg-bpppoe
Vídeo	rg-bridged (modo preferencial para Vídeo)	vídeo	bridge add 1-4-1-1/gpononu gem 403 gtp 1 downlink vlan 200 tagged video 0/4 eth 2 rg-bridged
	rg-brouted	vídeo	bridge add 1-4-1-1/gpononu gem 403 gtp 1 downlink vlan 200 tagged video 0/4 eth 2 rg-brouted
	rg-bpppoe	vídeo	bridge add 1-4-1-1/gpononu gem 403 gtp 1 downlink vlan 200 tagged video 0/4 eth 2 rg-bpppoe
Voice	rg-bridged (modo preferencial para Voz)	sip	bridge add 1-4-1-1/gpononu gem 501 gtp 1 downlink vlan 300 tagged rg-bridged sip (Cria serviços SIP VoIP em todas as portas FXS da ONU)
	rg-brouted	sip	bridge add 1-4-1-1/gpononu gem 501 gtp 1 downlink vlan 300 tagged rg-brouted sip (Cria serviços SIP VoIP em todas as portas FXS da ONU)
	rg-bpppoe	sip	bridge add 1-4-1-1/gpononu gem 501 gtp 1 downlink vlan 300 tagged rg-bpppoe sip (Cria serviços SIP VoIP em todas as portas FXS da ONU)

Criação de serviços RG utilizando o comando bridge add

Criando múltiplas conexões CPE que compartilham uma GEM Port

O exemplo a seguir cria serviços de dados em uma ONT com gerenciamento compartilhado com o modo RG-bridge. Isso cria uma bridge da OLT 8820 G e duas conexões CPE.

Essas duas conexões CPE compartilham o mesmo GEM Port ID, VLAN e GTP (Perfil de tráfego GPON).

1. Crie uma bridge da OLT e a primeira conexão CPE:

```
iSH> bridge add 1-1-3-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged eth 1 uni-vlan 100 rg-bridged
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record 1-1-3-303-gponport-100/bridge
CPE Connection 1-1-3-303/gponport/1/1/100/0 has been created
```

A primeira parte desse comando `bridge add 1-1-3-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged` cria um nova bridge na OLT 8820 G. A segunda parte desse comando `eth 1 uni-vlan 100 rg-bridged` cria uma conexão ONT+RG entre a GEM Port e a porta UNI. Também cria uma interface com bridge do lado WAN e uma interface com bridge no lado LAN na ONT.

Ao especificar GEM Ports no comando *bridge add*, perceba que qualquer ID de GEM Port na faixa de 257 até 3828 pode ser associada a qualquer ONU exceto as GEM Ports 5xx, onde os dois últimos dígitos do ID da GEM Port devem ser o número da porta ONU na faixa entre 1 e 64. Por exemplo, o GEM Port ID 564 deve pertencer à ONU 64. Cada um desses ID de GEM Port deve ser exclusivo para a porta OLT.

O GTP é um campo obrigatório no comando bridge *add* ao criar uma bridge na OLT 8820 G. Ele contém as informações de alocação de largura de banda para T-cont.

Exiba as bridges da OLT 8820 G:

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN    Physical          Bridge                          St Table Data
dwn             Tagged 100   1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge   UP D 00:02:71:19:4b:28
                                                                                 D 00:00:86:43:3c:e4
                                                                                 D 192.168.1.12
upl             Tagged 100   1/1/5/0/eth       ethernet5-100/bridge            UP S VLAN 100 default
2 Bridge Interfaces displayed
```

Exiba as conexões:

```
iSH> bridge show onu
GEM  ONU    DSCP     ONU UNI   OLT                                                OLT
ONU    Port  UNI  to COS     VLAN/SLAN   VLAN/SLAN  G-VLAN MVR Service  Rg-Mode  OLT Bridge    ST
1/3/1    303 eth 1 --- 100/----  Tagged 100   ----  ----  data  Bridged  1-1-3-303-gponport-100/bridge  UP
1 Bridge Interfaces displayed
1 GPON ONU Connections displayed
```

Exiba as interfaces WAN e LAN da ONT:

```
iSH> cpe show 1/3/1
CPE 1/3/1
Service: DATA
GEM    UNI      UNI-VLAN/SLAN   VLAN/SLAN   Admin   Oper   Rg-Mode
303    eth 1    100/----  Tagged 100         up      up     Bridged
```

```
iSH> cpe rg wan show all
                                                    Retry      Pppoe      Ip-Com   Port-Fwd
CPE    VLAN/SLAN     RG Mode    IP Address     Auth  Interval User Id  Profile  List Profile
1/3/1  100/----      Bridged             dhcp -      -          -        1        0
1 services displayed
```

```
iSH> cpe rg lan show all
                                                          Ip-Com     Dhcp Srvr
CPE    UNI          UNI-Vlan/Slan     Vlan/Slan    IP-Address    Profile     Profile     Rg-Mode
1/3/1  eth 1        100/----          Tagged 100   0.0.0.0       0           0           Bridged
Services displayed: 1
```

2. Crie a segunda conexão CPE e mapeie para o nova bridge da OLT.

```
iSH> bridge add 1-1-3-1/gpononu gem 303 gtp 1 tm 1 downlink vlan 100 tagged eth 2 uni-vlan 100 rg-bridged
CPE Connection 1-1-3-303/gponport/1/2/100/0 has been created
```

A primeira parte desse comando *`bridge add 1-1-3-1/gpononu gem 303 gtp 1 tm 1 downlink vlan 100 tagged`* indica a bridge da OLT 8820 G. A segunda parte desse comando *`eth 2 uni-vlan 100 rg-bridged`* cria conexões ONT + RG com essa bridge da OLT. Dado que a VLAN RG-Bridged já foi criada pelo comando anterior, esse exemplo adiciona a porta Ethernet UNI 2 como integrante.

Exiba as bridges da OLT:

```
iSH> bridge show
          Orig
Type VLAN/SLAN  VLAN/SLAN      Physical          Bridge                          St Table Data
dwn             Tagged 100     1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge   UP D 00:02:71:19:4b:28
                                                                                 D
                                                                                 00:00:86:43:3c:e4
                                                                                 D 192.168.1.12
upl             Tagged 100     1/1/5/0/eth       ethernet5-100/bridge            UP S VLAN 100 default
2 Bridge Interfaces displayed
```

Exiba as conexões CPE:

```
iSH> bridge show onu
GEM  ONU   DSCP     ONU UNI   OLT                                                OLT
ONU       Port  UNI     to COS    VLAN/SLAN   VLAN/SLAN   G-VLAN MVR  Service   Rg-Mode   OLT Bridge    ST
1/3/1     303  eth 1   ------   100/---- Tagged  100   ----  ----  data    Bridged  1-1-3-303-gponport-100/bridge  UP
1/3/1     303  eth 2   ------  100/---- Tagged  100  ----  ----  data    Bridged  1-1-3-303-gponport-100/bridge  DWN
1 Bridge Interfaces displayed
2 GPON ONU Connections displayed
```

Exiba as interfaces WAN e LAN da ONT:

```
iSH> cpe show 1/3/1
CPE 1/3/1
Service: DATA
GEM    UNI     UNI-VLAN/SLAN   VLAN/SLAN   Admin   Oper   Rg-Mode
303    eth 1   100/----  Tagged 100         up      up     Bridged
303    eth 2   100/----  Tagged 100         up      down   Bridged
```

```
iSH> cpe rg wan show 1/3/1
                                                          Retry      Pppoe      Ip-Com   Port-Fwd
CPE    VLAN/SLAN     RG Mode    IP Address       Auth    Interval   User Id    Profile  List Profile
1/3/1  100/----      Bridged              dhcp -       -          -          1        0
Pppoe User Id: --
1/3/1  100/----      Bridged              dhcp -       -          -          1        0
Pppoe User Id: --
2 services displayed
```

```
iSH> cpe rg lan show 1/3/1
                                                                 Ip-Com   Dhcp
CPE    UNI           UNI-Vlan/Slan Vlan/Slan      IP-Address    Profile  Profile  Rg-Mode
1/3/1  eth 1         100/----      Tagged 100     0.0.0.0       0        0        Bridged
1/3/1  eth 2         100/----      Tagged 100     0.0.0.0       0        0        Bridged
Services displayed: 2
```

Removendo bridges e conexões CPE associadas

O exemplo a seguir remove o mapeamento um-para-muitos entre a bridge da OLT e as duas conexões CPE.

Para remover a bridge da OLT e todas as conexões CPE associadas.

1. Para remover a bridge da OLT e todas as conexões CPE associadas ao mesmo tempo, pode utilizar o comando bridge *delete all;*

```
iSH> bridge delete 1-1-3-303-gponport-100/bridge all
CPE Connection 1-1-3-303/gponport/1/1/100/0 has been deleted
CPE Connection 1-1-3-303/gponport/1/2/100/0 has been deleted
1-1-3-303-gponport-100/bridge delete complete
```

2. Ou pode remover as conexões CPE primeiro e depois remover a bridge da OLT 8820 G.

```
iSH> bridge delete 1-1-3-303-gponport-100/bridge eth 1 uni-vlan 100
CPE Connection 1-1-3-303/gponport/1/1/100/0 has been deleted
```

Se existe somente uma conexão CPE associada a bridge da OLT, pode remover diretamente a interface da OLT.

```
iSH> bridge delete 1-1-3-303-gponport-100/bridge
CPE Connection 1-1-3-303/gponport/1/2/100/0 has been
deleted 1-1-3-303-gponport-100/bridge delete complete
```

Provisionamento OMCI com funções RG para serviços TriplePlay

Criação de serviços de dados no modo RG

Somente é necessário especificar o perfil ME interno uma vez para cada ONU.

Somente é necessário ativar a ONU uma única vez.

Criando um perfil de tráfego GPON

Crie um perfil de tráfego GPON. O GTP é necessário para o comando *bridge add*.

```
iSH> new gpon-traffic-profile 1
gpon-traffic-profile  1
Please provide the following:[q]uit.
guaranteed-upstream-bw: --------->       {0}:
traffic-class: ------------------->       {ubr}:
compensated: --------------------->       {false}:
shared: -------------------------->       {false}:
dba-enabled: --------------------->       {false}:true
dba-fixed-us-ubr-bw: ------------->       {0}:2048
dba-fixed-us-cbr-bw: ------------->       {0}:
dba-assured-us-bw: --------------->       {0}:
dba-max-us-bw: ------------------->       {0}:4096
dba-extra-us-bw-type: ------------>       {nonassured}:
.....................
 Save new record? [s]ave, [c]hange or [q]uit: s
 New record saved.
```

Especificando o perfil ME interno para a ONU

Especificando o perfil ME da ONU na configuração inicial, a OLT sabe que esse modelo de ONU é provisionado pelo modo RG.

```
iSH> onu set 1/3/1 meprof intelbras-1420g
```

Criando bridges de uplink/downlink e conexões CPE no modo RG-brouted para serviços de dados

No exemplo a seguir, a porta Ethernet 1 da ONT é integrante da VLAN100 brouted no modo RG. A função de NAT está ativo no lado WAN. Ao criar as interfaces do lado LAN na mesma RG VLAN, um servidor DHCP e um perfil IP-COM serão atribuídos a todas as interfaces. Por padrão, o primeiro número atribuído do índice é 100001, e a sub-rede IP é 192.168.1.1.

Os números de índice do servidor DHCP e do perfil IP-COM serão aumentados automaticamente se criar uma nova conexão CPE em outra VLAN RG.

Pode utilizar o servidor DHCP e perfil IP-COM padrão ou criar e atribuir outro servidor DHCP e perfil IP-COM na interface do lado LAN.

1. Crie uma bridge interface uplink na OLT;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 100
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record ethernet5-100/bridge
bridge-path added successfully
```

2. Crie uma bridge de downlink na OLT e uma conexão entre a GEM Port 303 da ONT 1-1-3-1 e porta ethernet 1 da ONT na VLAN 100;

```
iSH> bridge add 1-1-3-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged eth 1 rg-brouted
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record
1-1-3-303-gponport-100/bridge
CPE Connection 1-1-3-303/gponport/1/1/0/0 has been created
```

A primeira parte desse comando, *bridge add 1-1-3-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged* cria um nova bridge na OLT. A segunda parte desse comando *eth 1 rg-brouted* cria uma conexão na ONT 1-1-3-1 na porta eth 1 sem marcação (untagged) atrelado a GEM Port 303, e uma interface brouted no lado WAN da ONT, e uma interface brouted no lado LAN da ONT.

3. Visualize as bridges;

```
iSH> bridge show
          Orig
Type VLAN/SLAN   VLAN/SLAN  Physical          Bridge                          St Table Data
dwn              Tagged 100  1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge   UP
upl              Tagged 100  1/1/5/0/eth       ethernet5-100/bridge            UP S VLAN 100 default
2 Bridge Interfaces displayed
```

4. Visualize as interfaces WAN;

```
iSH> CPE> RG> WAN> show 1/3/1
                                                    Retry     Ip-Com   Port-Fwd
CPE    VLAN/SLAN     RG Mode    IP Address Auth     Interval  Profile  List Profile  G-VLAN
1/3/1  100/----      B-Routed         dhcp -        -         1        0             -
Pppoe User Id: --
1 services displayed
```

5. Visualize as interfaces LAN.

```
iSH> CPE> RG> LAN> show 1/3/1
                                                                    IP Com   Dhcp Srvr
CPE    UNI      UNI-VLAN/SLAN   VLAN/SLAN  G-VLAN   IP-Address     Profile  Profile      Rg-Mode
1/3/1  eth 1                    Tagged 100 -        192.168.1.1    Bridged  100001       B-Routed
Services displayed: 1
```

Ativando a ONU

Ative a ONU para adicioná-la ao sistema. No provisionamento USP (Unified Service Provisioning), após alterar as configurações de serviço de uma ONU ativada, as configurações de serviços serão atualizadas automaticamente.

1. Para ativar uma ONU, primeiro execute o comando *onu show* para exibir as ONU presentes na OLT e descobrir os números de série disponíveis;

O comando *onu show* possui opções para selecionar por slot e OLT. se executar o comando sem definir o slot/OLT, o comando buscará todos as ONTs em todos as portas PON.

```
iSH> onu show 1/3
Free ONUs for slot 4 olt 1:
1    2    3    4    5    6    7    8    9    10   11   12
13   14   15   16   17   18   19   20   21   22   23   24
25   26   27   28   29   30   31   32   33   34   35   36
37   38   39   40   41   42   43   44   45   46   47   48
49   50   51   52   53   54   55   56   57   58   59   60
61   62   63   64
Discovered serial numbers for slot 1 olt 3:
sernoID     Vendor     Serial Number    sernoID     Vendor    Serial Number
1            ZNTS         03194B28
```

2. Execute o comando onu set para associar um ID da porta PON a um número de série da ONT desejada:

```
iSH> onu set 1/3/1 1
Onu 1 successfully enabled with serial number ZNTS
03194B28
```

3. Execute o comando *onu show* para verificar se a ONT está ativada, e se o suporte OMCI foi adicionado à ONT (o perfil ME interno associado poderá ser exibido);

```
iSH> onu show 1/3/1
                                        Serial
ONU    Name      Enabled          Model #     Number          OMCI files and profiles
1      1-1-3-1   Yes              1420G       ZNTS 03194B28   ME        intelbras-1420g
Observação: NULL Model String indicates not able to get model ID
```

4. Execute o comando *onu status* para verificar se o Status de Configuração da OMCI está ativo.

```
iSH> onu status 1/3/1
ID      Onu      OperStatus  ConfigState  Download State  OLT Rx Power  ONT Rx Power  Distance (km)  GPON OnuStatus
1       1-1-3-1  Up          Active       NoUpgrade       -19.2 dBm     -20.0 dBm     18             Active
```

Criação de serviços de vídeo no modo RG

» **Criando um perfil de tráfego GPON**

O perfil de tráfego GPON é necessário ao utilizar o comando bridge *add*.

```
iSH> new gpon-traffic-profile 2
gpon-traffic-profile 2
Please provide the following: [q]uit.
guaranteed-upstream-bw: ---------->    {0}: 512
traffic-class: ------------------->    {ubr}:
compensated: --------------------->    {false}:
shared: -------------------------->    {false}:
dba-enabled: --------------------->    {false}:
dba-fixed-us-ubr-bw: ------------->    {0}:
dba-fixed-us-cbr-bw: ------------->    {0}:
dba-assured-us-bw: --------------->    {0}:
dba-max-us-bw: ------------------->    {0}:
dba-extra-us-bw-type: ------------>    {nonassured}:
.................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

» **Criando bridges de uplink/downlink na OLT 8820 G e conexões CPE no modo RG-bridged para serviços de vídeo**

No exemplo a seguir, a porta Ethernet 2 da ONT é integrante da VLAN200 com bridge no modo RG.

1. Crie uma bridge interface uplink na OLT 8820 G;

```
iSH> bridge add 1-1-5-0/eth uplink vlan 200
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record ethernet5-200/bridge
bridge-path added successfully
```

2. Crie uma bridge de downlink na OLT 8820 G e uma conexão entre a GEM Port 403 da ONT 1-1-3-1 e porta Eth 2 na VLAN 200;

```
iSH> bridge add 1-1-3-1/gpononu gem 403 gtp 2 downlink vlan 200 tagged
video 0/4 eth 2 rg-bridged
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record 1-1-3-403-gponport-200/bridge
CPE Connection 1-1-3-403/gponport/12/2/0/0 has been created
```

A primeira parte desse comando *bridge add 1-1-3-1/gpononu gem 403 gtp 2 downlink vlan 200 tagged* cria um nova bridge na OLT 8820 G. A segunda parte desse comando *eth 2 rg-bridged* cria uma conexão CPE na ONT 1-1-3-1 para a porta eth 2 atrelada a GEM Port 403, uma interface com bridge no lado WAN da ONT, e uma interface com bridge no lado LAN da ONT.

3. Visualize as bridges;

```
iSH> bridge show
          Orig
Type VLAN/SLAN   VLAN/SLAN   Physical          Bridge                          St Table Data
dwn              Tagged 100   1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge   UP D
dwn              Tagged 200   1/1/3/1/gpononu   1-1-3-403-gponport-200/bridge   UP
upl              Tagged 100   1/1/5/0/eth       ethernet5-100/bridge            UP   S VLAN 100 default
upl              Tagged 200   1/1/5/0/eth       ethernet5-200/bridge            UP   S VLAN 200 default
4 Bridge Interfaces displayed
```

4. Visualize as interfaces WAN;

```
iSH> CPE> RG> WAN> show 1/3/1
                                                        Retry     Ip-Com   Port-Fwd
CPE    VLAN/SLAN     RG Mode    IP Address    Auth     Interval  Profile  List Profile  G-VLAN
1/3/1  100/----      B-Routed           dhcp  -        -         1        0             -
Pppoe User Id: --
1/3/1  200/----      Bridged IP Unconfigured  -        -         0        0             -
Pppoe User Id: --
2 services displayed
```

5. Visualize as interfaces LAN.

```
iSH> CPE> RG> LAN> show 1/3/1
                                                                    Ip-Com   Dhcp Srvr
CPE    UNI         UNI-Vlan/Slan  Vlan/Slan         G-VLAN  IP-Address    Profile  Profile     Rg-Mode
1/3/1  eth 1                      Tagged 100 ----           192.168.1.1   100001   100001      B-Routed
1/3/1  eth 2                      Tagged 200 ----           0.0.0.0       0        0           Bridged
Services displayed: 2
```

Criação de serviços de voz no modo RG

» **Criando um perfil de tráfego GPON**

O perfil de tráfego GPON é necessário durante a utilização do comando bridge add.

```
iSH> new gpon-traffic-profile 3
gpon-traffic-profile  3
Please provide the following:[q]uit.
guaranteed-upstream-bw: ---------->     {0}: 512
traffic-class: ------------------->     {ubr}:
compensated: --------------------->     {false}:
shared: -------------------------->     {false}:
dba-enabled: --------------------->     {false}:
dba-fixed-us-ubr-bw: ------------->     {0}:
dba-fixed-us-cbr-bw: ------------->     {0}:
dba-assured-us-bw: --------------->     {0}:
dba-max-us-bw: ------------------->     {0}:
dba-extra-us-bw-type: ------------>     {nonassured}:
.................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved..
```

» **Criando bridges de uplink/downlink na OLT 8820 G e conexões CPE no modo RG-bridged para serviços SIP**

No exemplo a seguir, é criado o serviço SIP e as portas FXS da ONT são integrantes da VLAN 300 no modo rg-bridged.

1. Crie uma interface uplink na OLT 8820 G:

```
iSH> bridge add 1-1-5-0/eth uplink vlan 300
Adding bridge on 1-1-5-0/eth
Created bridge-interface-record ethernet5-300/bridge
bridge-path added successfully
```

2. Crie uma bridge de downlink na OLT 8820 G e uma conexão entre a GEM Port 501 da ONT 1-1-3-1 com as portas FXS da ONT na VLAN 300;

```
iSH> bridge add 1-1-3-1/gpononu gem 501 gtp 3 downlink vlan 300 tagged rg-bridged sip
Adding bridge on 1-1-3-1/gpononu
Created bridge-interface-record 1-1-3-501-gponport-300/bridge
CPE Connection 1-1-3-501/gponport/14/0/0/0 has been created
```

A primeira parte desse comando *bridge add 1-1-3-1/gpononu gem 501 gtp 3 downlink vlan 300 tagged* cria um nova bridge na OLT 8820 G. A segunda parte desse comando, *rg-bridged sip* cria uma conexão das portas FXS da ONT 1-1-3-1 para fazer uma bridge entre as portas FXS e a GEM Port 501, uma bridge interface no lado WAN da ONT para utilizar com o cliente interno de serviços de voz. Perceba que a interface padrão de sistema e o cliente DNS de sistema são destinados automaticamente para a VLAN de Voz.

3. Visualize as bridges;

```
iSH> bridge show
          Orig
Type    VLAN/SLAN   VLAN/SLAN  Physical          Bridge                          St Table Data
dwn             Tagged 100     1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge  UP D 00:02:71:19:4b:28
dwn             Tagged 200     1/1/3/1/gpononu   1-1-3-403-gponport-200/bridge  UP
dwn             Tagged 300     1/1/3/1/gpononu   1-1-3-501-gponport-300/bridge  UP D 00:02:71:19:4b:29
                                                                                  D 00:02:71:19:4b:28
upl             Tagged 100     1/1/5/0/eth       ethernet5-100/bridge            UP S VLAN 100 default
upl             Tagged 200     1/1/5/0/eth       ethernet5-200/bridge            UP S VLAN 200 default
upl             Tagged 300     1/1/5/0/eth       ethernet5-300/bridge            UP S VLAN 300 default
6 Bridge Interfaces displayed
```

4. Visualize as interfaces WAN;

```
iSH> CPE> RG> WAN> show 1/3/1
                                                    Retry     Ip-Com    Port-Fwd
CPE     VLAN/SLAN      RG Mode    IP Address  Auth  Interval  Profile   List Profile   G-VLAN
1/3/1   100/----       B-Routed          dhcp  -     -         1         0              -
Pppoe User Id: --
1/3/1   200/----       Bridged IP Unconfigured -     -         0         0              -
Pppoe User Id: --
1/3/1   300/----       Bridged           dhcp  -     -         1         0              -
Pppoe User Id: --
3 services displayed
```

5. Visualize as interfaces LAN.

```
iSH> CPE> RG> LAN> show 1/3/1
                                                                          IP Com   Dhcp Srvr
CPE     UNI      UNI-VLAN/SLAN    VLAN/SLAN   G-VLAN   IP-Address      Profile  Profile    Rg-Mode
1/3/1   eth 1                     Tagged 100  -        192.168.1.1     100001   100001     B-Routed
1/3/1   eth 2                     Tagged 200  -        0.0.0.0         0        0          Bridged
1/3/1   pots                      Tagged 300  -        -               -        -          Bridged
Services displayed: 3
```

» **Criando um perfil IP-COM para serviços de voz (opcional)**

Esse passo é opcional. Se a ONT está utilizando DHCP (configuração padrão) para obter o endereço IP do serviço de voz, pode ignorar esse passo.

Se deseja atribuir um endereço IP estático à ONT, precisa criar um perfil IP-COM estático na interface WAN e atribuir o endereço IP estático à interface WAN.

Criação de serviços de dados em interfaces sem fio

Bridges de uplink/downlink na OLT 8820 G e conexões CPE no modo RG-brouted

Esse exemplo cria os serviços de dados na interface WLAN 1 (ex. SSID 0 na ONT WebUI). Essa interface WLAN utiliza a mesma VLAN e GEM Port que da porta eth 1.

1. Esse exemplo não criará uma interface de uplink. Ele utiliza a VLAN já criada no uplink para serviços de dados;
2. Crie uma bridge de downlink na OLT 8820 G e uma conexão entre a GEM Port 303 da ONT 1-1-3-1 e a interface sem fio 1 do lado LAN da ONT (ex. SSID 0 na ONT WebUI) na VLAN 100;

```
iSH> bridge add 1-1-3-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged wlan 1 rg-brouted
CPE Connection 1-1-3-303/gponport/18/1/0/0 has been created
```

A primeira parte desse comando *`bridge add 1-1-3-1/gpononu gem 303 gtp 1 downlink vlan 100 tagged`* cria a bridge na OLT 8820 G. A segunda parte desse comando *`wlan 1 rg-brouted`* cria uma conexão com essa bridge, e uma interface sem fio no lado LAN roteado daONT. Um perfil de assinante WLAN também será criado.

3. Visualize as bridges;

```
iSH> bridge show
       Orig
Type VLAN/SLAN   VLAN/SLAN  Physical          Bridge                          St Table Data
dwn          Tagged 100    1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge   UP D
dwn          Tagged 200    1/1/3/1/gpononu   1-1-3-403-gponport-200/bridge   UP D
dwn          Tagged 300    1/1/3/1/gpononu   1-1-3-501-gponport-300/bridge   UP D
upl          Tagged 100    1/1/5/0/eth       ethernet5-100/bridge            UP S VLAN 100 default
upl          Tagged 200    1/1/5/0/eth       ethernet5-200/bridge            UP S VLAN 200 default
upl          Tagged 300    1/1/5/0/eth       ethernet5-300/bridge            UP S VLAN 300 default
6 Bridge Interfaces displayed
```

```
iSH> bridge show onu
       GEM   ONU     DSCP  ONU UNI OLT           OLT
ONU    Port  UNI     to COS VLAN/SLAN VLAN/SLAN  G-VLAN MVR  Service Rg-Mode OLT Bridge          ST
1/3/1  403   eth 2         Tagged 200 ----       iptv    Bridged 1-1-3-403-gponport-200/bridge   DOWN
1/3/1  303   eth 1         Tagged 100 ----       data   B-Routed 1-1-3-303-gponport-100/bridge   UP
1/3/1  303   wlan 1        Tagged 100 ----       data   B-Routed 1-1-3-303-gponport-100/bridge   -
1/3/1  501   pots          Tagged 300 ----       sip      Bridged 1-1-3-501-gponport-300/bridge  UP
3 Bridge Interfaces displayed
4 GPON ONU Connections displayed
```

4. Visualize as interfaces WAN;

```
iSH> CPE> RG> WAN> show 1/3/1
                                                        Retry    Ip-Com   Port-Fwd
CPE    VLAN/SLAN      RG Mode    IP Address     Auth    Interval Profile  List Profile  G-VLAN
1/3/1  100/----       B-Routed            dhcp  -       -        1        0             -
Pppoe User Id: --
1/3/1  200/----       Bridged IP Unconfigured   -       -        0        0             -
Pppoe User Id: --
1/3/1  300/----       Bridged             dhcp  -       -        1        0             -
Pppoe User Id: --
3 services displayed
```

5. Visualize as interfaces WLAN.

```
iSH> CPE> RG> LAN> show 1/3/1
                                                                IP Com   Dhcp Srvr
CPE     UNI     UNI-VLAN/SLAN    VLAN/SLAN   G-VLAN   IP-Address    Profile   Profile     Rg-Mode
1/3/1   eth 1                    Tagged 100  -        192.168.1.1   100001    100001      B-Routed
1/3/1   eth 2                    Tagged 200  -        0.0.0.0       0         0           Bridged
1/3/1   pots                     Tagged 300  -        0.0.0.0       0         0           Bridged
1/3/1   wlan 1                   Tagged 100  -        192.168.1.1   100001    100001      B-Routed
Services displayed: 4
```

» **Criando um perfil de assinante CPE WLAN e associando-o a um perfil CPE WLAN-COM ou a um perfil CPE WAN-COM-ADV (opcional)**

Por padrão, o status da interface Wireless LAN (WLAN) está up depois da criação da conexão CPE nessa interface. Por causa disso, o tráfego de Dados pode funcionar nessa interface WLAN UNI sem necessidade de mais configurações.

Se deseja mudar as configurações padrão da WLAN, pode utilizar o comando *cpe wlan add*. Com esse comando, o perfil de assinante CPE WLAN é criado manualmente. O ID da interface WLAN UNI especificado nesse comando deve corresponder àquele atribuído no comando bridge *add* ao criar a bridge de downlink e a conexão CPE.

Depois de criar um perfil de assinante CPE WLAN, se desejar mudar as configurações desse perfil, pode utilizar o comando *cpe wlan modify*, que possui a mesma sintaxe de comando que *cpe wlan add.*

Comando:

```
cpe wlan add <interface>/<port number>
[ admin-state < up | down > ]
[ ssid < value> ]
[ encrypt-key < value> ]
[ device-pin < value > ]
[ radius-key < value > ]
[ wlan-com-profile < index | profile-name > ]
[ wlan-com-adv-profile < index | profile-name > ]
```

A tabela a seguir fornece a descrição para as opções no comando *cpe wlan add.*

Opção	Descrição
interface/port number	ID da ONU e ID da interface WLAN das interfaces físicas.
admin-state value	Ativa ou desativa as funções executadas pela interface sem fio para esse assinante. Os valores possíveis são up e down. O valor padrão é *up*.
ssid value	Atribui o Service Set Identifier (SSID) à interface LAN sem fio. Um SSID é o nome público de uma rede local sem fio. Todos os serviços em uma rede local sem fio devem utilizar o mesmo SSID para comunicar-se uns com os outros. Pode ser uma string com 32 caracteres ou menos.
encrypt-key value	Configura a chave de criptografia para rede sem fio, afim de aumentar a segurança. Os dois tipos padrão de chave criptográfica são: Wired Equivalent Privacy (WEP) e Wi-Fi Protected Access (WPA): » Se é uma chave de criptografia WEP de 64 bites: o valor pode ser de 5 caracteres ASCII ou 10 dígitos hexadecimais. » Se é uma chave de criptografia WEP de 128 bites: o valor pode ser de 13 caracteres ASCII ou 26 dígitos hexadecimais. » Se é uma senha WPA: o valor pode ter 64 caracteres.
device-pin value	Configura o pin do dispositivo somente quando o método de segurança Wi-Fi Protected Setup (WPS) está ativado.
radius-key value	Configura a chave de autenticação do servidor Radius (Remote Authentication Dial In User Server). Esse campo não pode conter ESPAÇOS e é retornado como uma sequencia de asteriscos.
wlan-com-profile index | profile-name	Perfil WLAN-COM (perfil comum) é associado com interface WLAN Padrão: *1*. Indica que o perfil wlan-com utilizado é o de índice 1.
wlan-com-adv-profile index | profile-name	Perfil WLAN-COM-ADV (perfil avançado) é associado com a interface WLAN. Padrão: *1*. Isso indica que o perfil wlan-com-adv utilizado é o de índice 1.

Opções e descrições do comando cpe wlan add

Para criar um perfil de assinante CPE WLAN, utilize o comando cpe wlan add:

1. Esse exemplo configura o SSID e a chave de criptografia da interface WLAN 1 da ONU 1/3/1;

```
iSH> CPE> WLAN> add 1/3/1/1 ssid intelbras encrypt-key 1234567890
Service has been created
```

2. Exiba as configurações do Perfil de assinante CPE WLAN para a interface WLAN 1 da ONU 1/3/1. Como exibe o exemplo, o perfil comum padrão WLAN e o perfil comum avançado padrão WLAN com índice 1 foram atribuídos a esse perfil de assinante WLAN;

```
iSH> CPE> RG> LAN> show 1/3/1
CPE    WLAN   Admin    SSID    WLAN Com Prof    WLAN Com Adv Prof
1/3/1  1      up               intelbras        1                1
1 services displayed
```

3. Exiba todos os serviços criados na ONU.

```
iSH> cpe show 1/3/1
CPE 1/3/1
Service: DATA
GEM    UNI      UNI VLAN/SLAN  VLAN/SLAN        G-VLAN       Admin Oper   Rg-Mode
303    eth 1                   Tagged 100       0            up           up B-Routed
303    wlan 1                  Tagged 100       0            up           up B-Routed
Service: IPTV
GEM    UNI      UNI VLAN/SLAN  OLT VLAN/SLAN    G-VLAN       Admin Oper   Video Prof    Rg-Mode
403    eth 2                   Tagged 200       0            up           down          Bridged
Service: SIP
GEM    UNI      UNI VLAN/SLAN  OLT VLAN/SLAN    G-VLAN       Host IP      IP Srvr Prof
501    pots                    Tagged 300       0                         1
```

» **Criando um perfil CPE WLAN-COM (opcional)**

Esse passo é opcional. Pode utilizar o perfil comum WLAN se deseja adicionar alguns atributos comuns da interface WLAN.

O perfil comum WLAN nessa seção cobre as configurações comuns que podem ser utilizadas nas portas WLAN 1 a 4. O perfil comum avançado WLAN na próxima seção cobre as configurações avançadas que podem ser utilizadas somente na interface WLAN 1.

> **Observação:** o perfil comum WLAN somente poderá ser removido quando não estiver associado a nenhum perfil de assinante WLAN

Comando:

cpe wlan common add *<profile-name <string>>*

[*net-authen < open | shared | 802dot1x | wpa | wpa-psk | wpa2 | wpa2-psk | mixed-wpa2-wpa | mixed-wpa2-wpa-psk >]*

[hide-ap **< enabled | disabled >** *]*

[isolate-clients *< enabled | disabled >* **]**

[wmm-advertise *< enabled | disabled >* **]**

[mcast-forward *< enabled | disabled >* **]**

[max-clients *< value >* **]**

[wpa-group-rekey-interval *< value >* **]**

[wpa-encryption *< aes | tkip-aes >* **]**

[wep-encryption *< enabled | disabled >* **]**

[wep-strength *< 64bits | 128bits >* **]**

[radius-server-ip *< IP address >* **]**

[radius-port *< value >* **]**

[wpa2-preauth *< enabled | disabled >* **]**

[reauthen-interval *< value >* **]**

Esse comando cria um novo perfil. O nome do perfil deve ser fornecido e deve ser exclusivo. O índice de perfil será gerado automaticamente.

A tabela a seguir fornece a descrição para as opções do comando *cpe wlan common add.*

Opção	Descrição
profile-name <string>	Especifica um nome exclusivo do perfil wlan-com. Deve possuir no máximo 36 caracteres.
net-authen value	Configura o método de autenticação da rede. Valores: open, shared, 802dot1x, wpa, wpa-psk wpa2, wpa2-psk, mixed-wpa2-wpa, mixed-wpa2-wpa-psk
hide-ap value	Ativa ou desativa a supressão do anuncio do SSID do ponto de acesso. Se está ativado, os clientes precisarão configurar o SSID para fazer a associação. Valores: enabled, disabled Padrão: *disabled*
isolate-clients value	Isola clientes dentro da rede sem fio, impedindo-os de comunicar-se diretamente uns com os outros. Valores: enabled, disabled Padrão: *disabled*
wmm-advertise value	Wireless Multi Media (WMM) proporciona um subconjunto do padrão IEEE 802.11e QoS, que acrescenta a definição de prioridade à rede sem fio para melhorar o desempenho. Quando várias aplicações concorrentes estão na rede sem fio, cada aplicação pode ter diferentes necessidades em relação a latência e transmissão. WMM fornece ferramentas para essa melhoria, mas seu fornecimento pode ser lento. Valores: enabled, disabled Padrão: *disabled*
mcast-fwd value	Wireless Multicast Forwarding habilita a capacidade de enviar pacotes multicast para que sejam interceptados por todos os nós na faixa de transmissão do emissor. Valores: enabled, disabled Padrão: *disabled*
max-clients value	Número máximo de dispositivos clientes sem fio que podem estar conectados simultaneamente à rede sem fio. Valores: 1-50 Padrão: *16*
wpa-group-rekey-interval value	Especifica o intervalo WPA Group Rekey Valores: 0-9999999999 Padrão: *0*
wpa-encryption value	Modo de criptografia WPA. Valores: aes, tkip-aes Padrão: *aes*
wep-encryption value	Modo de criptografia WEP. Valores: enabled, disabled Padrão: *disabled*
wep-strength value	Nível da criptografia WEP. Valores: 64bit, 128bit Padrão: *128bit*
radius-server-ip value	Endereço IP do servidor Radius utilizado para autenticação 802.1x. Padrão: *0.0.0.0*
radius-port value	Porta UDP para acessar o servidor Radius. Valores: 0-9999999999 Padrão: *1812*
wpa2-preauth value	Ativa ou desativa a pré autenticação WPA2. Valores: enabled, disabled Padrão: *disabled*
reauthen-interval value	Tempo em segundos da re-autenticação WPA2. Valores: 0-9999999999 Padrão: *36000*

Opções e descrições do comando cpe wlan common add

1. Crie o perfil WLAN-COM;

```
iSH> CPE> WLAN> COMMON> add wifi net-authen wpa2-psk
Profile "wifi" has been created with index 2
```

2. Exiba os perfis comuns WLAN;

```
iSH> CPE> WLAN> COMMON> show all
                                                    WPA          WPA          WEP
Index  Profile Name      Net Authentication       Encrypt      Encrypt     Strength
1      default-wlan1     open                       aes       disabled     128bits
2      wifi              wpa2-psk                   aes       disabled     128bits
2 entries found.
```

3. Se os usuários desejam remover um perfil comum WLAN, utilize o comando *cpe wlan common delete <profile-index> | <profile-name>;*

```
iSH> CPE> WLAN> COMMON> delete 2
Profile has been deleted.
```

4. Os usuários podem utilizar o comando *find* para encontrar o perfil de assinante WLAN associado.

Esse exemplo assume que o perfil comum WLAN 1 está associado a um perfil de assinante na ONU 1/3/1:

```
iSH> CPE> WLAN> COMMON> find 1
cpe-wlan-subscriber 1-1-3-1/gpononu
1 profiles displayed
```

» **Criando um perfil CPE WLAN-COM-ADV (opcional)**

Esse passo é opcional. O perfil comum WLAN na seção anterior cobre as configurações comuns que podem ser utilizadas nas portas WLAN 1 a 4. O perfil comum avançado WLAN dessa seção cobre as configurações avançadas que podem ser utilizadas somente na interface WLAN 1.

> **Observação:** o perfil comum avançado WLAN somente poderá ser removido quando não estiver associado a nenhum perfil de assinante WLAN

Comando:

```
cpe wlan common advance add <profile-name <string>>
[ channel < auto | c1 | c2 | c3 | c4 | c5 | c6 | c7 | c8 | c9 | c10 | c11 | c12 | c13 > ]
[ auto-chan-timer < value > ]
[ 802dot11n-mode < auto | disabled > ]
[ 802dot11n-rate < auto | use54g | 6.5m | 13m | 19.5m | 26m | 39m | 58.5m | 65m | 78m | 104m | 117m | 130m > ]
[ 802dot11n-protect < auto | disabled > ]
[ 802dot11n-client-only < enabled | disabled > ]
[ 54g-rate < auto | 1m | 2m | 5.5m | 6m | 9m | 11m | 12m | 18m | 24m | 36m | 48m | 54m > ]
[ mcast-rate < auto | 1m | 2m | 5.5m | 6m | 9m | 11m | 12m | 18m | 24m | 36m | 48m | 54m > ]
[ basic-rate < default | all | 1n2m | std-rates > ]
[ fragment-threshold < 256 - 2346> ]
[ rts-threshold < 0-2347> ]
[ dtim-interval < 1-255> ]
[ beacon-interval < 1-65535 > ]
[ global-max-clients < 1-128 > ]
[ xpress-tech < enabled | disabled > ]
[ tx-power < 1-100 > ]
[ wmm < enabled | disabled > ]
[ wmm-no-ack < enabled | disabled > ]
[ wmm-apsd < enabled | disabled > ]
[ ap-mode < accesspoint | wirelessbridge > ]
[ bridge-restrict < enabled | enabledscan | disabled > ]
[ wps < enabled | disabled > ]
[ wps-add-client-method < push-button | station-pin| ap-pin > ]
[ wps-ap-mode < configured | unconfigured > ]
```

Esse comando cria um novo perfil. O <profile-name> deve ser fornecido e deve ser exclusivo para o tipo de perfil. O índice de perfil será gerado automaticamente.

A tabela a seguir fornece a descrição para as opções do comando *cpe wlan common add.*

Opção	Descrição
profile-name <string>	Especifica um nome exclusivo do perfil wlan-com-adv. Deve possuir no máximo 36 caracteres.
channel value	Define o canal wireless a ser utilizado. A opção 'auto' seleciona automaticamente um canal com baixa interferência. 802.11b e 802.11g utilizam canais para limitar a interferência de outros dispositivos. Valores: auto, c1, c2, c3, c4, c5, c6, c7, c8, c9, c10, c11, c12, c13 Padrão: *auto*
auto-chan-timer value	Quando configurado no modo auto, esse temporizador especifica a frequência (em minutos) para analisar novamente o espectro para selecionar um canal com baixa interferência. Observação: o novo escaneamento automático de canais somente ocorrerá quando não houver dispositivos ativos conectados. Valores: *0-2147483647* Padrão: 15
802dot11n-mode value	Modo de operação 802.11n MIMO EWC. 802.11n melhora as taxas de dados via MIMO (multiple-input, multiple-output) utlizando streams espaciais, cada um com largura de canal de 40 MHz ou 20 MHz. A utilização de 802.11n no modo 2.4 GHz depende da interferência com outros sistemas 802.11 ou sistema bluetooth na mesma frequência. Enhanced Wireless Consortium (EWC) fornece melhorias adicionais (adicionando a capacidade de definir canais de 20 MHz). Valores: auto, disabled Padrão: *auto*
802dot11n-rate value	Taxas 802.11n MIMO suportadas, em Mbps. Valores: auto, use54g, 6.5m, 13m, 19.5m, 26m, 39m, 58.5m, 65m, 78m, 104m, 117m, 130m Padrão: *auto*
802dot11n-protect value	Modos de proteção 802.11n MIMO. Valores: auto, disabled Padrão: *auto*
802dot11n-client-only value	Ativa ou desativa a restrição de acesso somente para clientes 802.11n. Quando ativado, evita a conexão de clientes 802.11 b/g. Valores: enabled, disabled Padrão: *disabled*
54g-rate value	A taxa quando o rádio opera no modo 802.11 b/g. Esse parâmetro somente se aplica quando a Taxa Multiple Input Multiple Output (MIMO) 802.11n é configurada como use54g. Valores: auto, 1m, 2m, 5.5m, 6m, 9m, 11m, 12m, 18m, 24m, 36m, 48m, 54m Padrão: *1m*
mcast-rate value	Taxa para tráfego multicast. Valores: auto, 1m, 2m, 5.5m, 6m, 9m, 11m, 12m, 18m, 24m, 36m, 48m, 54m Padrão: *auto*
basic-rate value	Taxa quando o rádio opera no modo básico 802.11 b/g. Valores: default, all, 1n2m, std-rates Padrão: *default*
fragment-threshold value	Limiar a partir do qual os pacotes são fragmentados. Valores: 256-2346 Padrão: *2346*
rts-threshold value	Tamanho do pacote de um request-to-send (RTS). Um limiar baixo implica que os pacotes RTS são enviados mais frequentemente, precisando de mais largura de banda, mas garantindo a transmissão de pacotes em uma rede ocupada. Valores: 0-2347 Padrão: *2347*
dtim-interval value	O intervalo em que as mensagens DTIM (Delivery Traffic Indication Messages) são geradas. Uma mensagem DTIM avisa a um cliente sem fio que um pacote está esperando para ser transmitido. Valores: 1-255 Padrão: *1*
beacon-interval value	O intervalo em que Beacons são gerados. Valores: 1-65535 Padrão: *100*
global-max-clients value	O número máximo de dispositivos clientes sem fio que podem estar conectados simultaneamente ao rádio. Esse valor deve incluir a soma total de todas as SSID ativas. Valores: 1-128 Padrão: *50*
xpress-tech value	Ativa ou desativa a Tecnologia XPress(TM). Valores: enabled, disabled Padrão: *disabled*

tx-power value	A porcentagem de energia total que deve ser utilizada na transmissões. Valores: 0-100 Padrão: *100*
wmm value	Ativa ou desativa o Wifi Multimedia. Se está ativado, os dados das aplicações de voz, vídeo e áudio têm prioridade em relação a outros tráfegos da rede. Valores: enabled, disabled Padrão: *enabled*
wmm-no-ack value	Ativa ou desativa a supressão de confirmação (acknowledgements) para quadros que não exigem uma confirmação (acknowledgements) QoS. Isso evita a transmissão desnecessária de confirmações para dados com nível crítico. Valores: enabled, disabled Padrão: *enabled*
wmm-apsd value	Ativa ou desativa o método de gerenciamento de energia Automatic Power Save Delivery (APSD). Essa função é útil para aplicações bidirecionais, como telefones VoIP. Valores: enabled, disabled Padrão: *enabled*
ap-mode value	Modos de operação Wireless: ponto de acesso e WDS ou somente WDS. Valores: access-point, wireless-bridge Padrão: *access-point*
bridge-restrict value	Modo de operação de restrição de bridge. Valores: enabled, enabled-scan, disabled Padrão: *disabled*
wps value	Ativa ou desativa o método de segurança WPS (WiFi Protected Setup). Se WPS está ativado, o método de autenticação da rede, a criptografia de dados e a chave da rede também devem ser configuradas para fazer a autenticação nessa rede sem fio. Está disponível para WPA-PSK, WPA2-PSK, WPA2/WPA-PSK Mixed e open (autenticação de rede aberta). Valores: enabled, disabled Padrão: *disabled*
wps-add-client-method value	Um cliente pode ser adicionado por três métodos diferentes: botão, pin de estação, ou pin de ponto de acesso. Valores: push-button, sta-pin, ap-pin Padrão: *push-button*
wps-ap-mode value	Se o provedor está utilizando um registro externo para segurança, selecione "Configured". O PIN para o modo AP é especificado pelo registrador. Forneça esse PIN ao cliente. Emita "Config AP" para começar o processo de registro com o cliente. Valores: configured, unconfigured Padrão: *configured*

Opções e descrições do comando wlan-com-adv add

1. Crie o perfil comum avançado WLAN;

```
iSH> CPE> WLAN> COM-ADV> add plan1 802dot11n-rate auto 802dot11n-client-only
disabled 54g-rate 1m mcast-rate auto basic-rate default xpress-tech disabled tx-power 100 wmm
enabled
Profile "plan1" has been created with index 4
```

2. Exiba os perfis comuns avançados WLAN;

```
iSH> CPE> WLAN> COM-ADV> show all
                                    802.11n   802.11n    54G   Mcast    Basic              Tx
Index  Profile Name          Channel    Rate      Only     Rate   Rate     Rate     Xpress   Pwr     WMM
1      Default_Cpe_WlanAdv   auto       26m     enabled    auto   12m      all     enabled   80   disabled
2      plan1                 auto       auto    disabled   1m     auto     default disabled  100  enabled
2 entries found.
```

3. Se os usuários desejam remover um perfil comum avançado WLAN, utilize o comando *cpe wlan com-adv delete <profile-index> | <profile-name>;*

```
iSH> CPE> WLAN> COM-ADV> delete 2
Profile has been deleted.
```

4. Os usuários podem utilizar o comando *find* para encontrar o perfil de assinante WLAN associado.

Esse exemplo assume que o perfil comum avançado WLAN 1 está associado a um perfil de assinante da ONT 1/3/1:

```
iSH> CPE> WLAN> COM-ADV> find 1
cpe-wlan-subscriber 1-1-3-1/gpononu
1 profiles displayed
```

Configurações padrão do nível de sistema CPE

As configurações padrão de nível de sistema CPE em uma ONT incluem:

- » Configurações de firewall.
- » Configurações sync-cookie-protection.
- » Configurações de cross VLAN routing.
- » Configurações de perfil de lista de rotas estáticas.
- » Configurações de perfil de lista de hosts DNS.
- » Configurações do TR-069, incluindo Username, Password, ACS URL, etc.
- » Gerenciamento do controle de acesso das ONTs: Admin, Support e User.

Estas configurações estão listadas no perfil comum de sistema CPE. Existe um perfil comum padrão de sistema CPE aplicado a todas as ONT no sistema. É possível modificar as configurações padrão se assim desejar, ou criar um novo perfil comum de sistema CPE e depois aplicá-lo à ONT.

> **Observação:** o perfil comum de sistema CPE somente poderá ser removido quando não estiver associado a nenhum perfil de sistema CPE

Para criar um perfil comum de sistema CPE, utilize o comando *cpe system common add*. Para aplicar o novo perfil comum de sistema CPE a uma ONT, utilize o comando *cpe system add.*

A tabela a seguir fornece a descrição para as opções do comando *cpe system common add.*

O comando *cpe system common modify* possui a mesma sintaxe.

Opção	Descrição
profile-name	Nome do perfil system-comom.
firewall value	Ativação ou desativação do firewall. A ativação do firewall pode proteger a ONT de invasões indesejadas. Quando o firewall está ativado, as conexões entrantes podem ser permitidas seletivamente através do firewall e configurações de encaminhamento de portas. Valores: enabled, disabled Padrão: *enabled*
sync-cookie-protection value	Protege contra ataques maliciosos que tentam utilizar TCP handshaking. Valores: enabled, disabled Padrão: *enabled*
cross-vlan-routing value	Se "enabled" é selecionado, é permitido o roteamento entre as VLAN. As buscas na tabela de roteamento ignoram a VLAN das portas de entrada e saída. Se houver uma correspondência, o pacote é enviado para a interface especificada na tabela de roteamento, independente da VLAN a que pertence. Se "disabled" é selecionado, os pacotes serão enviados para a Rota Padrão configurada para a VLAN onde chegaram, a menos que exista uma correspondência na tabela de roteamento dentro da mesma VLAN. O roteamento de pacotes entre as VLAN é evitado, fornecendo o isolamento do tráfego. Valores: enabled, disabled Padrão: *disabled*
static-route-list-profile value	Endereço do perfil static-route-list associado a essa ONT. Por padrão, não há um perfil static-route-list-profile criado.
dns-host-list-profile name	Índice do perfil dns-host-list associado a essa ONT, ou 0 se não existe. Padrão: *0*
tr69-inform value	Ativa ou desativa a geração de mensagens de informação para o TR-069 ACS (Auto Configuration Server). Valores: enabled, disabled Padrão: *enabled*
inform-interval seconds	Intervalo periódico (em segundos) em que as mensagens de Informação serão geradas. Isso é um parâmetro relacionado a TR-069. Padrão: *300*
acs-url value	Contém o endereço da página web do TR-069 ACS. Se a URL inclui um nome de domínio, o DNS deve estar ao alcance para resolver o nome de domínio. String com 256 caracteres no máximo.
acs-username username	Nome de usuário necessário para acessar o TR-069 ACS. String com máximo de 64 caracteres.
acs-password password	Senha de usuário necessária para acessar o TR-069 ACS. String com máximo de 64 caracteres.
admin-password password	Senha da conta "admin" na ONT. O padrão é intelbras, ou seja, o valor padrão existente na ONT não será sobrescrito. String com no máximo 16 caracteres. A conta "admin" possui acesso total para alterar e visualizar configurações da ONT, assim como a possibilidade de realização de diagnóstico.

support-password password	Senha da conta "support" na ONT. O padrão é intelbras. String com no máximo 16 caracteres. A conta "support" é utilizada para acessar a ONT para manutenção e execução diagnósticos, mas o usuário support não possui acesso total às telas de configuração.
user-password password	Senha da conta "user" na ONT. O padrão é user. String com no máximo 16 caracteres. A conta "user" pode acessar a ONT, visualizar um conjunto limitado de configurações e estatísticas, assim como atualizar o software da ONT.

Opções de descrições do comando system common add

Configurando o perfil comum de sistema CPE e aplicando-o a uma ONT

1. Exiba as configurações comuns padrão de sistema CPE:

```
iSH> CPE> SYSTEM> COMMON> show 1
                                    Sync Cookie       Cross VLAN    Static Rte    Dns Host     TR69      Inform
Index       Profile Name       Firewall  Protection     Routing        List          List      Inform   Interval
1     Default_Cpe_System_Common  enabled   enabled   disabled         0             0      enabled       300
Acs URL              :
Acs Username         :
Power Supply         : 0
Power Shutdown Delay : 0
Power Restore Delay  : 0
1 entries found.
```

2. Crie um novo perfil comum de sistema CPE:

```
iSH> CPE> SYSTEM> COMMON> add firewalldisable_System_Common
Cpe System Common profile "firewalldisable_System_Common" has been created with index 2
```

3. Modifique as configurações padrão;

```
iSH> CPE> SYSTEM> COMMON> modify firewalldisable_System_Common firewall disabled user-password 1234
Cpe System Common profile has been modified
```

4. Aplique o novo perfil comum a ONT 1/3/1:

```
iSH> CPE> SYSTEM> add 1/3/1 sys-common-profile firewalldisable_System_Common
System profile "1/3/1" has been created

iSH> CPE> SYSTEM> show 1/3/1
CPE              SYSTEM COMMON PROFILE
1/3/1            firewalldisable_System_Common/2
1 entries found.
```

Removendo um perfil comum de sistema CPE

Se deseja remover um perfil comum de sistema CPE, assegure-se primeiro de que nenhuma ONU esteja utilizando-o.

1. Para descobrir qual ONT está utilizando o perfil comum de sistema CPE:

```
iSH> CPE> SYSTEM> COMMON> find firewalldisable_System_Common
cpe-system 1-1-3-1/gpononu
1 profiles displayed
```

2. Remova o sistema CPE e depois poderá remover o perfil comum de sistema CPE:

```
iSH> CPE> SYSTEM> delete 1/3/1
Cpe System profile has been deleted.

iSH> CPE> SYSTEM> COMMON> delete firewalldisable_System_Common
Cpe System Common profile has been deleted.
```

» **Criando um perfil comum IP para a WAN**

O perfil comum IP padrão (ex. Default_Cpe_Ip_Server) especifica DHCP como a opção do campo host IP option. Isso indica que a ONT receberá o endereço IP automaticamente do servidor DHCP.

> **Observação:** o perfil comum IP padrão somente poderá ser removido quando não estiver associado a nenhum perfil CPE IP

Comando:

```
cpe rg wan ip-com add <profile-name>
[ host-ip-option < dhcp | static > ] [ netmask < value > ]
[ gateway < IP address > ]
[ primary-dns < IP address > ]
[ secondary-dns < IP address > ]
[ nat < nat | napt | disabled > ]
[ secure-fwd < enabled | disabled > ]
[ firewall-access < http | ping | snmp | snmptrap | ssh | telnet | all | none > ]
[ default-iface < true | false > ]
[ dns-src < true | false > ]
```

Opção	Descrição
profilename	Especifica um nome único para o perfil CPE RG WAN IP.
host-ip-option <dhcp| static>	Seleciona a opção relacionada ao IP. DHCP ou static. Se DHCP é selecionado, isso indica que ONT obterá o endereço IP automaticamente do servidor DHCP. Padrão: *DHCP*
netmask <value>	Especifica a máscara de sub-rede da ONT para os serviços IP.
gateway <IP address>	Especifica o endereço do gateway padrão utilizado pela ONT para os serviços IP. Padrão: *0.0.0.0*
primary-dns <IP address>	Especifica o endereço DNS primário. Se o valor é 0.0.0.0, não há um DNS primário definido. Padrão: *0.0.0.0*
secondary-dns <IP address>	Especifica o endereço DNS secundário. Se o valor é 0.0.0.0, não há um DNS secundário definido. Padrão: *0.0.0.0*
nat <nat | napt | disabled>	Quando NAT ou NAPT é selecionado, a função NAT/NAPT é executada para fazer a tradução entre o endereço IP público e endereços privados. Somente é suportado na interface WAN Padrão: *nat*
secure-fwd <enabled| disabled>	Quando o modo de encaminhamento seguro está ativo, os pacotes não são enviados a todas as portas. Ao invés disso, todos os pacotes são enviados à porta designada como porta de uplink. Nesse modo, os usuários não podem comunicar-se diretamente uns com outros, e os quadros broadcast são descartados. Padrão: *disabled*
firewall-access <http| ping | snmp |snmptrap |ssh |telnet |all |none>	Lista os protocolos permitidos na interface. A opção firewall deve estar ativada antes de que essas configurações sejam aplicadas.
default-iface <true| false>	Quando true for configurado, um pacote gerado internamente (ex. trap SNMP, SNTP, etc.) é enviado por essa itnerface se o endereço IP de destino não está definido na tabela de roteamento. O valor padrão é false. Padrão: *false*
dns-src <true| false>	Especifica a origem das informações DNS. Quando é configurada como true, a interface é utilizada pelo cliente DHCP para obter informações de DNS. Padrão: *false*

Opções e descrições do comando cpe rg wan ip-com

O exemplo a seguir cria um perfil comum IP para serviços de dados:

1. Crie um perfil comum IP com nome IPserver. O índice de perfil será gerado automaticamente;

```
iSH> CPE> RG> WAN> IP-COM> add IPserver host-ip-option static netmask
255.255.255.0 gateway 172.168.3.254 primary-dns 172.168.19.1
Profile "IPserver" has been created with index 2
```

2. Exiba o perfil comum IP configurado;

```
iSH> CPE> RG> WAN> IP-COM> show all
                                host IP                                  secure default
Index   Profile Name                  option      gateway      igmp fn   nat     fwd     iface    dns src   dns type
1       Default_Cpe_Ip_Server         dhcp        0.0.0.0      none      nat     disabl  false    false     default
2       IPserver                      static      172.168.3.254 none     nat     disabl  false    false     default
100001 default-lan-ip-server100001    static      0.0.0.0      none      disabl  disabl  false    false     default
3 entries found.
```

3. Se deseja remover um perfil comum IP criado, utilize o comando delete com o índice ou nome do perfil.

```
iSH> CPE> IP> IP-COM> delete IPserver
Profile has been deleted.
```

Configurações IP-COM LAN

» **Criando um perfil comum IP para a LAN**

O perfil comum IP padrão (ex.default-lan-ip-server100001) especifica static como a opção do campo host IP option. Isso indica que a ONT terá o endereço IP do host estático.

> **Observação:** o perfil comum IP somente poderá ser removido quando não estiver associado a nenhum perfil CPE IP

Comando:

```
cpe rg lan ip-com add <profile-name>
[ host-ip-option < dhcp | static > ]
[ netmask < value > ]
[ gateway < IP address > ]
[ primary-dns < IP address > ]
[ secondary-dns < IP address > ]
[ igmp-function < none | snooping | proxy | snoopingproxy> ]
[ firewall-access < http | ping | snmp | snmptrap | ssh | telnet | all | none > ]
[ dns-type < default | static | proxy > ]
```

Opção	Descrição
profilename	Especifica um nome único para o perfil CPE RG LAN IP.
host-ip-option <dhcp| static>	Seleciona a opção relacionada ao IP. DHCP ou static. Se DHCP é selecionado, isso indica que ONT obterá o endereço IP automaticamente do servidor DHCP. Padrão: *static*
netmask <value>	Especifica a máscara de sub-rede da ONT para os serviços IP.
gateway <IP address>	Especifica o endereço do gateway padrão utilizado pela ONT para os serviços IP. Padrão: *0.0.0.0*
primary-dns <IP address>	Especifica o endereço DNS primário. Se o valor é 0.0.0.0, não há um DNS primário definido. Padrão: *0.0.0.0*
secondary-dns <IP address>	Especifica o endereço DNS secundário. Se o valor é 0.0.0.0, não há um DNS secundário definido. Padrão: *0.0.0.0*
igmp-function <none| snooping | proxy | snoopingproxy>	Ativa a função IGMP. Padrão: *none*
firewall-access <http| ping | snmp |snmptrap |ssh |telnet | all |none>	Lista os protocolos permitidos na interface. A opção firewall deve estar ativada antes de que essas configurações sejam aplicadas.
dns-type <default| static | proxy>	Especifica o tipo de DNS: Default - Obtem as informações DNS da interface WAN, Static - As informações DNS são fornecidas manualmente, Proxy - Possibilita que a interface aja como proxy para solicitações DNS Padrão: *default*

Opções e descrições do comando cpe rg lan ip-com

O exemplo a seguir cria um perfil comum IP para serviços de dados:

1. Crie um perfil comum CPE IP com nome LANIPserver. O índice de perfil será gerado automaticamente;

```
iSH> CPE> RG> LAN> IP-COM> add LANIPserver host-ip-option static netmask
255.255.255.0 gateway 172.168.3.254 primary-dns 172.168.19.1
Profile "IPserver" has been created with index 3
```

2. Exiba os perfis comuns padrão CPE IP e perfis comuns CPE IP criados pelo usuário;

```
iSH> CPE> RG> LAN> IP-COM> show all
```

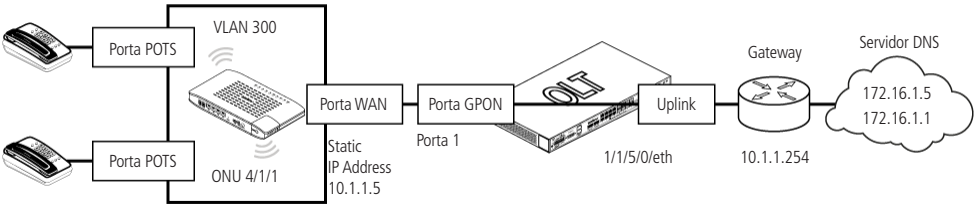
Index	Profile Name	Host IP option	gateway	secure default igmp	fn nat	fwd	iface	dns src	dns type
1	Default_Cpe_Ip_Server	dhcp	0.0.0.0	none	nat	disabl	false	false	default
2	IPserver	static	172.168.3.254	none	nat	disabl	false	false	default
3	LANIPserver	static	0.0.0.0	none	disabl	disabl	false	false	default
100001	default-lan-ip-server100001	static	0.0.0.0	none	disabl	disabl	false	false	default

4 entries found.

3. Se deseja remover um perfil comum IP, utilize o comando delete com o índice ou nome do perfil.

```
iSH> CPE> IP> IP-COM> delete LANIPserver

Profile has been deleted.
```

Configuração estática das interfaces do lado WAN (sem DHCP)



Configuração estática das interfaces WAN

Atribuição de um endereço IP estático para a interface WAN da ONT

Para atribuir um endereço IP estático à interface WAN, utilize o procedimento a seguir:

1. Crie serviços na ONT com o comando bridge add (utilizando os padrões de sistema);
2. Verifique os serviços criados na ONT:

```
iSH> bridge show
```

Type	Orig VLAN/SLAN	VLAN/SLAN	Physical	Bridge	St Table Data
dwn	Tagged	100	1/1/3/1/gpononu	1-1-3-303-gponport-100/bridge	UP D 00:02:71:19:4b:28
dwn	Tagged	200	1/1/3/1/gpononu	1-1-3-403-gponport-200/bridge	UP
dwn	Tagged	300	1/1/3/1/gpononu	1-1-3-501-gponport-300/bridge	UP D 00:02:71:19:4b:29
					D 00:02:71:19:4b:28
upl	Tagged	100	1/1/5/0/eth	ethernet5-100/bridge	UP S VLAN 100 default
upl	Tagged	200	1/1/5/0/eth	ethernet5-200/bridge	UP S VLAN 200 default
upl	Tagged	300	1/1/5/0/eth	ethernet5-300/bridge	UP S VLAN 300 default

6 Bridge Interfaces displayed

```
iSH> bridge show onu
        GEM   ONU     DSCP    ONU UNI OLT           OLT
ONU     Port  UNI     to COS VLAN/SLAN VLAN/SLAN   G-VLAN MVR  Service Rg-Mode OLT Bridge          ST
1/3/1   303   eth 1           Tagged 100----        data   B-Routed 1-1-3-303-gponport-100/bridge  DWN
1/3/1   303   wlan 1          Tagged 100----        data   B-Routed 1-1-3-303-gponport-100/bridge  -
1/3/1   403   eth 2           Tagged 200----        iptv    Bridged 1-1-3-403-gponport-200/bridge  DWN
1/3/1   501   pots            Tagged 300----        sip      Bridged 1-1-3-501-gponport-300/bridge UP
3 Bridge Interfaces displayed
4 GPON ONU Connections displayed
```

3. Verifique as configurações padrão das configurações de voz acima na interface WAN:

```
iSH> cpe> rg> wan > show 1/3/1 vlan 300
                                                    Retry      Ip-Com   Port-Fwd
CPE     VLAN/SLAN      RG Mode    IP Address  Auth  Interval   Profile  List Profile  G-VLAN
1/3/1   300/----       Bridged          dhcp -      -          1        0             -
Pppoe User Id: --
3 services displayed
```

4. Prepare a configuração de IP estático para o sistema:

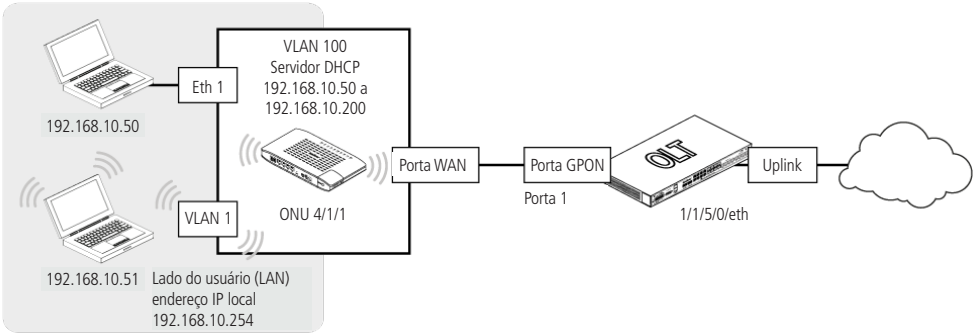
```
iSH> CPE> RG> WAN> IP-COM> add static-ip-config-1 host-ip-option static gateway
10.1.1.254 netmask 255.255.255.0 primary-dns 172.16.1.5 secondary-dns 172.16.5.11
Profile "static-ip-config-1" has been created with index 3
```

5. Aplique as configurações personalizadas de IP na interface WAN:

```
iSH> CPE> RG> WAN> modify 1/3/1 vlan 300 ip-com-profile static-ip-config-1 ip-addr 10.1.1.5
Service has been modified

iSH> CPE> RG> WAN> show 1/3/1 vlan 300
                                                    Retry      Ip-Com   Port-Fwd
CPE     VLAN/SLAN      RG Mode    IP Address  Auth  Interval   Profile  List Profile   G-VLAN
1/3/1   300/----       Bridged      10.1.1.5 -      -          3        0              -
Pppoe User Id: --
1 services displayed
```

Pode-se configurar um IP do lado da LAN e um servidor DHCP se a ONT estiver no modo rg-brouted ou rg-bpppoe. Essa seção configura as interfaces LAN Brouted com a mesma VLAN:

- » Atribuir um endereço IP estático como endereço IP local das interfaces LAN
- » Alterar a faixa de endereço IP do servidor DHCP
- » Alterar as configurações de acesso ao firewall nas interfaces LAN



Configuração estática das interfaces LAN

Atribuição de um endereço IP estático para a interface LAN da ONU

1. Crie serviços na ONT com o comando bridge *add* (utilizando os padrões de sistema);
2. Verifique os serviços criados na ONT;

```
iSH> bridge show
        Orig
Type  VLAN/SLAN   VLAN/SLAN Physical          Bridge                            St Table Data
dwn             Tagged 100     1/1/3/1/gpononu   1-1-3-303-gponport-100/bridge     UP D
dwn             Tagged 200     1/1/3/1/gpononu   1-1-3-403-gponport-200/bridge     UP D
dwn             Tagged 300     1/1/3/1/gpononu   1-1-3-501-gponport-300/bridge     UP D
upl             Tagged 100     1/1/5/0/eth       ethernet5-100/bridge              UP S VLAN 100 default
upl             Tagged 200     1/1/5/0/eth       ethernet5-200/bridge              UP S VLAN 200 default
upl             Tagged 300     1/1/5/0/eth       ethernet5-300/bridge              UP S VLAN 300 default
6 Bridge Interfaces displayed

 iSH> bridge show onu
        GEM   ONU     DSCP   ONU UNI OLT          OLT
 ONU    Port  UNI     to COS VLAN/SLAN VLAN/SLAN  G-VLAN MVR  Service Rg-Mode OLT Bridge         ST
 1/3/1  303   eth 1          Tagged 100----       data   B-Routed 1-1-3-303-gponport-100/bridge DWN
 1/3/1  303   wlan 1         Tagged 100----       data   B-Routed 1-1-3-303-gponport-100/bridge -
 1/3/1  403   eth 2          Tagged 200----       iptv    Bridged 1-1-3-403-gponport-200/bridge DWN
 1/3/1  501   pots           Tagged 300----       sip     Bridged 1-1-3-501-gponport-300/bridge UP
 3 Bridge Interfaces displayed
 4 GPON ONU Connections displayed
```

Como vimos acima, os serviços de dados são criados na Eth1 e WLAN 1 com conexões brouted, e ambas as interfaces estão na VLAN 100.

3. Verifique as configurações padrão das configurações de dados acima:

```
iSH> cpe> rg> wan > show 1/3/1 vlan 100
                                                    Retry     Ip-Com   Port-Fwd
CPE    VLAN/SLAN      RG Mode    IP Address  Auth    Interval  Profile  List Profile    G-VLAN
1/3/1  100/----       B-Routed          dhcp  -       -         1        0               -
Pppoe User Id: --
1 services displayed

 iSH> CPE> RG> LAN> show 1/3/1 vlan 100
                                                                  IP Com   Dhcp Srvr
CPE    UNI     UNI-VLAN/SLAN    VLAN/SLAN   G-VLAN   IP-Address   Profile  Profile    Rg-Mode
1/3/1  eth 1                    Tagged 100  -        192.168.1.1  100001   100001     B-Routed
1/3/1  wlan 1                   Tagged 100  -        192.168.1.1  100001   100001     B-Routed
Services displayed: 2
```

4. Crie um perfil comum IP:

```
iSH> CPE> RG> LAN> IP-COM> add hsi-lan host-ip-option static netmask 255.255.255.0 firewall-
--access all
Profile "hsi-lan" has been created with index 4

 iSH> CPE> RG> LAN> IP-COM> show hsi-lan
                              host IP                                          secure
 Index  Profile Name          option      gateway     igmp fn  nat    fwd   firewall-access

 4      hsi-lan               static      0.0.0.0       none    nat   disabl
 http+ping+snmp+snmptrap+ssh+telnet
 Net Mask: 255.255.255.0
 Primary Dns: 0.0.0.0
 Secondary Dns: 0.0.0.0
 1 entries found.
```

5. Crie um perfil de servidor DHCP:

```
iSH> CPE> RG> LAN> DHCP-SRVR> add hsi-dhcp start-addr 192.168.10.50 end-addr 192.168.10.200

Profile "hsi-dhcp" has been created with index 2
```

```
iSH> CPE> RG> LAN> DHCP-SRVR> show hsi-dhcp
Index    Profile Name              start addr          end addr       lease time
         hsi-dhcp                   192.168.10.50 192.168.10.200          -1
1 entries found.
```

6. Atribua um novo endereço IP, um novo perfil comum IP e um novo perfil de servidor DHCP para a interface LAN:

```
iSH> CPE> RG> LAN> modify 1/3/1 eth 1 vlan 100 dhcp-server-profile hsi-dhcp
ip-addr 192.168.10.254 ip-com-profile hsi-lan
Service has been modified
```

Como exibido a seguir, o endereço IP local das interfaces LAN BRouted e a faixa de endereços IP do servidor DHCP foram alterados.

```
iSH> CPE> RG> LAN> show 1/3/1 vlan 100
                                                                  IP Com   Dhcp Srvr
CPE    UNI     UNI-VLAN/SLAN   VLAN/SLAN   G-VLAN   IP-Address      Profile  Profile     Rg-Mode
1/3/1  eth 1                   Tagged 100  -        192.168.10.254  4        2           B-Routed
1/3/1  vlan 1                  Tagged 100  -        192.168.10.254  4        2           B-Routed
Services displayed: 2
```

Configuração do firewall

É possível ativar ou desativar o firewall na ONT. A ativação do firewall pode proteger a ONT de invasões indesejadas. Quando o firewall está ativado, as conexões entrantes podem ser aceitas por meio de seleção do acesso ao firewall e configurações de encaminhamento de portas. O firewall está ativado por padrão.

» **Ativação ou desativação do firewall**

Utilize o perfil comum de sistema CPE para ativar ou desativar as configurações de firewall.

1. Verifique as configurações de firewall na ONT:

```
iSH> CPE> SYSTEM> show 1/3/1
CPE        SYSTEM COMMON PROFILE
1/3/1      2/2
1 entries found.
```

```
iSH> CPE> SYSTEM> COMMON> show 2
                                                    Sync Cookie  Cross VLAN   Static Rte
Index                 Profile Name          Firewall   Protection    Routing       List
2                                          2 enabled     enabled     enabled     None/ 0
Acs URL         :

Acs Username    :
admin 1 entries found.
```

2. Modifique as configurações do firewall:

```
iSH> CPE> SYSTEM> COMMON> modify 2 firewall enabled
Cpe System Common profile has been modified
```

» **Configurando o acesso ao firewall**

O controle de acesso ao firewall gerencia os protocolos permitidos nas interfaces CPE WAN ou LAN. É preciso que a função firewall esteja ativada.

Os protocolos estão listados a seguir:

- **HTTP:** tráfego do navegador web.
- **PING:** ICMP Echo utilizado para testar a conexão.
- **SNMP:** Simple Network Management Protocol.
- **SNMP TRAP:** alarmes com o protolo Simple Network Management Protocol.
- **SSH:** Secure Shell.
- **TELNET:** suporte a Terminal Remoto.

Por padrão, todos esses protocolos estão ativados nas interfaces CPE LAN. Somente PING está ativo nas interfaces WAN. Pode utilizar o comando *cpe rg wan/lan ip-com add/modify* para configurar o acesso ao firewall nas interfaces WAN ou LAN.

> **Observação:** a modificação de um perfil comum IP iniciará a reconfiguração parcial em cada uma das ONTs que dependem desse perfil e isso pode provocar interrupções de serviço nessas ONTs

Para modificar as configurações padrão de firewall, utilize o procedimento a seguir:

1. Assegure-se de que a ONT esteja com o firewall ativado;
2. Modifique as configurações de acesso ao firewall na interface CPE WAN:
   a. Exiba as configurações de acesso ao firewall (ping) na interface CPE WAN:

```
iSH> CPE> RG> WAN> show 1/3/1
                                                Retry     Ip-Com   Port-Fwd
CPE    VLAN/SLAN     RG Mode    IP Address Auth  Interval  Profile  List Profile  G-VLAN
1/3/1  102/----      B-Routed       dhcp   -       -         1        0             -
Pppoe User Id: --
1 services displayed

iSH> CPE> RG> WAN> ip-com show 1
                             host IP                                          secure
                                                                               firewall-ac-
Index Profile Name           option       gateway      igmp fn   nat    fwd      cess
1     Default_Cpe_Ip_Server  dhcp         0.0.0.0       none     nat   enabl  ping
Net Mask: 255.255.255.0
Primary Dns: 0.0.0.0
Secondary Dns: 0.0.0.0
1 entries found.
```

   b. Esse exemplo cria um novo perfil comum IP com configurações de acesso ao firewall como ping e HTTP:

```
iSH> CPE> RG> WAN> IP-COM> add FWHTTP firewall-access ping HTTP
Profile "FWHTTP" has been created with index 2
```

   c. Aplique as novas configurações de acesso ao firewall na interface WAN:

```
iSH> CPE> RG> WAN> modify 1/3/1 ip-com-profile FWHTTP
Service has been modified
```

3. Modifique as configurações de acesso ao firewall na interface CPE LAN:
   a. Exiba as configurações padrão de acesso ao firewall (http+ping+snmp+snmptrap+ssh+telnet) na interface CPE LAN:

```
iSH> CPE> RG> LAN> show 1/3/1 eth 1
                                                                IP Com   Dhcp Srvr
CPE    UNI     UNI-VLAN/SLAN    VLAN/SLAN   G-VLAN  IP-Address     Profile  Profile      Rg-Mode
1/3/1  eth 1                    Tagged 102  -       192.168.1.1    100001   100001       B-Routed
Services displayed: 1

iSH> CPE> RG> LAN> ip-com show 100001
                                    host IP                                    secure
Index  Profile Name                 option      gateway    igmp fn   nat    fwd   firewall-access
```

```
100001  default-lan-ip-server100001  static     0.0.0.0     none     nat  disabl
http+ping+snmp+snmptrap+ssh+telnet
Net Mask: 255.255.255.0
Primary Dns: 0.0.0.0
Secondary Dns: 0.0.0.0
1 entries found.
```

b. Aplique as novas configurações de acesso ao firewall na interface LAN:

```
iSH> CPE> RG> LAN> modify 1/3/1 ip-com-profile FWHTTP
Saving this profile will trigger a partial reconfiguration on each
of the CPEs that depend on this profile and may cause service
interruptions on those CPEs
Do you want to save the profile? [yes] or [no]: yes
Do you want to exit from this request? [yes] or [no]: no
Are you sure? [yes] or [no]: yes
Service has been modified
```

```
iSH> CPE> RG> LAN> show 1/3/1 eth 1
                                                          IP Com   Dhcp Srvr
CPE    UNI     UNI-VLAN/SLAN   VLAN/SLAN  G-VLAN   IP-Address    Profile  Profile      Rg-Mode
1/3/1  eth 1                   Tagged 102  -        192.168.1.1   2        100001      B-Routed
Services displayed: 1
```

Configurando o encaminhamento de porta (PORT-FWD)

A lista de encaminhamento de portas reflete as normas de encaminhamento para as portas existentes. A lista de encaminhamento de portas somente pode ser criada em uma interface WAN com NAT ou NAPT ativo. Por padrão, não há uma lista de encaminhamento de portas associada à interface WAN.

A lista de encaminhamento de portas exige que a função firewall esteja ativada.

Para criar uma lista de encaminhamento de portas, utilize o comando *cpe rg wan port-fwd add*.

A tabela a seguir fornece a descrição para as opções do comando *cpe rg wan port-fwd add*.

Opção	Descrição
list-name	Especifica um nome único para o perfil PORT-FWD (encaminhamento de portas)
type <dmz | portrange | portremap>	Tipo de encaminhamento de porta. Valores: dmz: quando DMZ é escolhido, apenas esta regra é permitida na interface. Esta opção informa que todo o tráfego (em qualquer porta) será enviado ao endereço IP privado. Uma regra DMZ é efetivamente igual a uma regra com todas as portas incluídas. As regras com intervalos de porta são mais seguras que a regra DMZ, dado que as regras com intervalos de portas possibilitam que grupos de portas sejam abertos. portrange: esta opção informa que qualquer tráfego dentro de um intervalo de portas determinado será enviado ao endereço IP privado. portremap: esta opção indica que qualquer tráfego nessas portas serão enviados ao endereço IP privado na porta configurada. Padrão: *dmz*
start-port PortNumber	Porta inicial para configuração de intervalo de porta. Valores: 0-65535 Padrão: *0*
end-port PortNumber	Porta final para configuração de intervalo de porta. Esta opção pode ser igual a "start-port" se houver apenas uma única porta. Valores: 0-65535 (a porta final deve ser maior ou igual que porta inicial). Padrão: *0*
protocol <none | tcp |udp tcpudp | icmp | icmpv4>	Indica quais protocolos devem ser monitorados juntamente com suas respectivas portas. Valores: tcp, udp, tcp-udp, icmp, icmpv4, none. Padrão: *none*
private-port PortNumber	O número de porta ao qual deve ser enviado o tráfego. Valores: 0-65535 Padrão: *0*

private-ip IPaddress	O endereço IP ao qual deve ser enviado o tráfego. Padrão: *0.0.0.0*

Opções e descrições do comando cpe rg wan modify port-fwd

Para configurar o encaminhamento de porta, utilize o procedimento a seguir:

1. Assegure-se de que o CPE esteja com o firewall ativado;
2. Crie uma lista de encaminhamento de portas e adicione dois registros a ela:

```
iSH> CPE> RG> WAN> PORT-FWD> add port-fwd-1 type portrange start-port 80 end-port
81 protocol udp private-ip 192.168.10.2
Profile "port-fwd-1" has been created with index 1/1
iSH> CPE> RG> WAN> PORT-FWD> add port-fwd-1 type portrange start-port 5500
end-port 5500 protocol udp private-ip 192.168.10.2
Profile "port-fwd-1" has been created with index 1/2
```

```
iSH> CPE> RG> WAN> PORT-FWD> show all
Port-Fwd-List profile : port-fwd-1 (1)
ListIndex/                Start  End               Private  Private
EntryIndex   Type         Port   Port   Protocol   Port     Ip
1/1          portrange    80     81     udp        0        192.168.10.2
1/2          portrange    5500   5500   udp        0        192.168.10.2
2 entries found.
```

3. Associe a interface WAN com a lista de encaminhamento de portas. Perceba que a VLAN ID deve ser especificada.

```
iSH> CPE> RG> WAN> modify 1/3/1 vlan 102 port-fwd-list-profile 1
Service has been modified
```

Configuração do servidor DHCP

A configuração do servidor DHCP serve somente para as conexões no modo rg-brouted ou rg-bpppoe. A conexão no modo rg-bridged não precisa dessa configuração.

Depois de criar a conexão entre a GEM Port na OLT e a porta eth da ONT com o comando *bridge add*, um servidor DHCP padrão com índice 100001 é criado automaticamente para os dispositivos do lado LAN.

O servidor DHCP padrão possui as configurações a seguir:

Nome do Perfil= default-dhcp-server10001

Endereço IP inicial= 192.168.1.10

Endereço IP final= 192.168.1.100

Lease Time= 86400 segundos

Se não deseja utilizar o servidor DHCP padrão, pode criar um novo servidor DHCP para os dispositivos da LAN conforme procedimento a seguir.

Criando um novo servidor DHCP para a interface LAN

1. Crie as interfaces LAN da ONT para a conexão no modo RG-brouted;

```
iSH> bridge add 1-1-3-2/gpononu gem 302 gtp 1 downlink tagged vlan 102 eth 1 rg-brouted
```

2. Crie um novo perfil do servidor DHCP para os dispositivos da LAN da ONT:

```
CPE> RG> LAN> DHCP-SERVER> add example-dhcp start-address 192.168.10.10
end-address 192.168.10.100
Profile "example-dhcp" has been created with index 1
```

```
iSH> CPE> RG> LAN> DHCP-SRVR> show all
Index      Profile Name                  start addr      end addr          lease time
1          example-dhcp                  192.168.10.10   192.168.10.100    -1
100001     default-dhcp-server100001     192.168.1.10    192.168.1.100     86400
2 entries found.
```

3. Utilize o novo perfil do servidor DHCP na conexão RG brouted:

```
CPE> RG> LAN> modify 1/3/2 eth 1 vlan 102 dhcp-server-profile example-dhcp ip-addr 192.168.10.1
```

```
iSH> CPE> RG> LAN> show 1/3/2 vlan 102
                                                          IP Com   Dhcp Srvr
CPE    UNI     UNI-VLAN/SLAN   VLAN/SLAN  G-VLAN  IP-Address     Profile  Profile      Rg-Mode
1/3/2  eth 1                   Tagged 102 -       192.168.10.1   100001              B-Routed
Services displayed: 1
```

Configuração do nome de usuário e senha PPPoE

O Protocolo Point-to-Point over Ethernet (PPPoE) encapsula quadros PPP dentro de quadros Ethernet para criar um túnel PPPoE entre hosts conectados à ONT e a outros dispositivos da nuvem. Enquanto a Ethernet é baseada em pacotes (para que nenhuma conexão direta seja aberta), o PPP é uma conexão direta onde um dispositivo conecta-se diretamente a outro utilizando o protocolo. O PPPoE é uma conexão virtual (normalmente denominada túnel) entre dois dispositivos.

Especificando o modo *rg-bpppoe* no comando bridge *add*, pode adicionar um PPPoE em uma porta eth por VLAN. PPPoE/Bridge VLAN são similares a VLAN brouted, mas a interface do lado WAN é um cliente PPPoE que estabelece um túnel PPPoE para um BRAS de upstream. No lado LAN de um PPPoE/Bridge VLAN, todas as portas serão integrantes da mesma sub-rede IP.

A configuração da sessão PPPoE inclui os itens a seguir:

- Nome de usuário PPPoE (necessário)
- Senha PPPoE (necessária)
- Método de autenticação PPPoE (opcional, possui valor padrão)
- Intervalo de nova tentativa PPPoE (opcional, possui valor padrão)

Para configurar os itens acima, utilize o comando *cpe rg wan modify.*

A tabela a seguir fornece a descrição para as opções do comando PPPoE relacionadas ao comando *cpe rg wan modify.*

Opção	Descrição
pppoe-auth<auto | pap | chap | mschap>	Indica o protocolo de autenticação PPP a ser utilizado para a autenticação PPPoE. Valores: auto, pap, chap, mschap Padrão: *auto*
pppoe-retry-interval value	Especifica o tempo em segundos antes de fazer uma tentativa de recuperação da conexão. Valores: de 1 até 2147483647 segundos Padrão: *3*
pppoe-usr-id valor	Nome de usuário para utilizar na autenticação PPPoE. Valores: String única com no máximo 25 caracteres
pppoe-password valor	A senha para utilizar na autenticação PPPoE. Valores: String única com no máximo 25 caracteres

Opções e descrições do comando cpe rg wan modify - PPPoE

» **Especificando um nome de usuário e senha PPPoE**

1. Crie as interfaces LAN da ONT para a conexão no modo rg-bpppoe;

```
iSH> bridge add 1-1-3-2/gpononu gem 302 gtp 1 downlink tagged vlan 102 eth 1 rg-bpppoe
Adding bridge on 1-1-3-2/gpononu
Created bridge-interface-record 1-1-3-302-gponport-102/bridge
CPE Connection 1-1-3-302/gponport/1/2/0/0 has been created
```

2. Configure o nome e a senha de usuário PPPoE na interface WAN da ONT.

```
iSH> CPE> RG> WAN> modify 1/3/2 vlan 102 pppoe-usr-id smith pppoe-password
intelbras123

Service has been modified
```

```
iSH> CPE> RG> WAN> show 1/3/2 vlan 102
                                                 Retry      Ip-Com   Port-Fwd
CPE    VLAN/SLAN     RG Mode    IP Address Auth  Interval   Profile  List Profile  G-VLAN
1/3/2  102/----      B-Routed      dhcp    auto  3          1        0             -
Pppoe User Id: smith
1 services displayed
```

Configurar para o padrão de fábrica uma ONU

Para configurar uma ONU para o padrão de fábrica, pode-se utilizar o comando *onu set2default*, este comando faz com que a OLT restaure a ONU para o padrão de fábrica, após esse comando, a ONU será reiniciada automaticamente e voltará com suas configurações padrão. Esse comando é aplicável somente a ONU com suporte a provisionamento no modo RG através da OLT 8820 G.

Configure o padrão de fábrica para uma ONU:

```
iSH> onu set2default 1/4/2
```

12.4. Autoativação e autoconfiguração

As funções autoativação e autoconfiguração permitem que ONUs conectadas às portas PON sejam ativadas e configuradas automaticamente. Observe as instruções abaixo para configurar essas funções.

12.4.1 Autoativação

A função *Autoativação* permite que uma ONU conectada na rede seja automaticamente associada a uma posição livre da porta PON em que a ONU foi conectada, assim que ela for reconhecida pela OLT.

Esta função pode trabalhar juntamente com a função *Autoconfiguração*, fazendo com que a ONU seja ativada e posteriormente configurada automaticamente. Entretanto, é importante frisar que ambas as funções trabalham individualmente, podendo ou não estar habilitadas.

Para ativar a função *Autoativação*, execute o comando a seguir:

```
update cpe-cfg-global-settings auto-assign = enabled 0
```

Caso deseje desativar, execute o comando a seguir:

```
update cpe-cfg-global-settings auto-assign = disabled 0
```

É possível também ativar através do mesmo comando a função *Autoconfiguração* e *Autoativação*. Para isto, execute o comando a seguir:

```
update cpe-cfg-global-settings auto-config = enabled auto-assign = enabled 0
```

Obs.: *quando utilizada a função* Autoativação, *as ONUs conectadas às portas PON são ativadas de forma sequencial e crescente, não sendo possível o administrador da OLT determinar em qual posição a ONU será ativada.*

> **Nota:** a Intelbras recomenda que as funções *Autoativação* e *Autoconfiguração* somente sejam utilizadas em casos realmente necessários e que estas funções não fiquem habilitadas por padrão nas configurações do equipamento.

12.4.2 Autoconfiguração

A função *Autoconfiguração* permite a configuração automática de ONUs. Através desta funcionalidade é possível configurar templates, que funcionam como perfis, que serão associados a ONUs na rede PON.

Esta função pode trabalhar juntamente com a função *Autoativação*, que fará a ativação da ONU e posteriormente a Autoconfiguração fará a configuração. Entretanto, é importante frisar que ambas as funções trabalham individualmente, podendo ou não estar habilitadas.

Criando templates de Autoconfiguração

Para utilizar a função *Autoconfiguração*, primeiramente devemos configurar um template com as configurações que serão associadas à ONU assim que ela for ativada. Para isso, siga os passos a seguir:

1. Criar um template de serviço vazio, chamado TEMPLATE1:

```
iSH> srvtmpl add TEMPLATE1
Template "TEMPLATE1" has been created
```

2. Criar as bridges desejadas e adicioná-las ao template. Neste exemplo, serão criadas duas bridges, uma de dados e outra de voz:

```
iSH> bridge add TEMPLATE1 downlink vlan 200 tagged eth [1-3] rg-bpppoe
Adding bridge on TEMPLATE1
Created bridge-interface-record 1-0-0-257-gponport-200/bridge
CPE Connection 1-0-0-257/gponport/1/1/0/0 has been created
CPE Connection 1-0-0-257/gponport/1/2/0/0 has been created
CPE Connection 1-0-0-257/gponport/1/3/0/0 has been created
iSH> bridge add TEMPLATE1 downlink vlan 300 tagged sip rg-bridged
Adding bridge on TEMPLATE1
Created bridge-interface-record 1-0-0-258-gponport-300/bridge
CPE Connection 1-0-0-258/gponport/14/0/0/0 has been created
```

3. Verificar o template criado:

```
iSH> srvtmpl show TEMPLATE1
CPE 0/0/3     TEMPLATE1/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------ ------------------ ------ ----- ----- -------
257  eth 1                      0,200/----      0    up       B-PPPoE
257  eth 2                      0,200/----      0    up       B-PPPoE
257  eth 3                      0,200/----      0    up       B-PPPoE
Service: SIP
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN   Host IP      IP Srvr Prof
---- ------ ------------ ---------------- ------ --------------- ------------
258   pots                    0,300/----      0         0.0.0.0            1
```

Após a criação do template devemos criar uma regra de associação deste template em determinadas ONUs, conforme comando a seguir:

```
iSH> srvtmpl rule add R1 match-expression "model 1420G" service-template TEMPLATE1
Profile "R1" has been created with index 1
```

Neste exemplo criamos a regra R1, que indica que as ONUs modelo 1420G serão configuradas de acordo com o TEMPLATE1. Isto é, ONUs modelo 1420 G que forem ativadas na OLT receberão as bridges nas VLANs 200 para dados e 300 para voz.

Abaixo seguem os parâmetros que podem ser utilizados durante a criação das regras:

- **model:** cria regras por modelos de ONU, que podem ser: ONU110G, ONT1420G e ONT142NG. É possivel separar os modelos por vírgulas. Ex.: match-expression "model 142NG, 1420G".
  IMPORTANTE: o nome do modelo deve estar escrito em maiúsculo, conforme exemplo.
- **olt:** cria regras por portas da OLT. É possível separar por vírgulas e traços (para faixas). *Ex.: match-expression "olt 2-4,8"*

É possível também criar uma regra com o parâmetro "match-expression" vazio. Neste caso, esta regra será aplicada para qualquer ONU ativada, independentemente do modelo ou porta.

Após a criação da regra, podemos conferir se ela foi aplicada:

```
iSH> srvtmpl rule show R1
Index       Profile Name          admin-state   Service Template    priority  del-before-apply
===== ========================== =========== ================== ========== ================
1     R1                                  up            TEMPLATE1          1             true
Match Expression : model 1420G
Target UNI       :
1 entries found.
```

Ao finalizar as configurações dos templates e das regras, devemos ativar o serviço de *Autoconfiguração* através do seguinte comando:

update cpe-cfg-global-settings auto-config = enabled 0

Caso desejar, é possível desabilitar o serviço através do comando:

update cpe-cfg-global-settings auto-config = disabled 0

É possível também ativar através do mesmo comando a função *Autoconfiguração* e *Autoativação*. Para isto, execute o comando a seguir:

```
iSH> update cpe-cfg-global-settings auto-config = enabled auto-assign = enabled 0
cpe-cfg-global-settings  0
Record updated.
```

Obs.: *» A função* Autoconfiguração *adiciona as configurações de bridges às ONUs, portanto, as outras configurações como as de cpe, por exemplo, devem ser adicionadas diretamente em cada ONU ativada, quando necessário. Por exemplo, caso precise configurar um usuário PPP, é necessário configurá-lo individualmente conforme exemplo abaixo:*

cpe rg wan modify 1/1/1 vlan 200 pppoe-usr-id teste pppoe-password teste

» Caso sejam configuradas regras que se sobreponham, a última regra criada é a que terá efeito.

Nota: *a Intelbras recomenda que as funções* Autoativação *e* Autoconfiguração *somente sejam utilizadas em casos realmente necessários e que estas funções não fiquem habilitadas por padrão nas configurações do equipamento.*

Incluindo novas configurações em templates já criados

Para incluir novas configurações em templates já criados é necessário primeiramente remover as regras que utilizam o determinado template.

Seguindo o exemplo anterior, teremos que, primeiramente, remover a regra "R1", através do seguinte comando:

```
iSH> srvtmpl rule delete R1
Profile has been deleted.
```

E então podemos incluir as novas configurações no template como, por exemplo, criar uma bridge. Nesse caso, criaremos uma bridge de vídeo na VLAN 400 associada à porta LAN 4 da ONT:

```
iSH> bridge add TEMPLATE1 downlink vlan 400 tagged video 0/7 eth 4 rg-bridged
Adding bridge on TEMPLATE1
Created bridge-interface-record 1-0-0-262-gponport-400/bridge
CPE Connection 1-0-0-262/gponport/12/4/0/0 has been created
```

Podemos confirmar que a bridge foi criada no template:

```
iSH> srvtmpl show TEMPLATE1
CPE 0/0/4     TEMPLATE1/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
260  eth 1                      0,200/----      0    up       B-PPPoE
260  eth 2                      0,200/----      0    up       B-PPPoE
260  eth 3                      0,200/----      0    up       B-PPPoE
Service: IPTV
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN Admin Oper  Video Prof Rg-Mode
---- ------ ------------- ----------------- ------ ----- ----- ---------- -------
262  eth 4                    0,400/----      0    up                  Bridged
Service: SIP
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN   Host IP      IP Srvr Prof
---- ------ ------------- ----------------- ------ --------------- ------------
261   pots                    0,300/----      0         0.0.0.0            1
```

E então, recriamos a regra para associação do template nas ONUs.

```
iSH> srvtmpl rule add R1 match-expression "model 1420G" service-template TEMPLATE1
Profile "R1" has been created with index 2
```

Importante frisar que, após a alteração do template, as ONUs que já foram configuradas não serão reconfiguradas com a nova bridge criada. A nova configuração será aplicada apenas às novas ONUs, que serão ativadas. Caso tenha necessidade de incluir a nova bridge em ONUs que já foram configuradas, é necessário remover a ONU (através do comando ONU delete*) e ativá-la novamente, ou ainda, efetuar o comando* Bridge add *diretamente nas ONUs desejadas.*

Alterando Templates de Autoconfiguração

Para alterar templates já criados é necessário primeiramente remover as regras que utilizam determinado template. Seguindo o exemplo anterior, teremos que, primeiramente, remover a regra "R1", através do seguinte comando:

```
iSH> srvtmpl rule delete R1
Profile has been deleted.
```

Antes de fazermos as alterações, é interessante observarmos o que há no template.

```
iSH> cpe show virtual TEMPLATE1
CPE 0/0/1     DefaultData/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
3000  eth 1                        0,5/----      0    up       Bridged
CPE 0/0/3     TEMPLATE1/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
257  eth 1                       0,200/----      0    up       B-PPPoE
257  eth 2                       0,200/----      0    up       B-PPPoE
257  eth 3                       0,200/----      0    up       B-PPPoE
Service: IPTV
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN Admin Oper  Video Prof Rg-Mode
---- ------ ------------- ----------------- ------ ----- ----- ---------- -------
259  eth 4                      0,400/----      0    up                  Bridged
Service: SIP
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN   Host IP      IP Srvr Prof
---- ------ ------------- ---------------- ------ --------------- -----------
258   pots                      0,300/----      0         0.0.0.0           1
CPE 0/0/2     DefaultIpPhone/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
3001  eth 1        6/----             6/----      0    up       Bridged
```

E então podemos fazer as alterações necessárias. Neste caso, por exemplo, removeremos a bridge 200 da porta eth 3 das ONTs e associaremos a eth 3 à VLAN 500 em modo rg-bridged.

Removendo a bridge 200 da eth 3 no TEMPLATE1:

```
iSH> bridge delete TEMPLATE1 tagged vlan 200 eth 3
CPE Connection 1-0-0-257/gponport/1/3/0/0 has been deleted
```

Adicionando a bridge 500 na eth 3 em modo rg-bridged no TEMPLATE1:

```
iSH> bridge add TEMPLATE1 downlink tagged vlan 500 eth 3 rg-bridged
Adding bridge on TEMPLATE1
Created bridge-interface-record 1-0-0-260-gponport-500/bridge
CPE Connection 1-0-0-260/gponport/1/3/0/0 has been created
```

Após concluídas as alterações, podemos constatar se foram, de fato, inseridas no template.

```
iSH> cpe show virtual TEMPLATE1
CPE 0/0/1     DefaultData/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------ ------------------ ------ ----- ----- -------
3000  eth 1                        0,5/----      0    up       Bridged
CPE 0/0/3     TEMPLATE1/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------ ------------------ ------ ----- ----- -------
257  eth 1                      0,200/----      0    up       B-PPPoE
257  eth 2                      0,200/----      0    up       B-PPPoE
260  eth 3                      0,500/----      0    up       Bridged
Service: IPTV
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN Admin Oper  Video Prof Rg-Mode
---- ------ ------------ ----------------- ------ ----- ----- ---------- -------
259  eth 4                     0,400/----      0    up                  Bridged
Service: SIP
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN   Host IP      IP Srvr Prof
---- ------ ------------ ----------------- ------ --------------- ------------
258   pots                     0,300/----      0         0.0.0.0            1
CPE 0/0/2     DefaultIpPhone/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------ ------------------ ------ ----- ----- -------
3001  eth 1        6/----             6/----      0    up       Bridged
```

Neste caso podemos ver que a eth 3 alterou o modo de operação para *Bridged* e passou a trafegar na VLAN 500, conforme a alteração que fizemos.

Finalizadas as alterações, é necessário recriar a regra de associação do template.

```
iSH> srvtmpl rule add R1 match-expression "model 1420G" service-template TEMPLATE1

Profile "R1" has been created with index 1
```

Importante frisar que após a alteração do template as ONUs que já foram configuradas não serão reconfiguradas. A nova configuração será aplicada apenas às novas ONUs que serão ativadas. Caso tenha necessidade de alterar a bridge em ONUs que já foram configuradas, é necessário remover a ONU (através do comando onu delete) e ativá-la novamente, ou ainda, modificar diretamente nas bridges das ONUs.

Removendo templates de Autoconfiguração

Para remover templates, é necessário primeiramente remover as regras de associação do template, remover as bridges virtuais criadas pelo template e, por fim, remover o template em si. Para efetuar o procedimento, siga os passos a seguir:

1. Para visualizar as regras criadas, execute o seguinte comando:

```
iSH> srvtmpl rule show all
Index       Profile Name          admin-state   Service Template    priority  del-before-apply
===== ======================== =========== ================== ========== ================
1     R1                                 up            TEMPLATE1          1             true
Match Expression : model 1420G
Target UNI       :
1 entries found.
```

2. Verifique as regras que contenham o template que deseja excluir e remova com o seguinte comando:

```
iSH> srvtmpl rule delete R1
Profile has been deleted.
```

3. Agora precisamos remover as bridges virtuais criadas pelo template. Para visualizar as bridges criadas pelo template execute o seguinte comando:

```
iSH> cpe show virtual TEMPLATE1
CPE 0/0/1     DefaultData/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
3000  eth 1                          0,5/----      0    up       Bridged
CPE 0/0/3     TEMPLATE1/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
257  eth 1                       0,200/----      0    up       B-PPPoE
257  eth 2                       0,200/----      0    up       B-PPPoE
257  eth 3                       0,200/----      0    up       B-PPPoE
Service: IPTV
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN Admin Oper  Video Prof Rg-Mode
---- ------ ------------- ----------------- ------ ----- ----- ---------- -------
259  eth 4                     0,400/----      0    up                  Bridged
Service: SIP
GEM   UNI   UNI VLAN/SLAN  OLT VLAN/SLAN   G-VLAN   Host IP      IP Srvr Prof
---- ------ ------------- ----------------- ------ --------------- ------------
258   pots                     0,300/----      0         0.0.0.0            1
CPE 0/0/2     DefaultIpPhone/gpononu
Service: DATA
GEM   UNI   UNI-VLAN/SLAN VLAN/SLAN(COS,VID) G-VLAN Admin Oper  Rg-Mode
---- ------ ------------- ------------------ ------ ----- ----- -------
3001  eth 1        6/----              6/----      0    up       Bridged
```

4. Para remover todas as bridges virtuais criadas pelo template, execute o seguinte comando:

```
iSH> bridge delete TEMPLATE1 all
CPE Connection 1-0-0-257/gponport/1/1/0/0 has been deleted
CPE Connection 1-0-0-257/gponport/1/2/0/0 has been deleted
CPE Connection 1-0-0-257/gponport/1/3/0/0 has been deleted
1-0-0-257-gponport-200/bridge delete complete
CPE Connection 1-0-0-259/gponport/12/4/0/0 has been deleted
1-0-0-259-gponport-400/bridge delete complete
CPE Connection 1-0-0-258/gponport/14/0/0/0 has been deleted
1-0-0-258-gponport-300/bridge delete complete
3 bridge interfaces deleted out of 3 found
```

Importante: *a remoção dessas bridges virtuais não implica na remoção das bridges reais visualizadas através do comando* Bridge show.

5. Por fim, podemos remover o template desejado.

```
iSH> srvtmpl delete TEMPLATE1
Template "TEMPLATE1" has been deleted
```

12.5. Gerenciamento da ONU com OMCI

Atualizações do software da ONU

Atualização manual de uma ONU

A função de atualização de imagem da ONU através do protocolo OMCI possibilita ao administrador da OLT 8820 G atualizar manualmente o firmware de uma ONU. Antes de realizar o download do arquivo de imagem para a ONU, certifique-se que a imagem exista dentro da OLT 8820 G. O padrão OMCI define duas entidades gerenciadas para arquivos de imagem, denominadas como partições 0 e 1.

Essas ações são suportadas pela função de atualização manual da imagem por OMCI:

- **Download (baixar)**
  Fazer download de um arquivo de imagem da OLT para o ONU.
- **Activate (ativar)**
  Reiniciar utilizando uma imagem da partição especificada.
- **Commit (utilizar)**
  Configurar a imagem da partição especificada como padrão de reinício.
- **Abort (abortar)**
  Cancela o download solicitado.

De acordo com o padrão OMCI, o download somente é permitido em uma partição não ativa. Do mesmo modo, a ativação e utilização somente são permitidas se a partição é válida.

Antes de atualizar a imagem da ONU é necessária a utilização de um servidor TFTP para transferência da imagem para a OLT. Para transferir o arquivo de imagem para a OLT, execute o comando a seguir:

file download <ip_do_servidor_TFTP> <nome_do_arquivo_de_imagem> <diretorio_destino_na_OLT>

Exemplo: file download 192.168.10.110 1420.img /card1/1420.img

Depois de realizar o dowload do arquivo de imagem com sucesso, a ONU verifica automaticamente se a imagem é válida. Somente arquivos válidos podem ser ativados.

Atualize a imagem do firmware da ONU pela OLT 8820 G com o comando *onu image*.

onu image slot/olt/onu download filename | activate | commit |

download-activate filename | download-activate-commit filename | abort | show [part partition#]

A tabela a seguir fornece a descrição para as opções do comando *gpononu image*.

Opção	Descrição
download filename [part partition#]	Baixar um arquivo de imagem para a ONU a partir da OLT. O número da partição é opcional. O arquivo de imagem será baixado na partição que não está em uso (standby). Após o download, a ONU validará o arquivo.
activate [part partition#]	Inicializa o arquivo válido da partição em standby da ONU. O número da partição é opcional. Somente pode haver uma partição ativa por vez.
commit [part partition#]	Especifica um arquivo padrão para inicializar da próxima vez que a ONU for ligada. O número da partição é opcional. O arquivo será relacionado à partição não utilizada. Somente pode haver uma partição utilizada por vez.
download-activate filename [part partition#]	Faça o download e, se o arquivo passar pelo teste de validação, faça a ativação. O número da partição é opcional.
download-activate-commit filename [part partition#]	Execute as ações de download e ativação, e se a ONU permitir depois, selecione para utilizar. Se isso não ocorrer dentro de um período, haverá a ocorrência de erro. O número da partição é opcional.
abort	Cancela o download solicitado.
show	Exibe as configurações dos arquivos baixados. Pode visualizar a versão do arquivo, o status de validação, o status de ativação e o status de utilização de cada partição. Também apresenta o status de download, o ID do modelo da ONU, o horário de início da atualização, se foi ativada ou não, se será utilizada ou não e o tipo de atualização.
part partition#	Pode ter dois arquivos de imagem armazenados na ONU. Um na partição 0 e um na partição 1.

Opções e descrições do commando onu image

Os exemplos a seguir descrevem algumas configurações comuns durante a atualização de imagens GPON na ONU:

1. Baixe o arquivo *1420.img* que está na OLT para a ONU 1/3/1, e a ative. Utilize o comando *gpononu image slot/olt/onu download-active-commit;*

Lembre que, ao baixar o arquivo de imagem para a ONU, o arquivo de imagem ONU deve existir na OLT. A falta de especificação do diretório no campo fileName indica que o arquivo foi armazenado no diretório raiz, */card1*. O exemplo anterior não especificou o número de partição, portanto o arquivo será baixado para a partição em standby, que é a partição 0.

```
iSH> gpononu image 1/3/1 download-activate-commit 1420.img
Image "/card1/1420.img" downloading to onu 1/3/1.
```

2. Veja o status da atualização dessa ONU com o comando *onu image slot/olt/onu show.*

   Esse exemplo exibe que o download da imagem foi solicitado, e foi colocado na fila para o sistema realizar o download. O status do download é Queued (fila).

```
iSH> onu image 1/3/1 show
                      Partition 0         Partition 1
Version:              R2.0.8.16           R2.0.8.17
isCommitted:          False               True
isActive:             False               True
isValid:              True                True
Download status:              Queued
Onu model id:                 1420G
Upgrade start time:           OCT 01 23:15:32 2009
Will be activated:            True
Will be committed:            True
Upgrade type:                 Manual
```

Esse exemplo exibe que o download da imagem está em progresso ou se a validação da imagem baixada está em progresso. O status de download é Downloading (Baixando), e o status de validação na Partição 0 é False (Falso).

```
iSH> onu image 1/3/1 show
                        Partition 0          Partition 1
Version:                SOFTWAREIMAGE0       R2.0.8.17
isCommitted:            False                True
isActive:               False                True
isValid:                False                True
Download status:                Downloading
Onu model id:                   1420G
Upgrade start time:             OCT 01 23:15:32 2009
Will be activated:              True
Will be committed:              True
Upgrade type:                   Manual
```

Esse exemplo exibe que o arquivo de imagem foi baixado para a ONU e passou por validação, mas ainda não foi ativado. O status de download é Downloaded (Baixado), e o status de validação na Partição 0 é True (Verdadeiro).

```
iSH> gpononu image 1/3/1 show
                          Partition 0          Partition 1
Version:                  R2.0.8.18            R2.0.8.17
isCommitted:              False                True
isActive:                 False                True
isValid:                  True                 True
Download status:                  Downloaded
Onu model id:                     1420G
```

```
Upgrade start time:                  OCT 01 23:15:32 2009
Will be activated:                   True
Will be committed:                   True
Upgrade type:                        Manual
```

Esse exemplo exibe que o arquivo de imagem foi ativado. O status isActive é True (Verdadeiro).

```
iSH> gpononu image 1/3/1 show
                        Partition 0          Partition 1
Version:                R2.0.8.18            R2.0.8.17
isCommitted:            False                True
isActive:               True                 False
isValid:                True                 True
Download status:                Downloaded
Onu model id:                   1420G
Upgrade start time:             OCT 01 23:15:32 2009
Will be activated:              False
Will be committed:              True
Upgrade type:                   Manual
```

Esse exemplo exibe que os processos de download, ativação e utilização do arquivo da imagem da ONU foram finalizados com sucesso. O status isCommitted é True (Verdadeiro), e o status de Download é Complete (Completo).

```
iSH> gpononu image 1/3/1 show
                        Partition 0          Partition 1
Version:                R2.0.8.18            R2.0.8.17
isCommitted:            True                 False
isActive:               True                 False
isValid:                True                 True
Download status:                Complete
Onu model id:                   1420G
Upgrade start time:             OCT 01 23:15:32 2009
Will be activated:              False
Will be committed:              False
Upgrade type:                   Manual
```

Os valores possíveis para o status de Download são:

- **None (Nenhum):** a ONU não está funcionando, ou não há comunicação OMCI.
- **No Upgrade (Sem Atualização):** a ONU está funcionando, mas ainda não foi atualizada.
- **Queued (Fila):** um download de imagem foi solicitado, e foi colocado na fila para o sistema realizar o download.
- **Downloading (Baixando):** o download da imagem está em progresso ou a validação da imagem baixada está em progresso.
- **Downloaded (Baixado):** o software foi baixado para a ONU, mas ainda não foi ativado. Isso pode ser porque a ONU está reiniciando.
- **Complete (Completo):** o download, a ativação e a utilização do software para a ONU foram finalizados com sucesso.
- **Error:** houve falha na atualização devido a alguns erros.
- **Aborted (Abortado):** a ordem de atualização da ONU foi abortada por solicitação.
- **FileErr:** o arquivo de software para atualização não existe ou está corrompido.

Atualização automática de uma ONU

A função de atualização automática da ONU possibilita aos administradores da OLT 8820 G atualizar automaticamente as ONU instaladas com imagens desatualizadas durante a inicialização da ONU.

Se a atualização automática da ONU está ativada, quando a ONU faz a verificação, a OLT procura um modelo de atualização automática para esse modelo de ONU. O modelo de atualização automática é pré-definido pelo administrador para cada modelo de ONU. Este modelo contém o status da atualização automática, o ID do modelo, a versão de software permitida e o arquivo de imagem a ser carregado. Se é detectado um modelo correspondente para o modelo ONU especificado, a OLT compara a versão de software da ONU com a versão de software definida no modelo. Se elas são iguais, a atualização automática é interrompida. Se não, a OLT atualiza automaticamente a ONU.

As ações para atualizar automaticamente a imagem da ONU utilizando a comunicação OMCI são Download>Activate> Commit.

O download é realizado sempre na partição em standby. Se o download é finalizado com sucesso, a partição inativa é ativada e depois a imagem é utilizada na partição. Depois de utilizar a imagem, a atualização automática é finalizada.

Atualizando automaticamente uma ONU

1. Criar um modelo de atualização automática para um determinado modelo de ONU;
    a. Criar um modelo de atualização automática:

Lembre que, ao criar o modelo, o arquivo de imagem já deve existir no sistema da OLT, ou será exibida uma mensagem de erro; A falta de especificação do diretório no campo fileName indica que o arquivo foi armazenado no diretório raiz, /card1.

```
iSH> new remote-sw-upgrade-profile 4
remote-sw-upgrade-profile    4
Please provide the following: [q]uit.
enabled: ---->     {true}:
model: ------>     {}: 1420G
swVersion: -->     (): R2.0.8.18
filename: ---->    ():sip.2.0.8.18
.....................
Save new record?[s]ave, [c]hange or [q]uit:s
```

    b. Verique se o modelo foi criado:

```
iSH> list remote-sw-upgrade-profile
remote-sw-upgrade-profile    4
1 entry found.
```

2. Verifique se a atualização automática da ONU está ativada:

Para executar a atualização automática da ONU, tanto o modelo de atualização automática da ONU e o modelo de atualização automática do ID da ONU devem estar ativos. Por padrão, esses dois locais estão ativos.

    a. Verifique se o status de atualização automática de um modelo da ONU está ativado no modelo de atualização automática:

```
iSH> update remote-sw-upgrade-profile 4
remote-sw-upgrade-profile    4
Please provide the following: [q]uit.
enabled: ----->    {true}:
model: ------->    {1420G}:
swVersion: --->    (R2.0.8.18):
filename: ----->   (sip.2.0.8.18):
.....................
Save new record?[s]ave, [c]hange or [q]uit:s
```

b. Verifique se o status de atualização automática da ONU (ONU ID) está ativado no perfil gpon-olt-onu-config:

```
iSH> get gpon-olt-onu-config 1-1-3-1/gpononu
gpon-olt-onu-config 1-1-3-1/gpononu
serial-no-vendor-id: ---------------------->    {ZNTS}
serial-no-vendor-specific: ---------------->    {0}
password: --------------------------------->    {}
auto-learn: ------------------------------->    {enabled}
power-level: ------------------------------>    {0}
us-ber-interval: -------------------------->    {5000}
ds-ber-interval: -------------------------->    {5000}
onu-added: -------------------------------->    {false}
omci-file-name: --------------------------->    {}
ONU-Managed-Entity-Profile-name: ---------->    {}
ONU-Generic-Assignments-Profile-name: ----->    {}
physical-traps: --------------------------->    {disabled}
ont-traps: -------------------------------->    {disabled}
line-status-traps: ------------------------>    {disabled}
auto-upgrade: ----------------------------->    {enabled}
serial-no-vendor-specific-fsan: ----------->    {0}
use-reg-id: ------------------------------->    {disabled}
us-rx-power-monitoring-mode: -------------->    {monitoronly}
us-rx-power-high-threshold: --------------->    {-10}
us-rx-power-low-threshold: ---------------->    {-30}
dba-status-reporting: --------------------->    {disabled}
```

Ou pode visualizá-lo com o comando gpononu auto-upgrade show slot [/olt[/onu]] | all:

```
iSH> gpononu auto-upgrade show 1
Processing list of 512
This command may take several minutes to complete.
Do you want to continue?    (yes or no) [no] yes

Slot 15  olt 1

ONU      Name        Auto-upgrade
1        1-1-1-1     enabled
2        1-1-1-2     enabled
3        1-1-1-3     enabled
4        1-1-1-4     enabled
5        1-1-1-5     enabled
<SPACE> for next page, <CR> for next line,
A for all, Q to quit
```

c. Caso a atualização automática dessa ONU (ONU ID) esteja desativada, pode ser ativada pelo comando gpononu auto-upgrade enable *slot [/olt[/onu]]* | all:

```
iSH> gpononu auto-upgrade enable 1/1
This command may affect many OLTs and ONUs.
Do you want to continue?    (yes or no) [no] yes
Processing 1-1-1-1/gpononu...
Processing 1-1-1-2/gpononu...
processing 1-1-1-3/gpononu...
processing 1-1-1-4/gpononu...
processing 1-1-1-5/gpononu...
...
Operation successful.
```

3. Desativar a atualização automática da ONU.

A desativação da atualização automática da ONU faz com que a OLT 8820 G aborte o download solicitado.

a. Desativação da atualização automática em um modelo de atualização:

```
iSH> update remote-sw-upgrade-profile 4
remote-sw-upgrade-profile    4
Please provide the following:[q]uit.
enabled: -------->     {true}: false
model: ---------->     {2510}:
swVersion: ----->     (R2.0.8.18):
filename: ------->     (sip.cimg.2.0.8.18):
.....................
Save new record?[s]ave, [c]hange or [q]uit:s
```

b. Desative a atualização automática de uma ONU com o comando *gpononu auto-upgrade disable slot [/olt[/onu]] | all:*

```
iSH> gpononu auto-upgrade disable 1/1
This command may affect many OLTs and ONUs.
Do you want to continue? (yes or no) [no] yes
processing 1-1-1-1/gpononu...
processing 1-1-1-2/gpononu...
processing 1-1-1-3/gpononu...
processing 1-1-1-4/gpononu...
processing 1-1-1-5/gpononu...
...
Operation successful.
```

Visualização do status de atualização da ONU

» O status de atualização da ONU, tanto para atualização manual como para atualização automática, pode ser visualizado com o comando *onu upgrade show.*

Esse comando exibe o status de atualização da ONU (perceba que é igual ao status de Download do comando *onu image*), o modelo ONU, a data-hora em que foi feita a última atualização, o status de ativação, o status de utilização, o tipo de atualização (Manl ou Auto) e qual partição é utilizada.

» As informações detalhadas das partições de cada ONU podem ser visualizadas com o comando *onu image slot/olt/onu show.*

Visualizando o status de atualização da ONU

A seguir temos exemplos para cada comando de exibição:

1. Visualização do status de atualização de uma ONU:

```
iSH> onu upgrade show 1/3/1
ONU       State        Model     Start Time             Act   Cmt   Typ   Part
1/3/1     Complete     1420G     OCT 01 19:37:39 2009   F     F     Auto  1
```

Os valores possíveis para o campo Status são:

» **None (Nenhum):** a ONU não está funcionando, ou não há comunicação OMCI.

» **No Upgrade (Sem Atualização):** a ONU está funcionando, mas ainda não foi atualizada.

» **Queued (Fila):** um download de imagem foi solicitado, e foi colocado na fila para o sistema realizar o download.

» **Downloading (Baixando):** o download da imagem está em progresso ou a validação da imagem baixada está em progresso.

» **Downloaded (Baixado):** o software foi baixado para a ONU, mas ainda não foi ativado. Isso pode ser porque a ONU está reiniciando.

» **Complete (Completo):** o download, a ativação e a utilização do software para a ONU foram finalizados com sucesso.

» **Error:** houve falha na atualização devido a alguns erros.

» **Aborted (Abortado):** a ordem de atualização da ONU foi abortada por solicitação.

» **FileErr:** o arquivo de software para atualização não existe ou está corrompido.

2. Visualização do status de atualização de várias ONU com mesmo status de atualização:

```
iSH> onu upgrade show complete
ONU       State        Model     Start Time             Act   Cmt   Typ   Part
1/3/1     Complete     1420G     OCT 01 22:28:40 2009   F     F     Manl  1
1/3/2     Complete     1420G     OCT 01 19:37:39 2009   F     F     Auto  1
```

3. Visualização do status de atualização e das informações da partição de uma ONU:

```
iSH> onu image 1/3/1 show
                        Partition 0        Partition 1
Version:                R2.0.8.16          R2.0.8.17
isCommitted:            False              True
isActive:               False              True
isValid:                True               True
Download status:                Complete
Onu model id:                   1420G
Upgrade start time:             OCT 01 19:37:39 2009
Will be activated:              False
Will be committed:              False
Upgrade type:                   Auto
```

Monitoramento de status e alarmes da ONU

Visualize os status e alarmes gerados em uma ONU com o comando onu status.

A tabela a seguir fornece a descrição dos campos de saída para esse comando.

Campo	Descrição
ID	ID da ONU. Varia de 1 até 64.
Onu	O nome da interface ONU. Por padrão no formato Shelf ID – Slot ID – OLT ID – ONU ID
OperStatus	O status operacional da ONU. Valores: Up, Down
ConfigState	Os status da configuração OMCI da ONU. Detectado pela OLT em relação à ONU. Valores: None Exibido durante a inicialização. Sem solicitação de configuração. Queue Aguardando ser configurado. Configuring Em processo de configuração. Active configuração finalizada com sucesso. Inactive A ONU está desativada. Non-OMCI não provisionada por OMCI ou SNMP. RgComError (ONT com modo RG ativo) O SNMP não pode se comunicar com o ONT. RgServiceSetupErr (ONT com modo RG ativo) Um ou mais comandos SNMP falharam. OmciError ocorreu um erro durante a configuração OMCI. OmciErr+RgComErr ocorreu erro OMCI e falha na comunicação SNMP. OmciErr+RgServErr ocorreu erro OMCI e falha de um ou mais comandos SNMP.
GponOnuStatus	Alarmes padrão MAC GPON da ONU detectada na OLT. Valores: Active A ONU está ativa, sem alarme Inactive A ONU está inativa e não pode obter o alarme LOS Lost of Signal (Perda de Sinal) LOF Lost of Frame (Perda de quadro) DOW Drift of Window (Desvio da Janela) DG Dying Gasp SF Signal Fail (Falha do Sinal) SD Signal Degrade (Diminuição do Sinal) LCDG Lost of GEM Channel Delinquency RD Remote Defect (Defeito Remoto) RXPWRDSA Received Power of Range, and ONU is disabled (Recepção de Energia para Verificação, ONU desativada) TF Transmitter Failure (Falha na Transmissão) SUF Start Up Failure (Falha na Inicialização) LOA Lost of Ack (Perda da Confirmação) MEM Message error (Mensagem de Erro) PEE Physical equipment error (Erro do Equipamento Físico) OAML Lost of OAM (Perda do OAM)

DownloadState	Status de download das imagens do software da ONT. Valores: None, Queued, NoUpgrade, Downloading, Complete, Error, Aborted
OLT Rx Power	Nível de potência óptica upstream recebida na OLT.
ONT Rx Power	Nível de potência óptica downstream recebida na ONU.
Distance (km)	Cálculo da distância da ONU a partir da OLT.

Opções e descrições do comando onu status

Esse exemplo exibe uma ONU ativa e com provisionamento OMCI completo.

```
iSH> onu status 1/3/1
                                                Download        OLT          ONT       Distance      GPON
ID      Onu       OperStatus    ConfigState     State        Rx Power     Rx Power       (km)      OnuStatus
1     1-1-3-1        Up           Active      NoUpgrade      -19.2 dBm   -20.0 dBm       18         Active
```

Esse exemplo exibe uma ONU ativa que é desativada após o dying gasp.

```
iSH> onu status 1/3/1
                                          Download       OLT        ONT Rx     Distance            GPON
ID      Onu       OperStatus    ConfigState     State      Rx Power     Power       (km)           OnuStatus
1     1-1-3-1        Down         Active      NoUpgrade      -19.2 dBm   -20.0 dBm      18     Inactive+LOS+LOF+DG+OAML
```

Localizar ONU

Caso seja necessário localizar uma ONU, já devidamente provisionada, deverá ser utilizada a informação FSAN, número de série.

```
iSH> onu find fsan <FSAN>
```

O parâmetro deve ser preenchido da seguinte forma:

» **FSAN:** número de série da ONU.

Obs.: *o sistema diferencia caracteres maiúsculos dos minúsculos.*

Reinicialização, ressincronização e reprovisionamento das ONU

Os comandos nos tópicos anteriores aplicam-se ao provisionamento USP (Unified Service Provisioning).

Lembre que o comando *onu set2default* está relacionado a esses tópicos, mas somente é aplicável às ONU que suportam provisionamento por RG.

Reinicialização de uma ONU

Reinicialize a ONU remota utilizando o comando onu reboot.

```
iSH> onu reboot 1/3/1
```

Ressincronização de uma ONU

Sincronizar uma ONU através da OLT 8820 G utilizando o comando onu resync. Esse comando faz com que a OLT interrompa e restabeleça a conexão com a ONU e envie a configuração prévia (configuração OMCI, e configuração SNMP se aplicável) para a ONU. Não é comum utilizar o comando quando a ONU foi provisionada por USP (Unified Service Provisioning). Normalmente este comando é utilizado em debugs.

```
iSH> onu resync 1/3/1
```

Reaplicação de uma ONU

O comando *onu apply* emite o comando de configuração OMCI no perfil ME. Esse comando não força a ressincronização da ONU.

Se a ONU é provisionada por USP (Unified Service Provisioning), não é necessário utilizar o comando *onu apply*. Os novos serviços serão atualizados na ONU automaticamente.

```
iSH> onu apply 1/3/1
```

Monitoramento do status e alarmes e configuração do estado e velocidade das portas LAN das ONUs

Status das portas da ONU

Na OLT 8820 G, o status administrativo e operacional das portas eth da ONU podem ser obtidos utilizando o comando a seguir:

```
onu status [slot[/olt[/onu]] | interfaceName] port all | portType [portNumber]
```

O campo portType tem base nas configurações de compatibilidade do modelo da ONU. Os tipos de porta possíveis podem ser eth (portas ethernet), POTS (portas FXS).

O exemplo a seguir exibe o status de uma porta ethernet na ONU:

```
iSH> onu status 1/3/1 port eth 1
1/3/1     ONU Port Status
                  Ethernet Port Status - Port 1
                  Administrative State              up
                  Operational State                  active
```

Status das informações de alarmes da ONU

Visualize alarmes internos da ONU e das portas eth da ONU com o comando *onu alarms.*

```
iSH> onu alarms 1/3/1
1/3/1 ONU Active Alarms
PptpEthUni 0x0402 LanLos
PptpEthUni 0x0404 LanLos
```

Configuração do estado operacional das portas LAN da ONU

Habilitar ou desabilitar uma porta LAN da ONU

Na OLT 8820 G, o status administrativo da porta eth da ONU pode ser ativada ou desativado, ao utilizar o comando a seguir:

```
iSH> onu port [slot[/olt[/onu]] portType interfaceID up|down
```

O campo portType tem base nas configurações de compatibilidade do modelo da ONU. Os tipos de porta possíveis podem ser eth (portas ethernet), POTS (portas FXS).

1. Modifique o status da porta ethernet da ONU para down:

```
iSH> onu port 1/3/1 eth 1 down
```

2. Verifique o status da porta eth 1 da ONU 1/3/1:

```
iSH> onu status 1/3/1 port eth 1
1/3/1 ONU Port Status
         Ethernet Port Status - Port 1
         Administrative State                  down
         Operational State           inactive
```

3. Altere o status da porta eth da ONU para UP:

```
iSH> onu port 1/3/1 eth 1 up
```

4. Verifique se o status de administrador está para cima:

```
iSH> onu status 1/3/1 port eth 1
1/3/1 ONU Port Status
         Ethernet Port Status - Port 1
         Administrative State         up
         Operational State   active
```

Configuração da velocidade das portas lan da ONU

Por padrão, a velocidade da porta eth da ONU é configurada no modo automático. Para modificar essa configuração, utilize o comando *onu auto-detect:*

```
iSH> gpononu auto-detect <slot>/<olt>/<onu> portType <interface#>
< auto | 10F | 100F | 1000F | 10H | 100H | 1000H | 10FA | 1000A >
```

As configurações para esse comando são:

- » auto: detecção automática.
- » 10F: 10 Mbps, somente full duplex.
- » 100F: 100 Mbps, somente full duplex.
- » 1000F: 1000 Mbps, somente full duplex.
- » 10H: 10 Mbps, somente half duplex.
- » 100H: 100 Mbps, somente half duplex.
- » 1000H: 1000 Mbps, somente half duplex.
- » 10FA: 10 Mbps, full duplex e auto.
- » 1000A: 1000 Mbps auto.

O exemplo a seguir configura uma porta eth da ONU no modo 1000 full duplex:

```
iSH> onu auto-detect 1/3/1 eth 1 1000F
```

Removendo configurações da ONU

Para remover todas as configurações de uma ONU e configurar essa ONU para o padrão, pode-se utilizar o comando *onu delete slot[/olt[/onu]].*

O comando *onu delete* irá:

1. Remover todos os perfis de assinante CPE e conexões CPE que foram criadas na ONU, assim como todos os perfis CPE associados à ONU (ex. perfil de sistema CPE, se está configurado no provisionamento RG);
2. Removerá todas as bridges configuradas na OLT atrelada a essa ONU;
3. O perfil gpon-olt-onu-config da ONU voltará para o padrão.

Removendo a configuração de uma ONU

Esse exemplo remove a configuração da ONU 1/3/1.

1. Remova a configuração da ONU 1/3/1;

```
iSH> gpononu delete 1/3/1
Ok to delete ONU 1/3/1 and all of it's configuration? [yes] or [no]: yes
Do you want to exit from this request? [yes] or [no]: no
Are you sure? [yes] or [no]: yes
deleting ONU 1/3/1
ONU 1/3/1 has been deleted
```

2. Verifique se as bridges da OLT 8820 G criados nas GEM Ports de ONU 1/3/1 foram todas removidas;

```
iSH> bridge show
        Orig
Type VLAN/SLAN   VLAN/SLAN  Physical         Bridge                          St Table Data
dwn              Tagged 999  1/3/1/2/gpononu  1-3-1-257-gponport-999/bridge   UP
upl              ST     2/998  1/a/4/0/eth      ethernet4-2-998/bridge          UP S SLAN 998 VLAN 2 default
upl              ST     2/998  1/a/4/0/eth      ethernet4-3-998/bridge          UP S SLAN 998 VLAN 3 default
tls              Tagged 200    1/a/4/0/eth      ethernet4-300/bridge            UP
tls              Tagged 501    1/a/4/0/eth      ethernet4-501/bridge            UP
upl              Tagged 999    1/a/4/0/eth      ethernet4-999/bridge            UP S VLAN 999 default
upl              1001          1/a/8/0/eth      ethernet8/bridge                UP S VLAN 1001 default
7 Bridge Interfaces displayed
```

3. Verifique se as GEM Ports criadas na ONU 1/3/1 foram removidas;

```
iSH> onu gemports 1/3/1
                                    Fixed UBR      Fixed CBR   Assured      Max        Extra
                    traf            Bandwidth      Bandwidth   Bandwidth   Bandwidth  Bandwidth
ONU  GEM Port  Admin  prof  compn  share  Mbits/sec   Mbits/sec   Mbits/sec   Mbits/sec     Type     allocId  DBA
```

4. Verifique se as conexões CPE criadas nas portas eth da ONU 1/3/1 foram removidas;

```
iSH> bridge show onu
       GEM    ONU     DSCP     ONU UNI     OLT            OLT
ONU    Port    UNI     to COS   VLAN/SLAN   VLAN/SLAN   G-VLAN MVR   Service Rg-Mode   OLT Bridge   ST
```

5. Verifique se os perfis de assinantes CPE foram removidos dessa ONU;

```
iSH> CPE> ETH> show 1/3/1
No services found.
iSH> CPE> VOIP> show 1/3/1
No services found.
```

6. Para verificar se os perfis gpon-olt-onu-config foram modificados para o padrão, utilize o comando a seguir;

```
iSH> get gpon-olt-onu-config 1-1-3-1/gpononu
```

7. Verifique se o adminstatus, ifName, e os campos redundancy-param1 no perfil if-translation da ONU 1/3/1 foram colocados no padrão.

```
iSH> get if-translate 1-1-3-1/gpononu
if-translate 1-1-3-1/gpononu
ifIndex: ---------------------->     {175}
shelf: ------------------------>     {1}
slot: ------------------------->     {1}
port: ------------------------->     {3}
subport: ---------------------->     {1}
type: ------------------------->     {other}
adminstatus: ------------------>     {up}
physical-flag: ----------------->     {false}
iftype-extension: ------------>     {gponon}
ifName: ----------------------->     {1-1-3-1}
redundancy-param1: ------------>     {0}
description-index: ------------>     {0}
```

12.6. Provisionamento utilizando Reg ID

O ID de registro (Reg ID) fornece um método alternativo e flexível para uma possível substituição de ONU. O Reg ID é um número de 10 dígitos atribuído a uma ONU que é configurado na OLT. Esse Reg ID deve ser configurado como senha na ONU e pode ser utilizado por técnicos durante a instalação da ONU no campo.

O processo Reg ID é realizado da seguinte maneira:

- » Quando a OLT descobre um número de série, ele tenta relacioná-lo com um dos números de série provisionados.
- » Se houver um número de série correspondente, então a ONU é ativada.
- » Se não há número de série correspondente, então:

A senha (Reg ID) é obtida e comparada com a senha de cada ONU configurada com useRegId = True. Se há um resultado correspondente, a ONU é ativada.

Configuração do Reg ID

O comando onu set possibilita a configuração do Reg ID.

```
iSH> onu set <slot/olt/onu> regid <xxx> meprof <profile-onu>
```

Esse comando define a senha como *xxx*, desta forma o parâmetro *use-reg-id* é alterado para *Enabled* e o parâmetro *onu-added* é alterado para *True*, no perfil *gpon-olt-onu-config*.

> **Observação:** a senha cadastrada DEVE possuir 10 números e deve ser exclusiva para cada ONU do sistema

Para remover a senha configurada no Reg ID bem como definr o campo *use-reg-id* em *DISABLED*, utilize o comando a seguir:

```
iSH> onu clear <slot/olt/onu> regid
```

12.7. Alocação de largura de banda para tráfego upstream da ONU para a OLT

A alocação de banda para tráfego upstream da ONU para a OLT 8820 G é configurada no perfil de tráfego GPON (GTP).

Configuração do perfil de tráfego GPON (GTP)

A função geral de um perfil de tráfego GPON é determinar uma taxa máxima de transmissão upstream, classes de tipos de serviço e o tipo de alocação de banda por T-cont no PON. Ao criar uma GEM Port com o comando bridge *add*, deve ser associado um perfil de tráfego GPON a ela. Para minimizar a quantidade de configurações por assinante, um perfil de tráfego GPON é definido no sistema e esse perfil possui um índice que é utilizado durante a criação da bridge interface do assinante. Portanto, se muitos clientes desejam utilizar o mesmo serviço, pode ser criado um perfil de tráfego GPON, e seu índice pode ser utilizado para diferentes GEM Ports sem ter de definir os parâmetros de largura de banda toda vez que um novo assinante é provisionado.

Criando um perfil de tráfego GPON

A tabela a seguir fornece a descrição dos parâmetros do perfi de tráfego GPON (GTP).

Parâmetro	Descrição
guaranteed-upstream-bw	Especifica a largura de banda não DBA garantida para um T-cont em Kbps. O valor deve ser um múltiplo de 512 e não pode exceder 1.048.576 Kbps. Lembre que guaranteed-upstream-bw é somente para CBR e UBR, e não é utilizada com DBA. Se o DBA está desativado, a largura de banda garantida para upstream deve ser diferente de zero.
traffic-class	Especifica o tipo de classe de tráfego upstream para um T-cont. Não é utilizado com DBA. Padrão: *ubr* Valores: cbr Constant Bit Rate (Taxa de Bits Constante). A classe de tráfego CBR é utilizada por conexões que exigem uma taxa constante e garantida. O tempo de amostragem para CBR é constante, sem atrasos. ubr Unspecified Bit Rate (Taxa de Bits não Especificada). A classe de tráfego UBR não especifica garantias relacionadas ao tráfego. Não há compromissos numéricos feitos em relação a perda de pacotes ou atrasos. Com o serviço UBR, a largura de banda disponível é distribuída proporcionalmente entre os associados UBR ativos.
compensated	Modo de compensação do CBR. Algumas vezes, o acesso ao CBR será ignorado após a troca de mensagens GPON OAM entre a OLT e a ONU. Se selecionar true no modo de compensação, o acesso ao CBR poderá ser compensado imediatamente após a troca de mensagens GPON OAM para evitar a atraso do canal CBR. O modo de compensação não é utilizado no DBA. Padrão: *false* Valores: true, false
shared	A função shared deixa as GEM Ports da mesma ONU compartilharem a largura de banda upstream. Selecione true se a GEM Port que utiliza esse descritor de tráfego compartilha um T-CONT (ex. Alloc-ID) com outra GEM Port da mesma ONU. Em outros casos, selecione False. O modo shared é utilizado com e sem DBA. Valores: true, false Padrão: *false*
dba-enable	Ativa ou desativa o DBA. O valor padrão é false. Valores: true, false Padrão: *false*
dba-fixed-us-ubr-bw	Largura de banda garantida na direção upstream para tráfego do tipo UBR. É aplicável somente quando DBA está ativo. Os valores mínimos da largura de banda Fixa UBR podem ser 0 ou 128 Kbps. O valor máximo é 1.048.576 Kbps. Somente são permitidos múltiplos de 64 Kbps. Padrão: *0*

dba-fixed-us-cbr-bw	Largura de banda garantida na direção upstream para tráfego do tipo CBR. É aplicável somente quando DBA está ativo. Os valores mínimos da largura de banda Fixa CBR podem ser 0 ou 512 Kbps. O valor máximo é 454.208 Kbps. Somente são permitidos múltiplos de 64 Kbps. Padrão: *0*
dba-assured-us-bw	Largura de banda DBA garantida na direção upstream. É aplicável somente quando DBA está ativo. Será alocada quando existir a demanda de tráfego, e pode não ser disponibilizada se não houver demanda. O valor mínimo da largura de banda Garantida pode ser 0 ou 256 Kbps. O valor máximo é 1.048.576 Kbps. Somente são permitidos múltiplos de 64 Kbps. Padrão: *0*
dba-max-us-bw	Essa é a largura de banda DBA máxima que pode ser alocada para um T-CONT. Essa largura de banda máxima inclui a largura de banda garantida e largura de banda não garantida. Pode utilizar esse parâmetro para indicar a quantidade de largura de banda não garantida configurada para o perfil de tráfego. A classe de serviço não garantida pode ser do tipo nonassured ou besteffort, que é especificado no campo dba-extra-us-bw-type. O valor da largura de banda não garantida pode ser calculado usando o valor configurado nesse parâmetro sem a soma do dba-fixed-us-ubr-bw, dba-fixed-us-cbr-bw e dba-assured-us-bw. O valor configurado nesse parâmetro deve ser maior ou igual à soma do dba-fixed-us-ubr-bw, dba-fixed-us-cbr-bw e dba-assured-us-bw. Se o valor configurado é igual à soma de dba-fixed-us-ubr-bw, dba-fixed-us-cbr-bw e dba-assured-us-bw, então não há largura de banda atribuída para o tipo sem garantia. O valor máximo é 1.048.576 Kbps. Somente são permitidos múltiplos de 64 Kbps. Padrão: *0*
dba-extra-us-bw-type	Tipo de prioridade de largura de banda não garantida. Valores: nonassured Largura de banda concedida somente se a largura de banda está disponível, mas não garantida. Nonassured tem maior prioridade para obtenção de largura de banda não usado do que besteffort. besteffort Demanda concedida somente se há largura de banda restante disponível. Besteffort tem menor prioridade. Padrão: *nonassured*

Descrição dos parâmetros do perfil GTP (GPON Traffic Profile)

1. Crie um perfil de tráfego GPON com o comando *new gpon-traffic-profile index;*

O sistema proporciona uma validação do perfil afim de garantir que o valor de largura de banda especificada não exceda o valor máximo.

- » Se DBA está desativado, a validação do perfil é realizada para garantir que a largura de banda estática *guaranteed-upstream-bandwidth* não exceda o valor máximo.
- » Se DBA está ativo, a validação de perfil é realizada para garantir que cada largura de banda relacionada ao DBA não exceda os valores máximos, e a soma de *dba-fixed-us-ubr-bw, dba-fixed-us-cbr-bw* e *dba-assured-us-bw* não exceda *dba-max-us-bw* para o perfil de tráfego GPON.

```
iSH> new gpon-traffic-profile 512
gpon-traffic-profile 512
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------> {0}: 2600000
Invalid entry: guaranteed-upstream-bw range: [0 to 1048576] validação do perfil
guaranteed-upstream-bw: ------>       {0}: 512
traffic-class: ---------------->       {ubr}: cbr
compensated: ------------------>       {false}: true
shared: ---------------------->       {false}:
dba-enabled: ------------------>       {false}:
dba-fixed-us-ubr-bw: ---------->       {0}:
dba-fixed-us-cbr-bw: ---------->       {0}:
dba-assured-us-bw: ------------>       {0}:
dba-max-us-bw: ---------------->       {0}:
dba-extra-us-bw-type: -------->       {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

2. Consulte as configurações do perfil de tráfego GPON com o comando *get gpon-traffic-profile index.*

```
iSH> get gpon-traffic-profile 512
gpon-traffic-profile 512
guaranteed-upstream-bw: ------> {512}
traffic-class: ---------------->        {cbr}
compensated: ------------------>        {true}
shared: ----------------------->         {false}
dba-enabled: ------------------>        {false}:
dba-fixed-us-ubr-bw: ---------->        {0}:
dba-fixed-us-cbr-bw: ---------->        {0}:
dba-assured-us-bw: ------------>        {0}:
dba-max-us-bw: ---------------->        {0}:
dba-extra-us-bw-type: -------->         {nonassured}:
```

Compartilhamento de Alloc-ID entre GEM Ports

A função de compartilhamento de perfil de tráfego GPON permite às GEM Ports da mesma ONU compartilhem a largura de banda de upstream.

O sistema suporta até 384 Alloc-IDs DBA por porta física GPON e 768 Alloc-IDs por porta física GPON (incluindo DBA e estático).

Várias GEM Ports podem compartilhar um Alloc-ID se:

- » As GEM Ports utilizarem o mesmo perfil de tráfego.
- » O campo *shared* do perfil de tráfego GPON esteja definido como TRUE.
- » As GEM Ports estão sob a mesma ONU.

Para ativar a função de compartilhamento de compartilhamento de Alloc Ids, defina o parâmetro shared em *true* no perfil de tráfego GPON.

1. Visualize os valores de Alloc-ID atribuídos às GEM Ports quando a função shared está desativada;

Esse exemplo exibe que as GEM Ports 1-1-2-501 e 1-1-2-701 tem diferentes Alloc-ID, 501 e 701.

```
iSH> onu gemports 1/2
Processing list of 64
This command may take several minutes to complete.
Do you want to continue? (yes or no) [no] yes
```

ONU	GEM Port	Admin	traf prof	compn	share	Fixed UBR Bandwidth Mbits/sec	Fixed CBR Bandwidth Mbits/sec	Assured Bandwidth Mbits/sec	Max Bandwidth Mbits/sec	Extra Bandwidth Type	allocId	DBA
1-1-2-1	**1-1-2-501**	Up	1024	False	False	1.024	0	n/a	n/a	n/a	**501**	n/a
	1-1-2-701	Up	1024	False	False	1.024	0	n/a	n/a	n/a	**701**	n/a
1-1-2-2	1-1-2-502	Up	1024	False	False	1.024	0	n/a	n/a	n/a	502	n/a
	1-1-2-702	Up	1024	False	False	1.024	0	n/a	n/a	n/a	702	n/a

```
Total Available BW: 1130.663(Mb), Total Available BW for Compensated CBR: 454.246 (Mb)
```

2. Crie um perfil de tráfego GPON e ative a função shared:

```
iSH> new gpon-traffic-profile  512
gpon-traffic-profile  512
Please provide the following:[q]uit.
guaranteed-upstream-bw: --------->    {0}: 512
traffic-class: ------------------->    {ubr}:
compensated: --------------------->    {false}:
shared: -------------------------->    {false}: true
dba-enabled: --------------------->    {false}:
dba-fixed-us-ubr-bw: ------------->    {0}:
```

```
dba-fixed-us-cbr-bw: ------------>    {0}:
dba-assured-us-bw: -------------->    {0}:
dba-max-us-bw: ------------------>    {0}:
dba-extra-us-bw-type: ----------->    {nonassured}:
..........
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Aplique o perfil de tráfego GPON a várias GEM Ports utilizando o comando bridge *add;*
4. Liste todas as GEM Ports que utilizam esse perfil de tráfego GPON;

```
iSH> onu gtp list 512
To Abort the operation enter Ctrl-C
GEM Ports that use Traffic Profile 512
```

ONU Interface	GEM Port
1-1-1-1	1-1-1-501
1-1-1-1	1-1-1-701
1-1-1-2	1-1-1-502
1-1-1-2	1-1-1-702

5. Visualize os valores Alloc-ID atribuídos às GEM Ports quando a função shared está ativa.

Esse exemplo exibe que as GEM Ports 1-1-1-501 e 1-1-1-701 tem o mesmo Alloc-ID, 501.

```
iSH> gpononu gemports 1/1
Processing list of 64
This command may take several minutes to complete.
Do you want to continue?    (yes or no) [no] yes
```

ONU	GEM Port	Admin	traf prof	compn	share	Fixed UBR Bandwidth Mbits/sec	Fixed CBR Bandwidth Mbits/sec	Assured Bandwidth Mbits/sec	Max Bandwidth Mbits/sec	Extra Bandwidth Type	allocId	DBA
1-1-1-1	**1-1-1-501**	Up	512	False	True	0.5	0	n/a	n/a	n/a	**501**	n/a
	1-1-1-701	Up	512	False	True	0.5	0	n/a	n/a	n/a	**501**	n/a
1-1-1-2	1-1-1-502	Up	512	False	True	0.5	0	n/a	n/a	n/a	502	n/a
	1-1-1-702	Up	512	False	True	0.5	0	n/a	n/a	n/a	502	n/a

Modificação de um perfil de tráfego GPON

Modifique um perfil de tráfego GPON com o comando update gpon-traffic-profile index. Somente é possível modificar um perfil de tráfego GPON que não esteja sendo usado por uma GEM Port.

```
iSH> update gpon-traffic-profile 512
gpon-traffic-profile 512
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------>       {512}:
traffic-class: ---------------->       {cbr}: ubr
compensated: ------------------>       {true}: false
shared: ---------------------->       {false}:
dba-enabled: ------------------>       {false}:
dba-fixed-us-ubr-bw: ---------->       {0}:
dba-fixed-us-cbr-bw: ---------->       {0}:
dba-assured-us-bw: ------------>       {0}:
dba-max-us-bw: ---------------->       {0}:
dba-extra-us-bw-type: -------->       {nonassured}:
..................
Save new record? [s]ave, [c]hange or [q]uit: s
```

```
New record saved.
```

A validação de perfil verifica se o perfil está sendo utilizado por uma GEM Port. Um perfil de tráfego GPON é considerado em uso se já foi atribuído a uma GEM Port. Se um perfil de tráfego GPON está em uso, a modificação do perfil de tráfego GPON é rejeitada e uma mensagem de erro é exibida.

```
iSH> update gpon-traffic-profile 513
gpon-traffic-profile 513
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------>       {512}:
traffic-class: ---------------->       {cbr}: ubr
compensated: ------------------>       {true}: false
shared: ---------------------->       {false}:
dba-enabled: ------------------>       {false}:
dba-fixed-us-ubr-bw: ---------->       {0}:
dba-fixed-us-cbr-bw: ---------->       {0}:
dba-assured-us-bw: ------------>       {0}:
dba-max-us-bw: ---------------->       {0}:
dba-extra-us-bw-type: --------->       {nonassured}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
Profile Validation Error. The GTP profile is in use and cannot be modified.
Starting over....
```

Removendo um perfil de tráfego GPON

Remova um perfil de tráfego GPON com o comando *delete gpon-traffic-profile index*. Somente é possível remover um perfil de tráfego GPON que não está sendo usado por uma GEM Port.

```
iSH> delete gpon-traffic-profile 512
gpon-traffic-profile 512
1 entry found.
Delete gpon-traffic-profile 512? [y]es,[n]o,[q]uit: y
gpon-traffic-profile 512 deleted.
```

Visualização dos perfis de tráfego GPON

Visualize os perfis de tráfego GPON no sistema com o comando *list gpon-traffic-profile*.

```
iSH> list gpon-traffic-profile
gpon-traffic-profile 1
gpon-traffic-profile 1024
gpon-traffic-profile 2
```

Visualização das GEM Ports que utilizam o mesmo perfil de tráfego GPON

Visualização das GEM Ports que utilizam o mesmo perfil de tráfego GPON com o comando *onu gtp list index*.

```
iSH> onu gtp list 512
To Abort the operation enter Ctrl-C
GEM Ports that use Traffic Profile 512

 ONU Interface  GEM Port
-----------------------------
 1-1-1-1        1-1-1-501
 1-1-1-1        1-1-1-701
 1-1-1-2        1-1-1-502
 1-1-1-2        1-1-1-702
```

Alocação dinâmica de largura de banda (DBA)

Alocação de Largura de Banda Dinâmica (DBA) é especificado no padrão ITU 984.3. Este recurso é usado para conceder banda de upstream para ONUs com base no seu contrato de demanda e de nível de serviço. A OLT concederá para as ONUs um aumento em seu time slot proporcionando maior largura de banda, enquanto concede uma redução no time slot de outras ONUs. Através do DBA, um link GPON pode ter excessos de requerimentos para o tráfego upstream, e melhorar a eficiência de uso de banda.

Ativação e configuração da largura de banda DBA em T-cont

É possível ativar ou desativar o DBA e configurar a largura de banda DBA em cada T-cont com o perfil de tráfego GPON. É possível configurar largura de banda DBA garantida (ex. dba-fixed-us-ubr-bw, dba-fixed-us-cbr-bw, dba-assured-us-bw) e não garantida (ex. dba-max-us-bw). A largura de banda DBA não garantida é sempre para tráfego tipo UBR e não tem compensação.

1. Crie um perfil GPON-traffic com parâmetros relacionados a DBA. O DBA está ativo nesse GTP:

```
iSH> new gpon-traffic-profile 430080
gpon-traffic-profile 430080
Please provide the following: [q]uit.
guaranteed-upstream-bw: ------>      {0}: somente para CBR e UBR, não utilizado com DBA.
traffic-class: ---------------->      {ubr}: somente para CBR e UBR, não utilizado com DBA
compensated: ------------------>      {false}: não utilizado com DBA
shared: ----------------------->      {false}: com e sem DBA
dba-enabled: ------------------>      {false}: true somente para DBA
dba-fixed-us-ubr-bw: ---------->      {0}: 512 somente para DBA
dba-fixed-us-cbr-bw: ---------->      {0}: somente para DBA
dba-assured-us-bw: ------------>      {0}: 1024 somente para DBA
dba-max-us-bw: ---------------->      {0}: 1024000 somente para DBA
dba-extra-us-bw-type: -------->      {nonassured}: somente para DBA
.....................
Save changes? [s]ave, [c]hange or [q]uit:s
New record saved.
```

2. Verifique as configurações:

```
iSH> get gpon-traffic-profile 430080
gpon-traffic-profile  430080
guaranteed-upstream-bw: -------->      {0}:
traffic-class: ---------------->      {ubr}:
compensated: ------------------->      {false}:
shared: ----------------------->      {false}:
dba-enabled: ------------------->      {true}:
dba-fixed-us-ubr-bw: ---------->      {512}:
dba-fixed-us-cbr-bw: ---------->      {0}:
dba-assured-us-bw: ------------>      {1024}:
dba-max-us-bw: ----------------->    {1024000}:
dba-extra-us-bw-type: ---------->    {nonassured}:
```

3. Aplique o GTP com DBA ativo a uma GEM Port;

```
iSH> bridge add 1-1-1-5/gpononu gem 505 gtp 430080 downlink vlan 100 tagged
Adding bridge on 1-1-1-5/gpononu
Created bridge-interface-record 1-1-1-505-gponport-100/bridge
```

4. Visualize as configurações de largura de banda DBA nas GEM Port desejada. O allocID e tipo DBA não serão exibidos até que a ONU seja ativada.

```
iSH> onu gemports 1/1/5
                                    Fixed UBR  Fixed CBR  Assured    Max        Extra
                           traf     Bandwidth  Bandwidth  Bandwidth  Bandwidth  Bandwidth
ONU   GEM Port       Admin prof     Mbits/sec  Mbits/sec  Mbits/sec  Mbits/sec  Type
-------------------------------------------------------------------------------------
1-1-1-5 1-1-5-502    Up    430080   0.512      0          1.024      1.024      Nonassured
```

Alteração do tipo de DBA

Existem dois tipos de DBA, Status Reporting (SR) e Non-Status Reporting (NSR):

» **SR:** a ONU fornece as informações de status da largura de banda como parte da mensagem de tráfego upstream. O SR está especificado no Dynamic Bandwidth Report upstream (DBRu).

» **NSR:** é a opção de não fornecimento de status onde a OLT calcula a largura de banda disponível. A alocação é baseada no monitoramento de utilização de largura de banda da ONU em comparação à largura de banda alocada.

Por padrão, o tipo DBA de cada ONU é NSR. É possível alterar o tipo DBA para SR somente se a ONU está inativa.

> **Observação:** antes de trocar o tipo DBA de uma ONU do tipo NSR para SR, assegure-se de que a ONU suporte o tipo SR

Esse exemplo altera o tipo DBA de uma ONU ativa de NSR para SR.

1. Visualize o tipo de DBA nos GEM de uma ONU ativa;

```
iSH> onu gemports 1/1/5
                                    Fixed UBR  Fixed CBR  Assured    Max        Extra
                           traf     Bandwidth  Bandwidth  Bandwidth  Bandwidth  Bandwidth
ONU   GEM Port       Admin prof     Mbits/sec  Mbits/sec  Mbits/sec  Mbits/sec  Type
-------------------------------------------------------------------------------------
1-1-1-5 1-1-5-505    Up    430080   0.512      0          1.024      1.024      Nonassured
```

2. Ative o tipo SR de DBA da ONU;

```
iSH> update gpon-olt-onu-config 1-1-1-5/gpononu
gpon-olt-onu-config1-1-1-5/gpononu
Please provide the following: [q]uit.
serial-no-vendor-id: ---------------------->     {ZNTS}:** read-only **
serial-no-vendor-specific: ---------------->     {0}: ** read-only **
password: --------------------------------->     {}:
auto-learn: ------------------------------->     {enabled}:
power-level: ------------------------------>     {0}:
us-ber-interval: -------------------------->     {5000}:
ds-ber-interval: -------------------------->     {5000}:
onu-added: -------------------------------->      {false}:
omci-file-name: --------------------------->     {}:
ONU-Managed-Entity-Profile-name: ---------->     {}:
ONU-Generic-Assignments-Profile-name: ------>     {}:
physical-traps: --------------------------->     {disabled}:
ont-traps: -------------------------------->     {disabled}:
line-status-traps: ------------------------>     {disabled}:
auto-upgrade: ----------------------------->     {enabled}:
serial-no-vendor-specific-fsan: ---------->     {0}: ** read-only **
use-reg-id: ------------------------------->     {disabled}:
us-rx-power-monitoring-mode: -------------->     {monitoronly}:
us-rx-power-high-threshold: --------------->     {-10}:
us-rx-power-low-threshold: ---------------->     {-30}:
dba-status-reporting: --------------------->     {disabled}:enabled
.....................
```

```
Save changes? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3. Desregistre a ONU;

```
iSH> onu clear 1/1/5
```

4. Exiba a ONU atual na OLT e descobra os números de série disponíveis;

```
iSH> onu show 1/1
Free ONUs for slot 3 olt 1:
1   2   3   4   5   6   7   8   9   10  11  12
13  14  15  16  17  18  19  20  21  22  23  24
25  26  27  28  29  30  31  32  33  34  35  36
37  38  39  40  41  42  43  44  45  46  47  48
49  50  51  52  53  54  55  56  57  58  59  60
61  62  63  64
Discovered serial numbers for slot 1 olt 1:
sernoID     Vendor     Serial Number     sernoID     Vendor     Serial Number
1               ZNTS       138543368
```

5. Ative a ONU.

```
iSH> onu set 1/1/5 1
Onu 5 successfully enabled with serial number ZNTS
```

13. Configuração de agregação de link

A OLT 8820 G suporta agregação de links conforme padrão IEEE 802.3ad nas portas uplink. A agregação de links permite agregar as portas físicas de 10GE ou 100/1000 ethernet em uma única porta lógica agregada, afim de prover largura de banda adicional e resiliencia. Um grupo de agregação de link pode consisitir de até 8 portas.

13.1. Agregação de link e LACP

As portas uplink da OLT 8820 G suportam LACP (Link Aggregation Control Protocol), protocolo de camada 2 utilizado entre elementos de rede para trocar informações em relação à capacidade de agregação de um link.

Para configurações redundantes, as portas ethernet em ambos dispositivos devem estar configurados no modo active (ativo). Isso permite que as portas do link agregado forneça proteção redundante na porta uplink.

13.2. Comando lacp

Utilize o comando *lacp* para verificar o número da chave de agregação do parceiro ou para visualizar outras informações da agregação de link.

Sintaxe do comando *lacp*

```
iSH> lacp
Usage: lacp <agg|id|monitor|state> [portNo] | lacp stats [portNo] [clear]
```

Após conectar a OLT a um switch com LACP habilitado, é possível verificar que o número da chave do parceiro é correspondente a cada link do switch.

```
iSH> lacp monitor 2
PORT 2:
selected = SELECTED Disabled Traffic Enabled
actor state:7c
partner state:5a
1: partner key 4002, par port pri 8000, partner port # 2, actor state AGGREGATION SYNCHRONIZATION
COLLECTING DISTRIBUTING DEFAULTED, partner state LACP_TIMEOUT SYNCHRONIZATION COLLECTING
DEFAULTED
```

```
partner system: 00:00:00:00:00:00
1: agg id f03f5e0, par sys pri: 8000, agg partner key 4002
par sys: 00:00:00:00:00:00
iSH> lacp monitor 3
PORT 3:
selected = SELECTED Disabled Traffic Enabled
actor state:7c
partner state:5a
2: partner key 4002, par port pri 8000, partner port # 3, actor state AGGREGATION
SYNCHRONIZATION COLLECTING DISTRIBUTING DEFAULTED , partner state LACP _TIMEOUT
SYNCHRONIZATION COLLECTING DEFAULTED
partner system: 00:00:00:00:00:00
2: agg id f03f500, par sys pri: 8000, agg partner key 4002
par sys: 00:00:00:00:00:00
```

Agregação de link LACP modo ativo

O modo ativo suporta suporta o protocolo LACP e habilita o link ethernet para enviar e receber pacotes LACP.

Resiliência

A agregação de link permanece ativa enquanto um grupo de agregação está operacional. A agregação de link gerencia os links conforme eles falham e retornam a operação, causando a menor interrupção possível do serviço.

No entanto, se todos os links em um grupo de agregação falhar, o grupo de agregação é posto em down até que a conexão física seja restaurada.

Configuração de agregação de link

Quando o modo de agregação está ativa na porta uplink, o dispositivo envia e recebe quadros LACP e a redundância do link de agregação é dinâmica.

Configurando porta uplink para agregação de link com LACP

Ativar a agregação de link com LACP em uma porta uplink ethernet.

1. Conecte a OLT a um switch com LACP habilitado;
2. Crie a agregação de link no modo ativo e adicione a respectiva porta ethernet;

```
iSH> linkagg add group lagA/linkagg link 1-1-2-0/eth mode active
Interface lagA/linkagg does not exist
Link aggregation successfully created.

iSH> linkagg add group lagA/linkagg link 1-1-3-0/eth mode active
Link aggregation successfully created.
```

3. Para visualizar o status do modo de agregação;

```
iSH> get ether 1-1-2-0/eth
ether 1-1-2-0/eth
autonegstatus: --------->    {enabled}
mauType: --------------->    {mau1000baselxfd}
restart: --------------->    {norestart}
ifType: ---------------->    {mau1000baselxfd}
autonegcap: ------------>    {b10baseTFD+b100baseTXFD+b1000baseTFD}
remotefault: ----------->    {noerror}
clksrc: ---------------->    {automatic}
pauseFlowControl: ------>    {disabled}
aggregationMode: ------->    {active}
linkStateMirror: ------->    {0/0/0/0/0}
maxFrameSize: ---------->    {0}
ingressRate: ----------->    {0}
```

```
ingressBurstSize: ------>    {0}
egressRate: ------------>    {0}
egressBurstSize: ------->    {0}

iSH> get ether 1-1-3-0/eth
ether 1-1-3-0/eth
autonegstatus: --------->    {enabled}
mauType: --------------->    {mau1000baselxfd}
restart: --------------->    {norestart}
ifType: ---------------->    {mau1000baselxfd}
autonegcap: ------------>    {b10baseTFD+b100baseTXFD+b1000baseTFD}
remotefault: ----------->    {noerror}
clksrc: ---------------->    {automatic}
pauseFlowControl: ------>    {disabled}
aggregationMode: ------->    {active}
linkStateMirror: ------->    {0/0/0/0/0}
maxFrameSize: ---------->    {0}
ingressRate: ----------->    {0}
ingressBurstSize: ------>    {0}
egressRate: ------------>    {0}
egressBurstSize: ------->    {0}
```

4. Para visualizar a agregação de link.

```
iSH> linkagg show
LinkAggregations:
slot  unit   ifName   partner: Sys              Pri      grp ID  status   agg mode
1*    2      lagA     00:00:00:00:00:00         0x0      0x0     ACT      Active
             links    slot    port    subport   status
             1-1-2-0  1       2       0         ACT
             1-1-3-0  1       3       0         ACT
```

Removendo um grupo de agregação de link

Para remover uma porta ou um grupo de agregação de link, utilize o comando
iSH> linkagg delete group GRUPO_LAG link PORTA_ETH mode active.

Remova a porta eth 2 do grupo de agregação denominado lagA
iSH> linkagg delete group lagA/linkagg link 1-1-2-0/eth mode active
Link successfully deleted from aggregation.

Remova a porta eth 3 do grupo de agregação denominado lagA
iSH> linkagg delete group lagA/linkagg link 1-1-3-0/eth mode active
Link successfully deleted from aggregation.

> **Observação:** o grupo de agregação de link somente é removido após a remoção da última porta pertencente ao grupo de agreção em questão

Configurar bridges com agregação de link

As bridges podem ser adicionados a interfaces de agregação de links.

Criação de uma bridge linkagg intralink

É possível especificar o grupo da agregação de link ou apenas especificar uma das portas que pertence ao grupo do linkagg para que a interface de agregação de link seja adicionada em uma bridge.

Adicionando a bridge interface e especificando a interface de agregação de link. Todas as portas participantes do grupo de agregação estarão na bridge configurada.

```
iSH> bridge add lagA/linkagg intralink vlan 300
Adding bridge on lagA/linkagg
Created bridge-interface-record lagA-300/bridge
Bridge-path added successfully
```

Adicionando a bridge interface e especificando apenas uma das portas participantes do grupo de agregação de link. Todas as portas participantes do grupo de agregação estarão na bridge configurada.

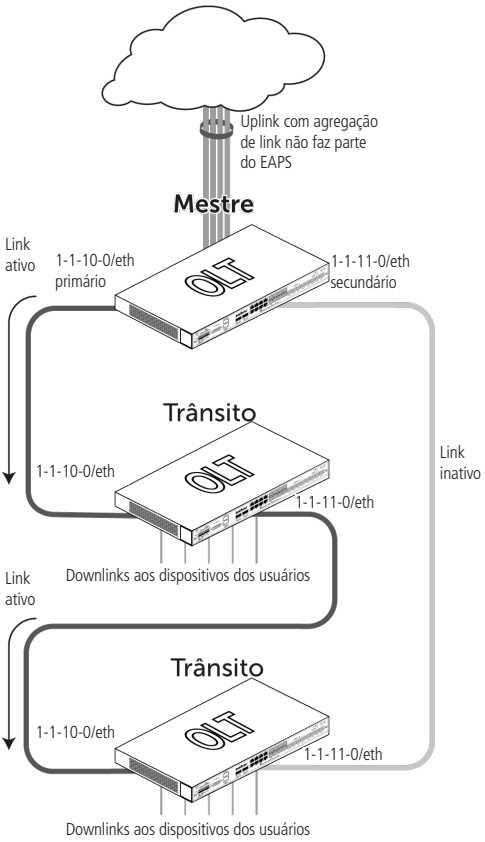
```
iSH> bridge add 1-1-2-0/eth uplink vlan 200
Adding bridge on 1-1-2-0/eth
Created bridge-interface-record 1-1-2-0-eth-200/bridge
Bridge-path added successfully
```

14. EAPS

O EAPS (RFC 3619) cria um sistema com tolerância de falhas de links fornecendo a transição rápida de um caminho primário a um caminho secundário para cada VLAN. Esse sistema é utilizado para criar um anel de modo que, se um caminho é quebrado, o outro sentido pode ser utilizado para enviar o pacote ao seu destinatário.

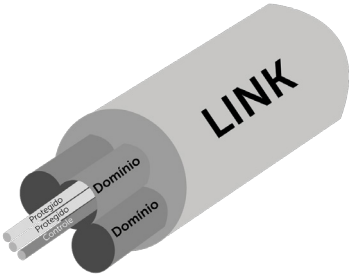
Em muitas topologias de acesso, o transporte entre nós de rede e nós da camada de distribuição devem circular por uma infraestrutura física em anel. Nesses casos, é necessário um suporte multi-plataforma para um protocolo capaz de se conectar e se comunicar com uma topologia em anel.

Como descrito na RFC 3619 "Em um Domínio EAPS existe um único anel Ethernet. Qualquer rede ethernet virtual (VLAN) a ser protegida, é configurada em todas as portas do anel para o referido domínio EAPS. Cada domínio EAPS possui um 'nó mestre'. Todos os outros nós desse anel são denominados 'nós de trânsito'.



Um anel EAPS possui um nó Mestre e um ou mais nós de trânsito. As setas exibem a direção downstream

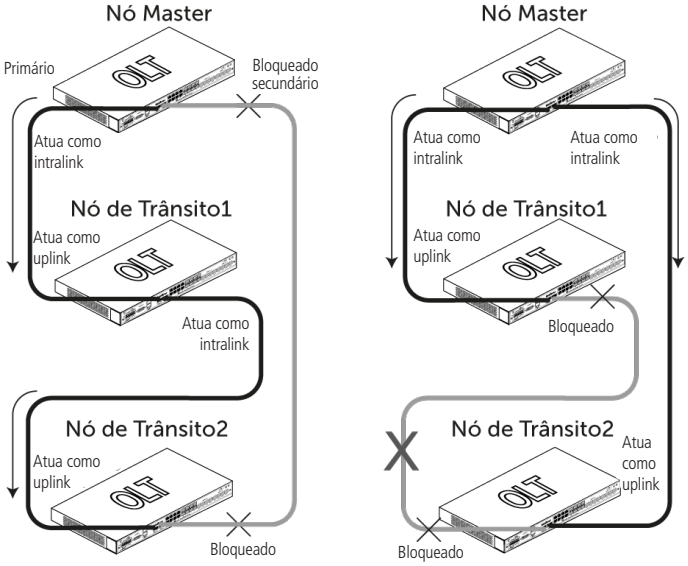
O EAPS é utilizado apenas em bridging de camada 2 e aproveita a presença de várias VLAN no mesmo link físico. Uma VLAN será configurada para ser a VLAN de controle, esta VLAN envia mensagens Health Check para todo o anel atuando como um anel de controle. Como uma bridge não pode fazer um loop em si mesmo, sempre há um link bloqueado para dados no anel EAPS, mas no anel, as mensagens de controle circulam normalmente pelo link bloqueado.



Com várias VLAN em um link, uma é a VLAN de controle que protege as outras VLAN

Cada nó mestre do anel possui duas portas que formam parte do anel. Uma é a porta primária e outra a secundária. O EAPS suporta bridges TLS e bridges assimétricas. Para bridge TLS, a porta primária de um nó mestre está ativo e a porta secundária está bloqueada e o último link no nó de trânsito que volta ao nó mestre (no estado inicial) será bloqueado, e os outros links serão deixados ativos.

Para bridges assimétricas, a porta primária no nó mestre (no estado inicial) irá agir como intralink, e o outra porta será bloqueada. Para os nós de trânsito, um rlink (nome dessas interfaces no nó de trânsito) irá agir como uplink. Se o outro nó vai para outro nó de trânsito, o outro rlink agirá como intralink. No último link que volta ao nó mestre, o rlink será bloqueado.



Ao detectar um link inativo, a interface ativa e a bloqueada podem se alterar

Se um nó de trânsito detecta que um link está desativado, ele envia a mensagem Link Fault ao nó mestre. Por isso, toda vez que houver uma mensagem Health Check em atraso ou uma mensagem Link Fault, o nó mestre mudará o sentido do tráfego para outros nós.

Quando um link está inativo, o EAPS manda mensagem na VLAN de controle informando aos outros nós que limpem suas bases de dados de brindging e altere o comportamento de cada link. Para um nó mestre, o nó bloqueado funcionará como intralink. O outro link no nó mestre e os rlinks serão ajustados também, dependendo de qual link estiver inativo.

14.1. Recomendações para sucesso no uso do EAPS

O modelo com bridge assimétrica é ideal para criar anéis EAPS maiores e mais seguros. Com o uplink e o intralink no nó mestre e rlinks nos nós de trânsito, o tráfego é circulado pelo anel utilizando a VLAN sem necessidade de multicast para determinar qual interface deve enviar o tráfego ou aprender endereços MAC. Quando a bridge TLS é utilizada, tanto o multicast como a aprendizagem do endereço MAC irão ocorrer, gerando uma carga extra desnecessária no sistema.

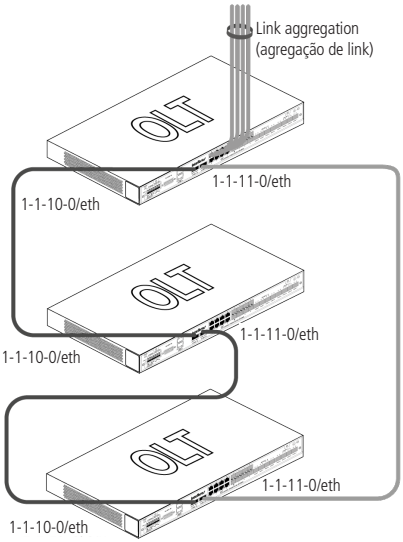
Se a bridge TLS for utilizada, é melhor que esteja isolado em um nó, ou seja, se tiver várias bridges TLS trabalhando juntos que não precisem passar por um dos rlinks. Após atravessar os rlinks, existe a questão dos endereços multicast e aprendizagem de endereços MAC, que pode se multiplicar rapidamente. Nesse ponto, as opções dos serviços de assinantes existentes nos nós podem ficar complexas em termos de carga em combinação com o EAPS.

14.2. Criação de anel EAPS assimétricos e anel EAPS TLS

O EAPS pode ser utilizado com bridges assimétricas e bridges TLS. De fato, dado que a VLAN de controle é simplesmente outra VLAN, as bridges assimétricas e TLS podem estar nas mesmas interfaces físicas.

> **Observação:** recomenda-se o uso de bridges assimétricas. Consulte Recomendações para sucesso no uso do EAPS para maiors informações. Para opções de gerenciamento de anéis EAPS, consulte Gerenciamento inband usando IP on Bridge com EAPS

EAPS assimétrico



Exemplo de EAPS assimétrico

Exemplo para criação do anel EAPS assimétrico

Os passos a seguir criam um anel EAPS como exibido na imagem anterior. Dado que os sentidos upstream e downstream são importantes em bridges assimétricas, o termo rlink é utilizado para designar as bridges interface dos nós de trânsito.

1. Configure o nó mestre;

> **Observação:** a agregação de link para o link upstream é opcional. Adicione a agregação de link para o uplink. Para esse exemplo, iremos criar uma agregação com nome de grupo lagA com seis links (portas), utilizando as portas 2, 3, 4, 5, 6 e 7. Lembre que o outro dispositivo deve estar ativo para que os links possam ser adicionados a um mesmo grupo de agregação

```
iSH> linkagg add group lagA/linkagg link 1-1-2-0/eth mode active
```

Os comandos a seguir adicionam os outros links.

```
iSH> linkagg add group lagA/linkagg link 1-1-3-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-4-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-5-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-6-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-7-0/eth mode active
```

Para verificar o linkagg:

```
iSH> linkagg show
LinkAggregations:
slot  unit  ifName  partner: Sys            Pri       grp ID    s t a - tus  agg mode
1*    1     lagA    00:01:47:d9:99:a0       0x8000    0x4000    ACT          Active
            links   slot   port   subport   status
            1-1-2-0 1      2      0         ACT
            1-1-3-0 1      3      0         ACT
            1-1-4-0 1      4      0         ACT
            1-1-5-0 1      5      0         ACT
            1-1-6-0 1      6      0         ACT
            1-1-7-0 1      7      0         ACT
```

a. Configure o nó como nó mestre, o *domain_id*, as interfaces primária e secundária e a VLAN de controle.

```
iSH> eaps add domain EAPS-Simetricro master 1-1-10-0/eth 1-1-11-0/eth control 100
```

Se não definir os valores interval, timeout e ctrlpri, serão utilizados os valores padrões:

- *interval*, 1 segundo
- *timeout*, 3 segundos
- *ctrlpri* (prioridade da VLAN de controle), 6

Ao configurar uma VLAN de controle, nenhum outro tráfego no seu dispositivo poderá utilizar essa VLAN.

b. Adicione as VLAN protegidas ao domínio.

```
iSH> eaps-vlan add domain EAPS-Simetricro 200,300,400
```

c. Habilite o nó mestre.

```
iSH> eaps enable domain EAPS-Simetricro
```

d. Adicione as bridges ao nó mestre.

```
iSH> bridge add lagA/linkagg uplink vlan 200 tagged (upstream para a nuvem, não forma parte do eaps)
iSH> bridge add 1-1-10-0/eth intralink vlan 200 tagged (link primário)
iSH> bridge add 1-1-10-0/eth intralink vlan 300 tagged (link primário)
iSH> bridge add 1-1-10-0/eth intralink vlan 400 tagged (link primário)
iSH> bridge add 1-1-11-0/eth intralink vlan 200 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth intralink vlan 300 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth intralink vlan 400 tagged (link secundário)
```

Recomenda-se o uso de intralinks ao invés de downlinks, dado que os downlinks irão salvar os endereços MAC no banco de dados de encaminhamento.

> **Observação:** dado que o nó mestre é a conexão upstream para o restante da rede, recomenda-se não colocar uma alta taxa de transferência nas portas de acesso do assinante

2. Configure o primeiro nó de trânsito;
   a. Configure o nó como nó de trânsito e defina o mesmo *domain_id* e *VLAN de controle* configurado no nó mestre. Defina as interfaces primária e secundária conforme desejado.

```
iSH> eaps add domain EAPS-Simetricro transit 1-1-10-0/eth 1-1-11-0/eth control 100
```

b. Adicione as VLAN protegidas ao domínio.

```
iSH> eaps-vlan add domain EAPS-Simetricro 200,300,400
```

c. Ative o nó de trânsito.

```
iSH> eaps enable domain EAPS-Simetricro
```

d. Adicione as bridges de transporte EAPS ao nó de trânsito.

```
iSH> bridge add 1-1-10-0/eth rlink vlan 200 tagged (link primário)
iSH> bridge add 1-1-10-0/eth rlink vlan 300 tagged (link primário)
iSH> bridge add 1-1-10-0/eth rlink vlan 400 tagged (link primário)
iSH> bridge add 1-1-11-0/eth rlink vlan 200 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth rlink vlan 300 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth rlink vlan 400 tagged (link secundário)
```

3. Configure o segundo nó de trânsito.

a. Configure o nó como nó de trânsito e defina o mesmo *domain_id* e *VLAN de controle* configurado no nó mestre. Defina as interfaces primária e secundária conforme desejado.

```
iSH> eaps add domain EAPS-Simetricro transit   1-1-10-0/eth 1-1-11-0/eth control 100
```

b. Adicione as VLAN protegidas ao domínio.

```
iSH> eaps-vlan add domain EAPS-Simetricro 200,300,400
```

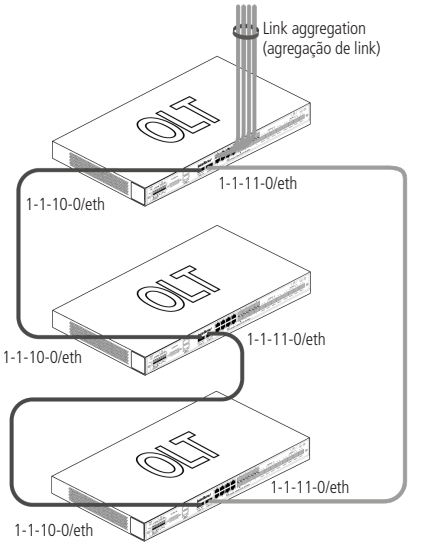
c. Ative o nó de trânsito.

```
iSH> eaps enable domain EAPS-Simetricro
```

d. Adicione as bridges de transporte EAPS ao nó de trânsito.

```
iSH> bridge add 1-1-10-0/eth rlink vlan 200 tagged (link primário)
iSH> bridge add 1-1-10-0/eth rlink vlan 300 tagged (link primário)
iSH> bridge add 1-1-10-0/eth rlink vlan 400 tagged (link primário)
iSH> bridge add 1-1-11-0/eth rlink vlan 200 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth rlink vlan 300 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth rlink vlan 400 tagged (link secundário)
```

EAPS simétrico (TLS)



Exemplo de anel EAPS utilizanda bridge simétrica (TLS)

Exemplo para criação do anel EAPS simétrico (TLS)

A única diferença entre criar um anel EAPS simétrico, utilizando a bridges TLS com EAPS assimétrico é que, ao invés de designar a bridge interface como *rlink* no caso das bridges assimétricas, a bridge interface é designada como *tls*. O exemplo da criação do anel EAPS simétrico (TLS) é exibido na imagem anterior.

1. Configure o nó mestre;

> **Observação:** a agregação de link para o link upstream é opcional. Adicione a agregação de link para o uplink. Para esse exemplo, iremos criar uma agregação com nome de grupo lagA com seis links (portas), utilizando as portas 2, 3, 4, 5, 6 e 7. Lembre que o outro dispositivo deve estar ativo para que os links possam ser adicionados a um mesmo grupo de agregação

```
iSH> linkagg add group lagA/linkagg link 1-1-2-0/eth mode active
```

Os comandos a seguir adicionam os outros links.

```
iSH> linkagg add group lagA/linkagg link 1-1-3-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-4-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-5-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-6-0/eth mode active
iSH> linkagg add group lagA/linkagg link 1-1-7-0/eth mode active
```

Para verificar o linkagg:

```
iSH> linkagg show
LinkAggregations:
slot  unit   ifName   partner: Sys            Pri       grp ID    s t a - tus  agg mode
1*    1      lagA     00:01:47:d9:99:a0       0x8000    0x4000    ACT          Active
             links    slot   port   subport   status
             1-1-2-0  1      2      0         ACT
             1-1-3-0  1      3      0         ACT
             1-1-4-0  1      4      0         ACT
             1-1-5-0  1      5      0         ACT
             1-1-6-0  1      6      0         ACT
             1-1-7-0  1      7      0         ACT
```

a. Configure o nó como nó mestre, o *domain_id*, as interfaces primária e secundária e a VLAN de controle.

```
iSH> eaps add domain EAPS-Assimetricro master 1-1-10-0/eth 1-1-11-0/eth control 100
```

Se não definir os valores interval, timeout e ctrlpri, serão utilizados os valores padrões:

- *interval*, 1 segundo.
- *timeout*, 3 segundos.
- *ctrlpri* (prioridade da VLAN de controle), 6.

b. Adicione as VLAN protegidas ao domínio.

```
iSH> eaps-vlan add domain EAPS-Assimetricro 200,300,400
```

c. Ative o nó mestre.

```
iSH> eaps enable domain EAPS-Assimetricro
```

d. Adicione as bridges ao nó mestre.

```
iSH> bridge add lagA/linkagg uplink vlan 200 tagged (upstream para a nuvem, não forma parte do eaps)
iSH> bridge add 1-1-10-0/eth intralink vlan 200 tagged (link primário)
iSH> bridge add 1-1-10-0/eth intralink vlan 300 tagged (link primário)
iSH> bridge add 1-1-10-0/eth intralink vlan 400 tagged (link primário)
iSH> bridge add 1-1-11-0/eth intralink vlan 200 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth intralink vlan 300 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth intralink vlan 400 tagged (link secundário)
```

> **Observação:** dado que o nó mestre é a conexão upstream para o restante da rede, recomenda-se não colocar uma alta taxa de transferência nas portas de acesso do assinante

2. Configure o primeiro nó de trânsito;

a. Configure o nó como nó de trânsito e defina o mesmo *domain_id* e *VLAN de controle* configurado no nó mestre. Defina as interfaces primária e secundária conforme desejado.

```
iSH> eaps add domain EAPS-Assimetricro transit 1-1-10-0/eth 1-1-11-0/eth control 100
```

Ao configurar uma VLAN de controle, nenhum outro tráfego no seu dispositivo poderá utilizar essa VLAN.

b. Adicione as VLAN protegidas ao domínio.

```
iSH> eaps-vlan add domain EAPS-Assimetricro 200,300,400
```

c. Ative o nó de trânsito.

```
iSH> eaps enable domain EAPS-Assimetricro
```

d. Adicione as bridges ao nó de trânsito.

```
iSH> bridge add 1-1-10-0/eth tls vlan 200 tagged (link primário)
iSH> bridge add 1-1-10-0/eth tls vlan 300 tagged (link primário)
iSH> bridge add 1-1-10-0/eth tls vlan 400 tagged (link primário)
iSH> bridge add 1-1-11-0/eth tls vlan 200 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth tls vlan 300 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth tls vlan 400 tagged (link secundário)
```

3. Configure o segundo nó de trânsito.

a. Configure o nó como nó de trânsito e defina o mesmo *domain_id* e *VLAN de controle* configurado no nó mestre. Defina as interfaces primária e secundária conforme desejado.

```
iSH> eaps add domain EAPS-Assimetricro transit 1-1-10-0/eth 1-1-11-0/eth control 100
```

b. Adicione as VLAN protegidas ao domínio.

```
iSH> eaps-vlan add domain EAPS-Assimetricro 200,300,400
```

c. Ative o nó de trânsito.

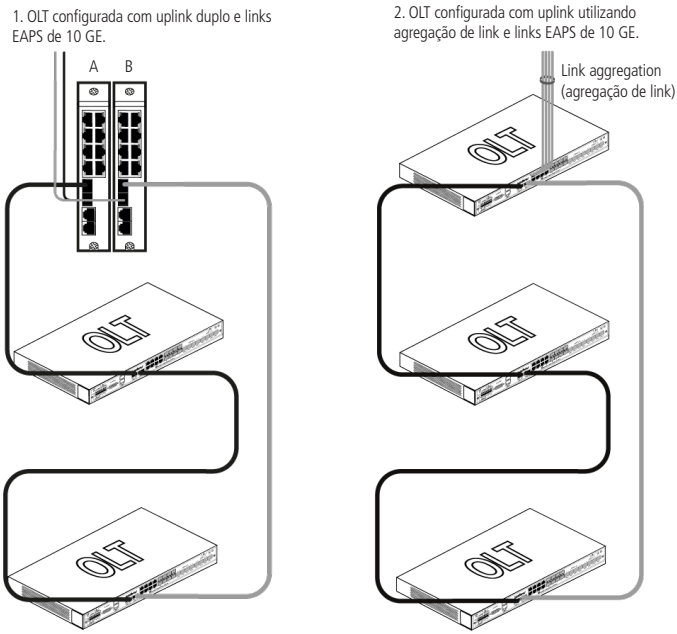
```
iSH> eaps enable domain EAPS-Assimetricro
```

d. Adicione as bridges ao nó de trânsito.

```
iSH> bridge add 1-1-10-0/eth tls vlan 200 tagged (link primário)
iSH> bridge add 1-1-10-0/eth tls vlan 300 tagged (link primário)
iSH> bridge add 1-1-10-0/eth tls vlan 400 tagged (link primário)
iSH> bridge add 1-1-11-0/eth tls vlan 200 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth tls vlan 300 tagged (link secundário)
iSH> bridge add 1-1-11-0/eth tls vlan 400 tagged (link secundário)
```

14.3. Topologias comuns de configuração de anel EAPS

O EAPS é extremamente flexível a respeito do cabeamento entre nós do anel EAPS. Os anéis EAPS podem ser criados com links 10G ou 1GE. Os anéis EAPS podem ser combinados com uma agregação de links. Até oito links podem ser agregados para criar um anel EAPS. Alguns nós possuem uplinks duplos (normalmente o nó Mestre), e outros podem ter só um uplink.



Cenários EAPS mais comuns podem combinar uplinks simples e duplos

14.4. Comandos de topologia EAPS

Para visualizar a topologia de um anel EAPS, utilize o comando *eaps topo* ou *eaps topo2*. O comando *eaps show* exibirá o status geral do anel e as informações da VLAN de controle.

```
iSH> eaps show
                Domain                Status           Type   Primary    Secondary  CtrlVlan
                example_simple_ring   Active-Healthy   M      1-1-10-0   1-1-11-0   4089
```

O comando eaps topo exibe a topologia eaps partindo da visão da OLT onde o comando foi inserido (através da identificação **** e 0 hops), o endereço MAC da bridge de uplink, o endereço IP (se houver), se o nó é um nó mestre ou nó de trânsito (M/T). Se um link estiver como down, será exibido um "x" na interface em que o link do anel eaps está com falha.

O comando *eaps topo* ainda está disponível através do comando *eaps topo2* e possui a mesma ideia de identificação da topologia conforme descrito anteriormente, em vez do comando retornar "x" em caso de falha em algum link, o retorno será (up/dn).

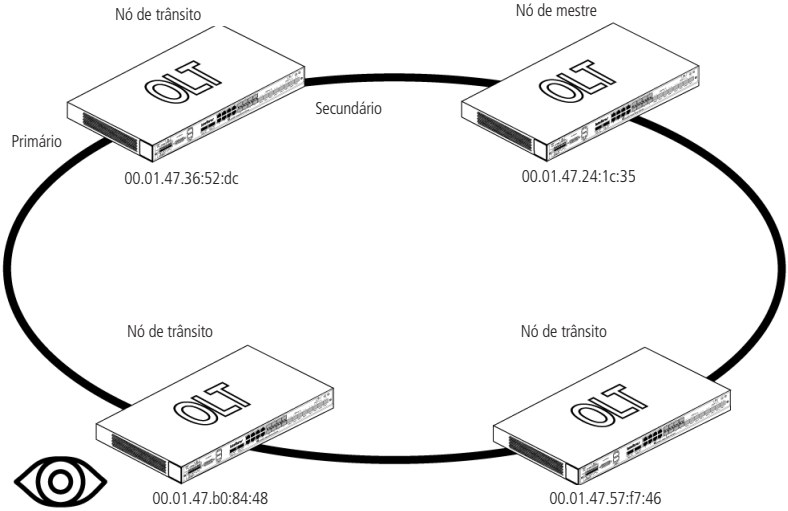
O comando *eaps topo2* também exibe o caminho de ambos os sentidos a partir do nó de visualização, de modo que haverá *2n-1* linhas na exibição das informações do anel. Assim em um anel eaps com 4 nós em perfeito estado de funcionamento, será exibo 7 linhas de informação ao realizar o comando *eaps topo2*. Para um aneal eaps com falha em algum link, será exibido a informação de entrada para cada nó.

Eaps topo

O olho no diagrama exibe em qual nó o comando é executado; observe que no resultado do comando, a linha que conter a informação **** informa o nó de onde foi executado o comando. O comando exibe os nós da topologia EAPS em cada sentido até alcançar o nó que foi executado o comando, ou caso houver algum link com falha no anel.

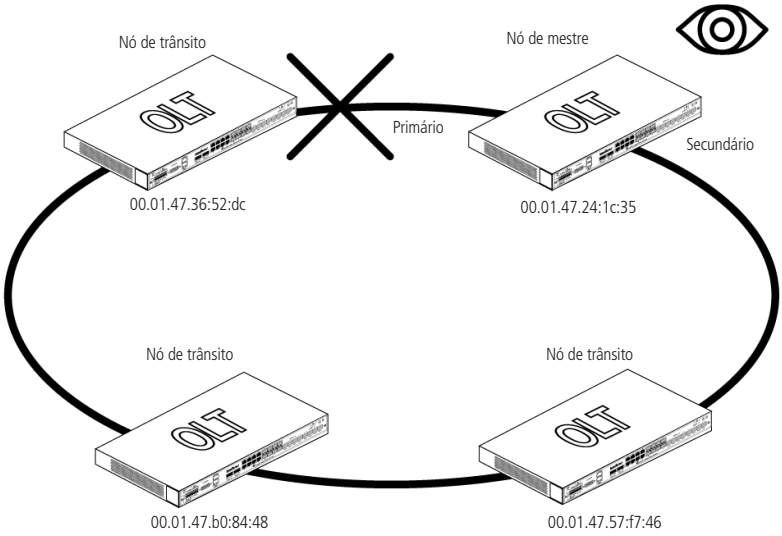
A informação exibe o nome do domínio, assim como a VLAN de controle e o status do anel EAPS.

```
iSH> eaps topo
Domain "4nodes"    [CtrlVlan:2000,State:Active-Healthy]:
Ring      Hop      Mac Addr           IP           Addr   Type      Links
Pri       3        00:01:47:24:1c:35  10.55.5.198  M      1-1-11-0  1-1-10-0
Pri       2        00:01:47:36:52:dc  10.51.13.1   T      1-1-11-0  1-1-10-0
Pri       1        00:01:47:57:f7:46  10.51.12.1   T      1-1-11-0  1-1-10-0
****      0        00:01:47:b0:84:48  10.55.2.199  T      1-1-11-0  1-1-10-0
```



Anel EAPS com quatro nós em estado normal

Se houver uma falha no anel, o link será designada por um *x* onde a interface detectou a falha.



O comando topo será exibido até a ruptura

```
iSH> eaps topo
Domain "4nodes"    [CtrlVlan:2000,State:Active-Healthy]:
Ring      Hop      Mac Addr            IP           Addr   Type        Links
****      0        00:01:47:24:1c:35   10.55.5.198  M      1-1-11-0    1-1-10-0 x
Sec       3        00:01:47:36:52:dc   10.51.13.1   T      1-1-11-0 x  1-1-10-0
Sec       2        00:01:47:57:f7:46   10.51.12.1   T      1-1-11-0    1-1-10-0
Sec       1        00:01:47:b0:84:48   10.55.2.199  T      1-1-11-0    1-1-10-0
```

Com o sistema log ativo, os alertas serão exibidos na sessão.

```
iSH> MAR 17 11:47:47: alert: 1/10/0: eapsrp: _EapsNodeStateSet(): l=10176: bcmRX: Domain 4nodes:
Active-Healthy --> Ring Fault
```

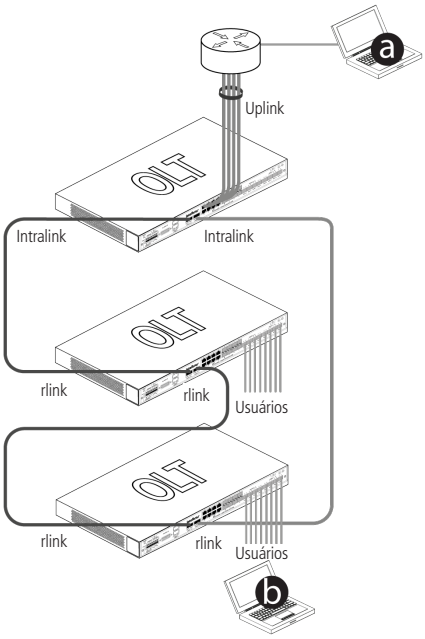
14.5. Gerenciamento inband usando IP on Bridge com EAPS

EAPS é uma solução em camada 2. Para gerenciamento via IP, uma interface ipobridge é criada no nó como interface de gerenciamento.

Gerenciamento em um anel EAPS assimétrico

O nó mestre deve ser configurado com uma interface uplink e interfaces intralinks; os nós de trânsito utilizam rlinks, como descrito em EAPS Assimétrico.

No nó mestre, deve ser criado um *ipobridge* na VLAN de gerenciamento de um dos intralinks. Para os nós de trânsito, deve ser criado um *ipobridge* na VLAN de gerenciamento de um dos rlinks.



Para gerenciar a partir de dentro da rede o nó mestre do EAPS necessita estar em um sub-rede separada

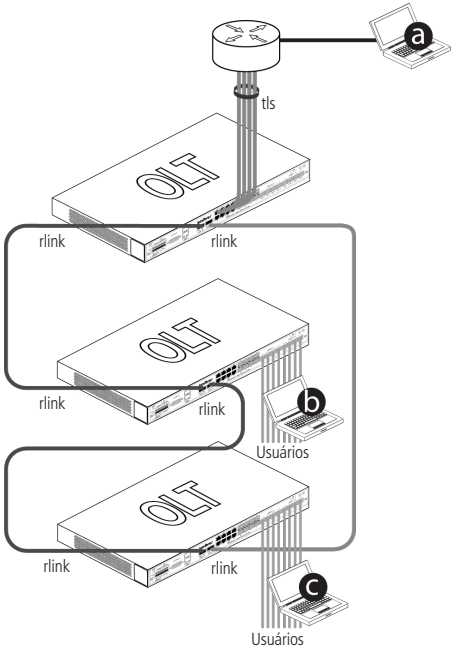
Dado que o EAPS é uma solução de camada 2, o roteador irá aprender os endereços MAC para o nó mestre do anel EAPS.

Se todos os nós estão na mesma sub-rede IP, somente será possível gerenciar os nós do anel a partir do lado externo do anel, como designado no gráfico PC a.

Para gerenciar a partir de dentro do anel EAPS assimétrico, a interface *ipobridge* para o nó mestre deve estar em uma sub-rede IP diferente daquela onde estão os nós de trânsito. Os nós de trânsito podem estar na mesma sub-rede IP. Não há problemas se os nós de trânsito estão na mesma sub-rede IP. Desse modo, o gerenciamento do anel EAPS pode ser realizado pelos computadores designados como PCs b e c no gráfico.

Gerenciamento em um anel EAPS simétrico (TLS)

Para um anel EAPS simétrico (TLS), inserir a interface ipobridge em um dos rlinks de cada nó, seja ele mestre ou de trânsito. A bridge interface TLS fará multicast para encontrar e armazenar os endereços MAC. Ao ter a tabela de encaminhamento completa os dispositivos do anel eaps podem estar na mesma sub-rede IP.



Exemplo de gerenciamento em anel EAPS (TLS)

Criação de uma interface ipobridge para um aneal EAPS

Os comandos a seguir assumem um nó mestre e dois nós de trânsito. Em conjunto com outras VLAN, a VLAN 300, 301 e 302 são adicionadas como VLAN protegidas. Como nos exemplos de configuração acima, o uplink utiliza linkagg (para criar um anel EAPS (exemplo assimétrico) e para criar um anel EAPS (exemplo TLS)).

Perceba que, enquanto a interface virtual ou física é fornecida, o ipobridge é criado na VLAN, então somente uma interface ipobridge precisa ser criada por nó TLS. O ipobridge será TLS se foi criado em uma VLAN TLS, e será downlink se foi criada em uma VLAN assimétrica.

1. Adicione a interface ip ao nó mestre;

```
iSH> interface add lagA/linkagg vlan 300 192.168.120.1/24
```

O nó mestre deve ser configurado com um uplink e intralinks.

2. Adicione a interface ip ao nó de trânsito;

```
iSH> interface add 1-1-10-0/ipobridge vlan 301 193.168.121.1/24
```

os nós de trânsito devem utilizar a bridge TLS, porque o comando *interface add ipobridge* cria automaticamente uma bridge interface TLS na VLAN.

> **Observação:** bridge interfaces assimétricas (uplink, downlink, intralink, rlink) não podem ser utilizadas na mesma VLAN onde há interfaces TLS

3. Adicione a interface ipobridge ao outro nó de trânsito.

```
iSH> interface add 1-1-10-0/ipobridge vlan 302 194.168.122.1/24
```

Os nós de trânsito devem utilizar a bridge TLS, porque o comando *interface add ipobridge* cria automaticamente uma bridge interface TLS na VLAN.

> **Observação:** bridge interfaces assimétricas (uplink, downlink, intralink, rlink) não podem ser utilizadas na mesma VLAN onde há interfaces TLS

14.6. Comandos EAPS

Eaps

O comando *eaps* configura um nó mestre ou de trânsito em um anel EAPS.

Sintaxe **eaps <add|delete|disable|enable|help|modify|show|topo>**

Sintaxe `eaps add domain domain_id <master|transit> control vlan <interface1> interface1/type <interface2> interface2/type <interval value> <drop value> <timeout value> <trap [yes|no]> <cntlpri value>`

O comando *eaps add* cria um nó EAPS como nó mestre ou de trânsito, define quais interfaces são interfaces primárias e secundárias do nó, define a VLAN de controle para o nó EAPS (a VLAN de controle deve ser igual em todos os nós do anel EAPS) e define outras variáveis, como os intervalos entre mensagens Health Check, a quantidade de tempo antes de determinar a falha do link, se envia mensagens de alerta SNMP e define a prioridade das mensagens na VLAN de controle e nas VLAN protegidas. Um nó novo recém adicionado é colocado com status Inactive.

» **domain domain_id**

domain é o valor alfanumérico (ex. nome da linha) do domínio. è atribuído pelo assinante e deve representar a descrição do Domínio (por exemplo, a qual anel pertence o nó, como em "South_Campus", qual nó, "transit_node_2", ou uma combinação desses dados "South_Campus_transit_node_2").

» **master|transit**

O parâmetro *master|transit* define o status do nó em um anel; em um domínio, somente um nó pode ser mestre e somente uma VLAN pode ser de controle. Todos os outros nós devem ser de trânsito.

<interface1> interface1/type

O parâmetro interface1 define a porta primária.

<interface2> interface2/type

O parâmetro interface2 define a porta secundária.

» **control vlan**

O parâmetro *control* define a VLAN de controle para o domínio do anel EAPS. Todos os nós no mesmo anel EAPS devem utilizar a mesma VLAN de controle.

» **interval time**

O parâmetro *interval* determina o tempo em segundos entre as mensagens Health (frequência) para transmiti-las para fora da porta primária do anel. O parâmetro interval somente é válido para nós mestre. O valor padrão utilizado para interval quando não há configuração determinada no comando é de um segundo.

» **timeout time**

O parâmetro *timeout* determina a duração da desconexão em segundos. Para o Nó Mestre ese é o intervalo desde o último recebimento de uma mensagem HELLO antes de que o nó mestre informe a falha do anel. O valor padrão utilizado para *timeout* quando não há configuração determinada no comando é de três segundos.

Para um Nó de Trânsito, esse é o intervalo em que o Nó permanecerá no status Preforwarding antes de passar (no caso de recebimento de mensagem Ring Up) para o modo Health. O valor padrão utilizado para *timeout* quando não há configuração determinada no comando é de quinze segundos.

» **trap <on | off>**

O parâmetro trap determina se o nó enviará um alerta SNMP descrevendo a mudança de status.

» **cntlpri priority**

O parâmetro *cntlpri* determina a prioridade com que as mensagens Control serão enviadas. O valor padrão utilizado para *cntlpri* quando não há configuração determinada no comando é de seis segundos.

Sintaxe `eaps modify domain domain_id <master|transit> <control vlan> <interface1 interface1/type> <interface2 interface2/type> <interval value> <drop value> <timeout value> <trap [yes|no]> <cntlpri value>`

O comando *eaps modify* altera as variáveis configuráveis de um nó EAPS. O nó EAPS deve ser desativado antes de utilizar o comando *eaps modify.*

» **Sintaxe:** eaps show domain <domain_id|all>

O comando *eaps show* exibe a lista de VLAN protegidas para o domínio, se tal lista existir. O comando retorna um erro se o *domain_id* fornecido não existe.

» **domain domain_id|all>**

domain é o valor alfanumérico (ex. nome da linha) do domínio. è atribuído pelo assinante e deve representar a descrição do Domínio (por exemplo, a qual anel pertence o nó, como em "South_Campus", qual nó, "transit_node_2", ou uma combinação desses dados "South_Campus_transit_node_2").

All exibe todas as conexões eaps do nó.

» **Sintaxe:** eaps topo domain domain_name

Exibe as informações de topologia correspondentes aos anéis EAPS nos quais o nó participa.

» **Sintaxe:** eaps disable domain domain_id

O comando *eaps disable* desativa o domínio existente no nó. (o nó não encaminha tráfego). Para modificar um nó com o comando *eaps modify*, o nó deve ser desativado primeiro.

» **Sintaxe:** eaps enable domain domain_id

O comando *eaps enable* ativa o domínio existente no nó. O comando *eaps enable* altera o status do domínio de disabled para enabled, para que o nó possa encaminhar o tráfego dasVLAN protegidas.

eaps-vlan

O comando *eaps-vlan* cria, modifica, remove ou exibe VLAN protegidass em um nó EAPS.

» **Sintaxe**

```
eaps-vlan <add | delete | modify | show > domain domain_id VLAN_List
```

» **Sintaxe:** eaps-vlan add domain domain_id VLAN_List

O comando *eaps-vlan add* cria uma VLAN protegida ou uma lista de VLAN protegidas para um domínio existente. O comando retornará um erro se o domain_id fornecido não existe.

A lista de VLAN protegidas está composta de registros separados por vírgula. Um registro pode ser uma VLAN ID simples ou um conjunto de VLAN ID separados por traços. As VLAN ID devem ser maiores do que zero e menores que 4090. Pode utilizar no máximo quatro registros. Não são permitidos espaços, ex. "eaps-vlan add domain metro2 100-113,205,370-420,999" criaria uma lista de VLAN protegidas para o Domínio "metro2" formada pelas VLAN 100 até 113, VLAN 205, VLANs 370 até 420 e VLAN 999.

» **Sintaxe:** eaps-vlan delete domain domain_id VLAN_List

O comando *eaps-vlan delete* remove uma VLAN protegida ou uma lista de VLAN protegidas de um domínio existente. O comando retornará um erro se o *domain_id* fornecido não existe.

» **Sintaxe:** eaps-vlan modify domain domain_id VLAN_List

O comando *eaps-vlan modify* altera uma VLAN protegida ou uma lista de VLAN protegidas de um domínio existente. O comando retornará um erro se o *domain_id* fornecido não existe.

» **Sintaxe:** eaps-vlan show domain <domain_id|all>

O comando *eaps-vlan show* exibe a lista de VLAN protegidas de um domínio existente. O comando retornará um erro se o *domain_id* fornecido não existe.

15. Diagnósticos e gerenciamento

15.1. Logs da OLT 8820 G

Resumo

Os logs possibilitam aos administradores monitorar eventos de sistema gerando mensagens do sistema. As mensagens são enviadas para:

- Uma sessão de gerenciamento temporário (seja na porta serial ou em uma sessão telnet/SSH).
- Um servidor syslog (opcional).
- Módulos de log para criar arquivos de log permanentes.

O tipo de informações enviado nessas mensagens pode ser configurado utilizando o comando log. Por padrão, o sistema envia o mesmo tipo de informação para todos os destinatários da mensagens de log. Se desejar enviar diferentes tipos de mensagens para um syslog, utilize o comando *syslog*.

Nível padrão de armazenamento de logs

Por padrão a OLT 8820 G armazena os logs com nível de criticidade de emergência (emergency), portanto ao realizar o comando *log display* é exibido apenas as mensagens de nível de emergência. Para salvar os registros de log do console dentro do diretório /card1/log da OLT, utilize o comando *consolelog on*. Utilize o comando *consolelog off*. para parar de salvar os registros de log. Os comandos *consolelog on* e *consolelog off* estão habilitados apenas para usuários com nível de permissão debug.

Ao utilizar o comando *log cache* são exibidos todas as mensagens que foram gravadas no console.

Utilize os comandos *cd log* e *dir* para visualizar o histórico de arquivos de log. Os arquivos de log nesse diretório gravam as atividades do console da OLT 8820 G preservando uma cópia dos dois últimos reinícios. Os arquivos *consolelog1.txt* e *consolelog2.txt* mantem as últimas 10000 linhas de saída do console de cada arquivo. Uma vez que o arquivo chega a 10000 linhas, o nome do arquivo é alterado para *.old* e um novo arquivo *.txt* é usado. Após uma reinicialização, os arquivos *.txt* também são salvos como arquivos *.old*. Use o comando *consolelog display <filename>* para visualizar os conteúdos para um arquivo consolelog. Esses arquivos são usados para resolução de problemas e monitoramento da atividade do sistema.

Notificação de login de usuário

As notificações de login de usuários são enviadas ao log do console.

```
SEP 28 10:51:12: alert      : 1/1/1027: clitask0: User admin logged in on slot 1
SEP 28 10:26:39: alert      : 1/1/1028: clitask1: User admin logged out from slot
```

Comando log filter

O comando *log filter* permite que os usuários configurem níveis de logs customizados.

Log filter

O comando *log filter* permite que os usuários configurem níveis de logs customizados por:

- ifindex.
- slot e porta.
- VPI e VCI para um VCL.
- Terminal do usuário.
- Grupo de interface e CID.
- ifstack high-ifindex, low-ifindex.

As entradas do objeto especificado são armazenadas bem como todas as entradas dos níveis de log superiores ou iguais ao nível selecionado. Os níveis de logs são classificados conforme sua criticidade e possuem a seguinte sequencia (maior criticidade para menor criticidade): emergency (emergência), alert (alerta), critical (crítico), error (erro), warning (aviso), notice (notificação), information (informação) e debug (debug). Os carateres curingas "*" e "ANY" podem ser utilizados para gerenciar múltiplos filtros.

Sintaxe **`log filter set [ifindex ifindex] | [port slot/port] | [vcl ifindex vpi vci] | [subscriber endpoint] | [igcrv ivcrv] | [ifstack ifindex high-ifindex low-ifindex] loglevel`**

» **ifindex**

Número ifindex desejado. Use o comando *if-translate* para exibir o número ifindex.

```
iSH> get if-translate 1-1-2-0/eth
if-translate 1-1-2-0/eth
ifIndex: ----------------->    {4}
shelf: ------------------->    {1}
slot: -------------------->    {1}
port: -------------------->    {2}
subport: ----------------->    {0}
type: -------------------->    {eth}
adminstatus: ------------->    {up}
physical-flag: ------------>    {true}
iftype-extension: -------->    {none}
ifName: ------------------>    {1-1-2-0}
redundancy-param1: ------>    {0}
description-index: ------>    {0}
```

» **slot port**

Slot e porta aos quais o filtro de log é aplicado.

» **vpi vci**

Caminho e canal virtual aos quais o filtro de log é aplicado.

» **endpoint**

Terminal do usuário ao qual o filtro de registros é aplicado.

» **vpi vci cid**

Caminho e canal virtual e identificador de chamada aos quais o filtro de log é aplicado.

» **ig crv**

Grupo de interface e registro de usuários aos quais o filtro de log é aplicado.

» **high-ifindex low-ifindex**

Valores altos e baixos de ifindex aos quais o filtro de log é aplicado.

» **loglevel**

Define o nível em que as entradas de log são salvas. As entradas são registradas para o nível de log selecionado e para todos os níveis superiores.

» **Sintaxe:** log filter show

Exibe todos os filtros atualmente definidos.

» **Sintaxe:** log filter delete index

Exemplo

```
iSH> log filter set port 1 1 alert
     New filter saved.
     iSH> log filter show

     iSH> log filter delete 1
     Log filter 1 deleted
```

Habilitar/desabilitar log de sessões temporário

Por padrão, mensagens de log são habilitadas na porta serial. Use o comando *log session* e o comando *log serial* para habilitar/desabilitaras mensagens de log:

O comando log session habilita/desabilita mensagens de log somente para a sessão telnet/SSH atualmente conectado. Se o usuário fizer logout, a configuração de log retorna para o padrão:

```
iSH> log session off
Logging disabled.

iSH> log session on
Logging enabled.
```

O comando *log serial* habilita/desabilita mensagens de log para a sessão na porta serial.

```
iSH> log serial on
Serial port logging enabled.

iSH> log serial off
Serial port logging disabled.
```

Enviar informações de log para um servidor syslog

A tabela a seguir descreve os parâmetros no perfil *syslog-destination* para enviar mensagens para um servidor syslog.

Parâmetro	Descrição
address	Endereço de IP da máquina hospedando o servidor syslog. Padrão: *0.0.0.0*
port	Porta UDP à qual as mensagens syslog serão enviadas. Padrão: *514*
facility	Recursos do syslog à qual as mensagens syslog serão enviadas. Valores: local0, local1, local2, local3, local4, local5, local6, local7, no-map Padrão: *local0*
severity	O nível de criticidade das mensagens enviadas ao servidor syslog. Valores: emergency, alert, critical, error, warning, notice, info, debug Padrão: *debug*

Parâmetros do perfil syslog-destination

```
iSH> new syslog-destination 1
Please provide the following: [q]uit.
address: ----->    {0.0.0.0}: 192.200.42.5 Endereço IP do servidor syslog
port: ------->     {514}: Preferencialmente, deixar o valor padrão
facility: --->     {local0}:
severity: --->     {debug}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Criar módulos de registro

O comando *log-module* cria arquivos de logs que persistirão durante reinicializações da OLT. O perfil *log-module* suporta a configuração de mensagens de log persistentes, mensagens syslog e níveis de armazenamento persistente por módulo. Modifique este perfil quando você desejar enviar mensagens diferentes para sessões de admin, para logs persistentes e para o servidor syslog. A tabela a seguir descreve os parâmetros *log-module*.

Parâmetro	Descrição
name	O nome do módulo cujo registro é controlado por este perfil. Padrão: *logtest*
display	Exibe as mensagens de log do nível de criticidade igual ou superior ao escolhido. Valores: emergency, alert, critical, error, warning, notice, info, debug Padrão: *error*
syslog	Controla o formato das mensagens enviadas ao servidor syslog descritas no perfil syslog-destination . Este campo é semelhante ao campo display, exceto para o valor trackdisplay. Valores: emergency, alert, critical, error, warning, notice, info, debug, trackdisplay Mensagens de log iguais ou superiores ao nível determinado no parâmetro display também serão gravados no servidor syslog. Padrão: *trackdisplay*
store	Controla o armazenamento persistente das mensagens. Este campo é semelhante ao campo display, exceto para o valor trackdisplay. Valores: emergency, alert, critical, error, warning, notice, info, debug, trackdisplay Mensagens de log iguais ou superiores ao nível determinado no parâmetro display também serão gravados no servidor syslog. Padrão: *trackdisplay*

Parâmetros do perfil log-module

```
iSH> new log-module 1
Please provide the following: [q]uit.
name: --------->    {logtest}: test1
display: ----->    {error}: warning
syslog: ------>    {trackdisplay}:
store: -------> {trackdisplay}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Formato das mensagens de log

A tabela a seguir descreve as informações que cada mensagem de log pode conter.

Opção	Descrição
Time	Identificação de tempo da mensagem de log. Ativado como padrão.
Date	Identificação de data da mensagem de log. Ativado como padrão.
Level	Nível de criticidade da mensagem de log. Ativado como padrão.
Taskname	Nome da tarefa que gerou a mensagem de log. Esta informação é útil somente para o P&D da Intelbras. Ativado como padrão.
Task ID	Identificação da tarefa que gerou a mensagem de log. Esta informação é útil somente para o P&D da Intelbras. Ativado como padrão.
File	Nome do arquivo que gerou a mensagem de log. Esta informação é útil somente para o P&D da Intelbras. Ativado como padrão.
Function	Função que gerou a mensagem de log. Esta informação é útil somente para o P&D da Intelbras. Ativado como padrão.
Line	Linha de código que gerou a mensagem de log. Esta informação é útil somente para o P&D da Intelbras. Ativado como padrão.

Campos da mensagem de log padrão

Para exibir ou alterar as informações das mensagens de log, use o comando *log option:*

```
iSH> log option
Usage: log option              < time            | 1 > < on       | off >
                               < date            | 2 > < on       | off >
                               < level           | 3 > < on       | off >
                               < taskname        | 4 > < on       | off >
                               < taskid          | 5 > < on       | off >
                               < file            | 6 > < on       | off >
                               < function        | 7 > < on       | off >
                               < line            | 8 > < on       | off >
                               < port            | 9 > < on       | off >
                               < category        | 10 > < on      | off >
                               < system          | 11 > < on      | off >
                               < ticks           | 12 > < on      | off >
                               < stack           | 13 > < on      | off >
                               < globalticks     | 14 > < on      | off >
                               < all             | 14 > < on      | off >
                               < default         | 15 > < on      | off >
> options 'time' & 'date' supercede option 'ticks'
time: date: level: address: log: port: category: system: (0x707)
```

Para habilitar ou desabilitar os campos de informações das mensagens de log, insira a opção "on" ou "off". Por exemplo, o comando a seguir desativará o ID de tarefa nas mensagens de log.

```
iSH> log option taskid off
time: date: level: address: log: taskname:     (0xf)
```

Modificar níveis de criticidade

Para modificar os níveis de criticidade dos logs, use o comando *log*. Para modificar mensagens syslog, use o comando *syslog*.

Para exibir os níveis de criticidade de todos os módulos de log, use o comando *log show:*

```
iSH> log show
MODULE                LEVEL          STATUS
alarm_mgr             error          enabled
bds                   error          enabled
bridge                error          enabled
bridgemib             error          enabled
bridgerp              error          enabled
bulkstats             error          enabled
bulkstatshdlr         error          enabled
cam                   error          enabled
card                  error          enabled
card_resource         error          enabled
cli                   error          enabled
cssagent              error          enabled
dhcpclient            error          enabled
dhcpclib              error          enabled
dhcpmibhandler        error          enabled
dhcpsax               error          enabled
dhcpserver            error          enabled
diags                 error          enabled
.....
```

Os níveis de criticidade de log determinam o número de mensagens exibidas no console. Quanto maior for o nível de criticidade, mais mensagens são exibidas. A OLT 8820 G suporta os seguintes níveis de criticidade de log:

- 1: emergency (emergência)
- 2: alert (alerta)
- 3: critical (crítico)
- 4: error (erro)
- 5: warning (aviso)
- 6: notice (notificação)
- 7: information (informação)
- 8: debug (debug)

Para alterar o nível de criticidade de log, use o comando *log module level*. Por exemplo, o comando a seguir altera o nível de criticidade do módulo *card* para emergência:

```
iSH> log level card emergency
Module: card at level: emergency
```

Para habilitar ou desabilitar níveis de criticidade de um módulo, use os comandos log enable ou log disable. Por exemplo:

```
iSH> log disable card
Module: card is now disabled
```

Utilização do log cache

O comando *log cache* exibe as mensagens de log não persistentes. Ele utiliza a sintaxe a seguir:

- **Log cache**

Exibe as mensagens de log em cache.

» **Log cache max length**

Define o número máximo de mensagens de log a armazenar. O tamanho máximo de cache de registros é 2147483647, dependendo da quantidade de memória disponível.

» **Log cache grep pattern**

Busca no cache de logs a expressão regular especificada.

» **Log cache clear**

Limpa o cache de logs.

» **Log cache size**

Define o tamanho máximo de memória para o cache de logs. Sem opções, exibe o tamanho atual do log.

» **Log cache help**

Exibe ajuda do comando *log cache*.

Exemplos

Para alterar o tamanho atual do cache de log configurado:

```
iSH> log cache max 200
Maximum number of log messages that can be saved: 200
```

O exemplo a seguir procura pela linha *Major* no cache de logs:

```
iSH> log cache grep Major
Searching for: "Major"
[1]: FEB 07 11:18:42: alert:1/1/1025: alarm_mgr: tLineAlarm: 01:01:01 Major D
S1 Down Line 1:1:1:0 (FarEnd Rx LOF)
[2]: FEB 07 11:18:42:alert: 1/1/1025: alarm_mgr: tLineAlarm: 01:01:02 Major D
S1 Down Line 1:1:2:0 (FarEnd Rx LOF)
[3]: FEB 07 11:18:42:alert: 1/1/1025: alarm_mgr: tLineAlarm: 01:01:03 Major D
S1 Down Line 1:1:3:0 (FarEnd Rx LOF)
...
...
```

Visualizar logs persistentes

Use o comando *log display* para visualizar os logs persistentes.

15.2. SNMP

Criação comunidades SNMP e listas de acesso

O perfil *community-profile* especifica o nome da comunidade e um nível de acesso para que o gerenciador SNMP acesse o sistema. Opcionalmente é possível especificar um *community-access-profile* que será utilizado para verificar o endereço IP de origem do gerenciador SNMP. O sistema suporta até 50 listas de acesso diferentes.

São suportados os seguintes níveis de acesso à comunidade:

» **noaccess:** a comunidade não tem acesso.

» **read:** a comunidade somente têm acesso de leitura ao sistema, com exceção das informações em *community-profile* e *community-access-profile*.

» **readandwrite:** a comunidade tem acesso de leitura/escrita ao sistema, com exceção das informações em *community-profile* e *community-access-profile*.

» **admin:** a comunidade tem acesso de leitura e escrita em todo o sistema, incluindo as informações em *community-profile* e *community-access-profile*.

Criação de uma comunidade SNMP

O exemplo a seguir define o nome da comunidade *public* com privilégios de leitura:

```
iSH> new community-profile 1
Please provide the following: [q]uit.
community-name: ------>    {}: public
```

```
permissions: --------->    {read}:
access-table-index: -->    {0}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Criação de listas de acesso a uma comunidade SNMP

O exemplo a seguir define uma comunidade com o nome *private* com privilégios de leitura/escrita e também cria uma lista de acesso para verificar que os gerentes SNMP que tentarem acessar a OLT sejam provenientes dos endereços IP conhecidos 192.168.9.10 e 192.168.11.12:

Primeiro, crie uma lista de acesso para o primeiro endereço IP:

```
iSH> new community-access-profile 2
Please provide the following: [q]uit.
access-table-index: ----->    {0}: 1
ip-address: ------------->    {0.0.0.0}: 192.168.9.10
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Depois, crie uma lista de acesso para o segundo endereço IP com a mesma *access-table-index* (1):

```
iSH> new community-access-profile 3
Please provide the following: [q]uit.
access-table-index: ----->    {0}: 1
ip-address: ------------->    {0.0.0.0}: 192.168.11.12
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Finalmente, crie a comunidade SNMP utilizando o perfil *community-profile* especificando o nome da comunidade e utilize a lista de controle de acesso de índice 1 conforme foi configurado no perfil *community-access-profiles:*

```
iSH> new community-profile 4
Please provide the following: [q]uit.
community-name: -------->    {}: private
permissions: ------------>    {read}: readandwrite
access-table-index: ---->    {0}: 1
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Configuração de traps SNMP

O perfil *trap-destination* define um destinatário (receptor) das mensagens trap enviadas pela OLT 8820 G. Para configurar um destinatário das mensagens trap deve ser de conhecimento as seguintes informações:

- Endereço IP utilizado pela gerenciador SNMP.
- Nome da comunidade configurado no gerenciador SNMP para recepção das mensagens trap.

O IP de origem utilizado em todos os traps gerados pela OLT 8820 G é o endereço IP definido no perfil *system 0*. O exemplo a seguir configura um destinatário de trap SNMP com o endereço IP 192.168.3.21:

```
iSH> new trap-destination 32
Please provide the following: [q]uit.
trapdestination: ------->    {0.0.0.0}: 192.168.3.21
communityname: ---------->    {}: public
resendseqno: ------------>    {0}:
ackedseqno: ------------->    {0}:
```

```
traplevel: ------------->    {low}:
traptype: -------------->    {(null)}: 0
trapadminstatus: ------->    {enabled}:
gatewaytrapserveraddr:-->    {36}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

15.3. Estatísticas SNMP

A OLT 8820 G suporta as seguintes estatísticas SNMP:

- **Estatísticas MIB II:**
  - ifHCIn/OutOctets.
  - ifHCIn/OutUCastPkts.
  - ifHCIn/OutMultiCastPkts.
  - ifHCIn/OutBroadCastPkts.
  - ifInDiscards.
  - ifOutDiscards.
  - ifInErrors.
  - ifOutErrors.
  - ifOperStatus.
  - ifLastChange.
- **Estatísticas Ethernet:**
  - Quadro transmitido inibido por uma única colisão
  - Quadro transmitido inibido por várias colisões
  - Quadros recebidos que excedem o tamanho máximo
  - Quadros recebidos que falharam a verificação FCS
- **Estatísticas OLT**
- **Estatísticas ONU**

15.4. Estatísticas de bridge

O comando bridge stats exibe as informações de pacote de todas as bridges configuradas.

```
iSH> bridge stats
Interface                              Received Packets         Transmitted Packets
Name                                UCast   MCast   BCast   UCast   MCast   BCast   Error
1-1-2-901-gponport-998/bridge       --      --      --      0       40      0       0
1-1-2-902-gponport-998/bridge       --      --      --      0       40      0       0
1-1-2-903-gponport-998/bridge       --      --      --      0       40      0       0
1-1-1-732-gponport-998/bridge       --      --      --      0       39      0       0
1-1-9-0-eth-840/bridge              --      --      --      --      --      --      --
5 Bridge Interfaces displayed
```

O comando bridge *stats* interface exibe as informações de pacote para a interface designada.

```
iSH> bridge stats 1-1-9-0-eth-840/bridge
Interface                        Received Packets         Transmitted Packets
Name                          UCast   MCast   BCast   UCast   MCast   BCast   Error
1-1-9-0-eth-840/bridge        --      --      --      --      --      --      --
1 Bridge Interfaces displayed
```

```
iSH> bridge stats 1-1-2-901-gponport-998/bridge
Interface                          Received Packets         Transmitted Packets
Name                            UCast   MCast   BCast   UCast   MCast   BCast   Error
1-1-2-901-gponport-998/bridge   --      --      --      0       44      0       0
1 Bridge Interfaces displayed
```

15.5. Estatísticas aprimoradas da porta Ethernet

Utilize o comando port stats para exibir ou limpar as informações de estatísticas.

port stats <ifName/Type> <intf|rmon|eth|all|clear>

O comando *port stats interface/type intf* exibe as informações de estatísticas mib2 da interface.

```
iSH> port stats 1-1-3-0/eth intf
Interface Name                  1-1-3-0
Operational Status              Up
Received Bytes                  0
Received Packets                0
Received Multicast Packets      0
Received Broadcast Packets      0
Transmitted Bytes               45056
Transmitted Unicast Packets     0
Transmitted Multicast Packets   2
Transmitted Broadcast Packets   702
Received Discards               0
Received Errors                 0
Received Unknown Protocols      0
Transmitted Discards            0
Transmitted Errors              0
Speed Bits per Second           *** n/a ***
Speed Megabits per Second       1000
```

O comando *port stats interface/type rmon* exibe as informações de estatísticas rmon da interface.

```
iSH> port stats 1-1-3-0/eth rmon
Total Dropped Events                    0
Total Dropped Frames                    0
Total Bytes                             45696
Total Packets                           714
Transmitted Oversize Packets            0
Received Oversize Packets               0
Fragments                               0
Jabbers                                 0
Collisions                              0
Transmitted No Errors                   714
Received No Errors                      0
IPMC Bridged Packets                    0
IPMC Routed Packets                     0
Transmitted IPMC Dropped Packets        0
Received IPMC Dropped Packets           0
Total Packets 0 to 64 Bytes71           4
Total Packets 65 to 127 Bytes           0
Total Packets 128 to 255 Bytes          0
Total Packets 256 to 511 Bytes          0
```

```
Total Packets 512 to 1023 Bytes               0
Received Packets 0 to 64 Bytes                0
Received Packets 65 to 127 Bytes              0
Received Packets 128 to 255 Bytes             0
Received Packets 256 to 511 Bytes             0
Received Packets 512 to 1023 Bytes            0
Transmitted Packets 0 to 64 Bytes             714
Transmitted Packets 65 to 127 Bytes           0
Transmitted Packets 128 to 255 Bytes          0
Transmitted Packets 256 to 511 Bytes          0
Transmitted Packets 512 to 1023 Bytes         0
Transmitted Packets 1024 to 1518 Bytes        0
Transmitted Packets 1519 to 2047 Bytes        0
Transmitted Packets 2048 to 4095 Bytes        0
Transmitted Packets 4095 to 9216 Bytes        0
```

O comando *port stats interface/type eth* exibe informações de estatísticas dot3 da interface.

```
iSH> port stats 1-1-3-0/eth eth
Alignment Errors                      0
FCS Errors                            0
Single Collision Frames               0
Multiple Collision Frames             0
SQE Test Errors                       0
Deferred Transmissions                0
Late Collisions                       0
Excessive Collisions                  0
Internal Mac Transmit Errors          0
Carrier Sense Errors                  0
FrameTooLongs                         0
InternalMacReceiveErrors              0
SymbolErrors                          0
DuplexStatus                          Full
```

O comando *port stats interface/type all* exibe todas as informações de estatísticas da inteface.

```
iSH> port stats 1-1-3-0/eth all
******   eth      ******
Alignment Errors                      0
FCS Errors                            0
Single Collision Frames               0
Multiple Collision Frames             0
SQE Test Errors                       0
Deferred Transmissions                0
Late Collisions                       0
Excessive Collisions                  0
Internal Mac Transmit Errors          0
Carrier Sense Errors                  0
FrameTooLongs                         0
InternalMacReceiveErrors              0
SymbolErrors                          0
DuplexStatus                          Full
```

```
******    rmon      ******
Total Dropped Events                    0
Total Dropped Frames                    0
Total Bytes                             47360
Total Packets                           740
Transmitted Oversize Packets            0
Received Oversize Packets               0
Fragments                               0
Jabbers                                 0
Collisions                              0
Transmitted No Errors                   740
Received No Errors                      0
IPMC Bridged Packets                    0
IPMC Routed Packets                     0
Transmitted IPMC Dropped Packets        0
Received IPMC Dropped Packets           0
Total Packets 0 to 64 Bytes             740
Total Packets 65 to 127 Bytes           0
Total Packets 128 to 255 Bytes          0
Total Packets 256 to 511 Bytes          0
Total Packets 512 to 1023 Bytes         0
Total Packets 1024 to 1518 Bytes        0
Total Packets 1519 to 2047 Bytes        0
Total Packets 2048 to 4095 Bytes        0
Total Packets 4095 to 9216 Bytes        0
Received Packets 0 to 64 Bytes          0
Received Packets 65 to 127 Bytes        0
Received Packets 128 to 255 Bytes       0
Received Packets 256 to 511 Bytes       0
Received Packets 512 to 1023 Bytes      0
Transmitted Packets 0 to 64 Bytes       0
Transmitted Packets 65 to 127 Bytes     0
Transmitted Packets 128 to 255 Bytes    0
Transmitted Packets 256 to 511 Bytes    0
Transmitted Packets 512 to 1023 Bytes   0
****** intf ******
Interface Name                          1-1-3-0
Operational Status                      Up
Received Bytes                          0
Received Packets                        0
Received Multicast Packets              0
Received Broadcast Packets              0
Transmitted Bytes                       47360
Transmitted Unicast Packets             0
Transmitted Multicast Packets           2
Transmitted Broadcast Packets           738
Received Discards                       0
Received Errors                         0
Received Unknown Protocols              0
Transmitted Discards                    0
Transmitted Errors                      0
```

```
Speed Bits per Second                *** n/a ***
Speed Megabits per Second            1000
```

O comando *port stats clear interface/type* limpa todas as contagens de estatísticas da interface.

```
iSH> port stats clear 1-1-3-0/eth
INTF Stats cleared
```

A tabela a seguir contém a descrição dos parâmetros exibidos.

Parâmetro	Descrição
eth	
Alignment Errors	Uma contagem de quadros recebidos em uma interface com falha na verificação FCS. A contagem representada por uma instância desse objeto é aumentada quando o status Alignment Error é retornado pelo serviço MAC ao LLC (ou a outro assinante MAC). Quadros recebidos para os quais condições de erro múltiplas são contadas exclusivamente de acordo com o status de erro apresentado ao LLC, de acordo com as convenções de Gerenciamento de Camada IEEE 802.3. Essa contagem não aumenta para esquemas de codificação em grupo de 8 bit. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
FCS Errors	Uma contagem de quadros recebidos em uma interface com falha na verificação FCS. Essa contagem não inclui quadros recebidos com o erro frame-too-long ou frame-too-short. A contagem representada por uma instância desse objeto é aumentada quando o status frameCheckError é retornado pelo serviço MAC ao LLC (ou a outro assinante MAC). Quadros recebidos para os quais condições de erro múltiplas são contadas exclusivamente de acordo com o status de erro apresentado ao LLC, de acordo com as convenções de Gerenciamento de Camada IEEE 802.3. Observação: erros de codificação detectados pela camada física para velocidades acima de 10 Mb/s provocarão a falha do quadro na verificação FCS. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Single Collision Frames	Uma contagem de quadros transmitidos com sucesso em uma interface para a qual a transmissão foi bloqueada por causa de uma única colisão. Um quadro contado por instância nesse objeto também é contado pela instância correspondente de ifOutUcastPkts, ifOutMulticastPkts ou ifOutBroadcastPkts, e não é contado pela instância correspondente do objeto dot3StatsMultipleCollisionFrames. Essa contagem não aumenta quando a interface está operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer no reinício do sistema de gerenciamento ou em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Multiple Collision Frames	Uma contagem de quadros transmitidos com sucesso em uma interface para a qual a transmissão foi bloqueada por causa de mais de uma colisão. Um quadro contado por instância nesse objeto também é contado pela instância correspondente de ifOutUcastPkts, ifOutMulticastPkts ou ifOutBroadcastPkts, e não é contado pela instância correspondente do objeto dot3StatsSingleCollisionFrames. Essa contagem não aumenta quando a interface está operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
SQE Test Errors	A contagem de vezes em que a mensagem SQE TEST ERROR foi gerada pela sub-camada PLS para uma interface. SQE TEST ERROR é determinada de acordo com as normas de verificação do mecanismo de detecção SQE na Função PLS Carrier Sense, como descrito no padrão IEEE 802.3, Edição de 1998, seção 7.2.4.6. Essa contagem não aumenta em interfaces operando com velocidades superiores a 10 Mb/s ou em interfaces operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Deferred Transmissions	Uma contagem de quadros para os quais a primeira tentativa de transmissão em uma interface foi atrasada porque o meio está ocupado. A contagem representada por uma instância desse objeto não inclui quadros envolvidos em colisões. Essa contagem não aumenta quando a interface está operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Late Collisions	O número de vezes que uma colisão é detectada em uma interface após um slotTime na transmissão de um pacote. Uma colisão (atrasada) incluída em uma contagem representada por uma instância desse objeto também é considerada como uma colisão (genérica) para o objetivo de outras estatísticas relacionadas a colisões. Essa contagem não aumenta quando a interface está operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer no reinício do sistema de gerenciamento ou em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Excessive Collisions	Uma contagem de quadros para os quais a transmissão em uma interface falha devido a colisões em excesso. Essa contagem não aumenta quando a interface está operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.

Internal Mac Transmit Errors	Uma contagem de quadros para os quais a transmissão em uma interface falha devido a um erro de transmissão na sub-camada MAC interno. Um quadro somente é contado pela instância desse objeto se não é contado pela instância correspondente do objeto dot3StatsLateCollisions, dot3StatsExcessiveCollisions ou dot3StatsCarrierSenseErrors. O significado preciso da contagem representada pela instância desse objeto é específico da implementação. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Carrier Sense Errors	O número de vezes que a condição carrier sense foi perdida ou não foi apontada durante a tentativa de transmissão de um quadro em uma interface. A contagem representada pela instância desse objeto é aumentada pelo menos uma vez por tentativa de transmissão, mesmo se a condição carrier sense sofre oscilação durante a tentativa de transmissão. Essa contagem não aumenta quando a interface está operando em modo full-duplex. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
FrameTooLongs	Uma contagem de quadros recebidos em uma interface que excedem o tamanho máximo permitido de quadro. A contagem representada por uma instância desse objeto é aumentada quando o status frameTooLong é retornado pelo serviço MAC ao LLC (ou a outro assinante MAC). Quadros recebidos para os quais condições de erro múltiplas são contadas exclusivamente de acordo com o status de erro apresentado ao LLC, de acordo com as convenções de Gerenciamento de Camada IEEE 802.3. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
InternalMacReceive Errors	Uma contagem de quadros para os quais a transmissão em uma interface falha devido a um erro de recepção na sub-camada MAC interno. Um quadro somente é contado pela instância desse objeto se não é contado pela instância correspondente do objeto dot3StatsFrameTooLongs, dot3StatsAlignmentErrors ou dot3StatsFCSErrors. O significado preciso da contagem representada pela instância desse objeto é específico da implementação. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
SymbolErrors	Para uma interface operando a 100 Mb/s, o número de vezes que houve um símbolo de dado inválido quando um transportador válido estava presente. Para uma interface operando em modo half-duplex a 1000 Mb/s, o número de vezes que o meio de recepção não está inativo (um evento carrier) por um período de tempo igual ou maior do que slotTime, e durante o qual houve pelo menos uma ocorrência de um evento que provocou que o PHY indicasse 'Data reception error' ou 'carrier extend error' no GMII. Para uma interface operando em modo full-duplex a 1000 Mb/s, o número de vezes que o meio de recepção não está inativo (um evento carrier) por um período de tempo igual ou maior do que minFrameSize, e durante o qual houve pelo menos uma ocorrência de um evento que provocou que o PHY indicasse 'Data reception error' no GMII. A contagem representada pela instância desse objeto é aumentada pelo menos uma vez por evento carrier, mesmo se ocorrem erros de símbolo múltiplos durante o evento carrier. Essa contagem não aumenta se há uma colisão presente. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
DuplexStatus	O modo atual de operação da entidade MAC. 'unknown' indica que o modo duplex atual não pôde ser determinado. O controle de gerenciamento do modo duplex é feito através de MAU MIB. Quando uma interface não suporta negociação automática ou quando a negociação automática está desativada, o modo duplex é controlado utilizando ifMauDefaultType. Quando a negociação automática é suportada e está ativa, o modo duplex é controlado utilizando ifMauAutoNegAdvertisedBits. Em qualquer caso, o modo duplex atualmente ativo é refletido nesse objeto e em ifMauType. Perceba que esse objeto fornece informações redundantes com ifMauType. Normalmente, objetos redundantes não são recomendados. No entanto, nessa instância, isso possibilita que uma aplicação de gerenciamento determine o status duplex da interface sem ter de conhecer cada valor possível de ifMauType. Isso foi considerado útil o suficiente para justificar a redundância. Valores: unknown, halfDuplex, fullDuplex
rmon	Remote Network Monitoring.
Total Dropped Events	O número total de eventos nos quais pacotes foram perdidos pela sonda devido à falta de recursos. Perceba que esse número não é necessariamente o número de pacotes perdidos; é somente o número de vezes que essa condição foi detectada.
Total Dropped Frames	O número total de quadros que foram recebidos pela sonda e portanto não são contados em EtherStatsDropEvents, mas que a sonda decidiu não incluir na contagem por qualquer motivo. Normalmente, esse evento ocorre quando a sonda não possui alguns recursos e decide diminuir a carga dessa coleta. Essa contagem não inclui pacotes que não foram contados porque possuíam erros de camada MAC. Perceba que, diferente da contagem dropEvents, esse número é o número exato de pacotes perdidos.

Total Bytes	O número total de octetos de dados (incluindo aqueles pacotes com erro) transmitidos e recebidos na rede. Esse objeto pode ser utilizado como estimativa razoável para uso de ethernet 10 Mega bits. Se deseja maior precisão, os objetos EtherStatsPkts e EtherStatsOctets devem ser amostrados antes e depois de um intervalo comum. As diferenças nos valores amostrados são Pkts e Octets respectivamente, e o número de segundos no intervalo é Interval. Esse valores são utilizados para calcular a utilização como segue: Pkts * (9.6 + 6.4) + (Octets *.8) Utilization = ---------- Interval * 10,000 O resultado dessa equação é o valor de utilização, que é a percentagem de uso do segmento ethernet com um valor de 0 a 100%.
Total Packets	O número total de pacotes (incluindo pacotes com erros, pacotes broadcast e pacotes multicast) transmitidos e recebidos.
Transmitted Packets	O número total de pacotes (incluindo pacotes com erros, pacotes broadcast e pacotes multicast) transmitidos.
Received Packets	O número total de pacotes (incluindo pacotes com erros, pacotes broadcast e pacotes multicast) recebidos.
Transmitted Multicast Bytes	Bytes Multicast transmitidos.
Received Multicast Bytes	Bytes Multicast recebidos.
Received Multicast Dropped Bytes	Bytes Multicast perdidos.
Transmitted Average Throughput	Taxa de transferência média de transmissão em bits por segundo desde a última solicitação. Para efeitos de precisão, recomenda-se que esse objeto seja solicitado em intervalos de cinco (5) segundos ou mais.
Received Average Throughput	Taxa de transferência média de recepção em bits por segundo desde a última solicitação. Para efeitos de precisão, recomenda-se que esse objeto seja solicitado em intervalos de cinco (5) segundos ou mais.
Transmitted Bandwidth Occupancy	Porcentagem de largura de banda em uso no momento para a transmissão de tráfego. Essa taxa é calculada com base em delta entre a solicitação atual e anterior desse objeto. Para efeitos de precisão, recomenda-se que esse objeto seja solicitado em intervalos de cinco (5) segundos ou mais.
Received Bandwidth Occupancy	Porcentagem de largura de banda em uso no momento para a recepção de tráfego. Essa taxa é calculada com base em delta entre a solicitação atual e anterior desse objeto. Para efeitos de precisão, recomenda-se que esse objeto seja solicitado em intervalos de cinco (5) segundos ou mais.
Total Broadcast Packets	O número total de pacotes sem erros transmitidos e recebidos que foram direcionados ao endereço broadcast. Perceba que isso não inclui pacotes multicast.
Total Multicast Packets	O número total de pacotes sem erros transmitidos e recebidos que foram direcionados ao endereço multicast. Perceba que esse número não inclui pacotes direcionados ao endereço broadcast.
CRC Align Errors	O número total de pacotes recebidos com tamanho (excluindo bits de enquadramento, mas incluindo octetos FCS) entre 64 e 1518 octetos, inclusive, com falha de Frame Check Sequence (FCS) e número inteiro de octetos (FCS Error) ou FCS sem número inteiro de octetos (Alignment Error).
Undersize Packets	O número total de pacotes recebidos com menos de 64 octetos de comprimento (excluindo bits de enquadramento, mas incluindo octetos FCS) e que exceto por esse fato foram bem formado.
Oversize Packets	O número total de pacotes transmitidos e recebidos com mais de 1518 octetos de comprimento (excluindo bits de enquadramento, mas incluindo octetos FCS) e que exceto por esse fato foram bem formado.
Transmitted Oversize Packets	O número total de pacotes transmitidos com mais de 1518 octetos de comprimento (excluindo bits de enquadramento, mas incluindo octetos FCS) e que exceto por esse fato foram bem formado.
Received Oversize Packets	O número total de pacotes recebidos com mais de 1518 octetos de comprimento (excluindo bits de enquadramento, mas incluindo octetos FCS) e que exceto por esse fato foram bem formado.
Fragments	O número total de pacotes recebidos com tamanho inferior a 64 octetos de comprimento (excluindo bits de enquadramento, mas incluindo octetos FCS) com falha de Frame Check Sequence (FCS) e número inteiro de octetos (FCS Error) ou FCS sem número inteiro de octetos (Alignment Error).
Jabbers	O número total de pacotes recebidos com tamanho superior a 1518 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS) com falha de Frame Check Sequence (FCS) e número inteiro de octetos (FCS Error) ou FCS sem número inteiro de octetos (Alignment Error). Perceba que essa definição de jabber é diferente da definição do IEEE-802.3 na seção 8.2.1.5 (10BASE5) e na seção 10.3.1.4 (10BASE2). Esses documentos definem jabber como a condição onde qualquer pacote excede 20 ms. A faixa permitida para detecção de jabber é entre 20 e 150 ms.
Collisions	A melhor estimativa do número total de colisões nesse segmento Ethernet. O valor retornado dependerá da localização da sonda RMON. As Seções 8.2.1.3 (10BASE-5) e 10.3.1.3 (10BASE-2) do padrão IEEE 802.3 definem que uma estação deve detectar uma colisão, no modo de recepção, se três ou mais estações estão transmitindo ao mesmo tempo. Uma porta com repetição deve detectar uma colisão quando duas ou mais estações estiverem transmitindo simultaneamente. Portanto, uma sonda colocada em uma porta de repetição poderia gravar mais colisões que uma sonda conectada a uma estação no mesmo segmento. A localização da sonda tem uma importância muito menor ao considerar que 10BASE-T. 14.2.1.4 (10BASE-T) do padrão IEEE 802.3 define uma colisão como a presença simultânea de sinais nos circuitos DO e RD (transmitindo e recebendo ao mesmo tempo). Uma estação 10BASE-T somente pode detectar colisões quando está transmitindo. Portanto, sondas colocadas em uma estação e em um repetidor devem relatar o mesmo número de colisões. Perceba também que uma sonda RMON dentro de um repetidor deve relatar colisões entre o repetidor e um ou mais hosts (colisões de transmissões como definido por IEEE.802.3k) além das colisões de recepção observadas em qualquer segmento ao qual o repetidor estiver conectado.

Transmitted No Errors	O número total de pacotes TX transmitidos sem erro.
Received No Errors	O número total de pacotes RX recebidos sem erro.
IPMC Bridged Packets	Contagem de Pacotes Broadcom IPMC Bridged.
IPMC Routed Packets	Contagem de Pacotes Broadcom IPMC Routed.
Transmitted IPMC Dropped Packets	Contagem de Pacotes Broadcom IPMC Tx perdidos.
Received IPMC Dropped Packets	Contagem de Pacotes Broadcom IPMC Rx perdidos.
Total Packets 0 to 64 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com 64 octetos de comprimento (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 65 to 127 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 65 e 127 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 128 to 255 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 128 e 255 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 256 to 511 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 256 e 511 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 512 to 1023 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 512 e 1023 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 1024 to 1518 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 1024 e 1518 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 1519 to 2047 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 1519 e 2047 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 2048 to 4095 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 2048 e 4095 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Total Packets 4095 to 9216 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos e recebidos com comprimento entre 4095 e 9216 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 0 to 64 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 0 e 64 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 65 to 127 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 65 e 127 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 128 to 255 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 128 e 255 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 256 to 511 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 256 e 511 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 512 to 1023 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 512 e 1023 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 1024 to 1518 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 1024 e 1518 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 1519 to 2047 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 1519 e 2047 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 2048 to 4095 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 2048 e 4095 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Received Packets 4095 to 9216 Bytes	O número total de pacotes (incluindo pacotes com erros) recebidos com comprimento entre 4095 e 9216 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 0 to 64 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 0 e 64 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 65 to 127 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 65 e 127 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 128 to 255 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 128 e 255 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 256 to 511 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 256 e 511 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).

Transmitted Packets 512 to 1023 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 512 e 1023 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 1024 to 1518 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 1024 e 1518 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 1519 to 2047 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 1519 e 2047 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 2048 to 4095 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 2048 e 4095 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
Transmitted Packets 4095 to 9216 Bytes	O número total de pacotes (incluindo pacotes com erros) transmitidos com comprimento entre 4095 e 9216 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS).
intf	Interface statistics.
Interface Name	O nome textual da interface. O valor desse objeto deve ser o nome da interface como atribuído pelo dispositivo local, e deve ser adequado para a utilização em comandos inseridos no 'console' do dispositivo. Pode ser um nome de texto, como 'le0' ou um número de porta, como '1', dependendo da sintaxe de nomenclatura de interface do dispositivo. Se vários registros juntos em ifTable representam uma só interface como foi nomeada pelo dispositivo, então cada um terá o mesmo valor de ifName. Perceba que, para um agente que responda a solicitações SNMP relativas a uma interface em outro dispositivo (aproximado), o valor de ifName para tal interface é o nome local do dispositivo aproximado atribuído a ela. Se não houver nome local, ou se esse objeto não for aplicável, então esse objeto possui uma linha com comprimento zero.
Operational Status	O status operacional atual da interface. O status testing(3) indica que nenhum pacote operacional pode ser transmitido. Se ifAdminStatus está down(2), então ifOperStatus também deve estar down(2). Se ifAdminStatus é colocado em up(1), então ifOperStatus deve mudar para up(1) se a interface está pronta para transmitir e receber tráfego de rede; deve mudar para dormant(5) se a interface aguarda ações externas (como uma linha serial aguardando uma conexão de entrada); deve permanecer down(2) se e somente se há uma falha que evite a colocação no status up(1); deve permanecer como notPresent(6) se a interface possui componentes faltantes (normalmente hardware). Valores: up, down, testing, unknown, dormant, notPResent, lowerLayerDown
Received Bytes	O número total de octetos recebidos na interface, incluindo caracteres de enquadramento. Esse objeto é uma versão de 64 bits de ifInOctets. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Received Multicast Packets	O número de pacotes multicast recebidos na interface, incluindo endereços de Grupo. Esse objeto é uma versão de 64 bits de ifInMulticastPkts. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Received Broadcast Packets	O número de pacotes broadcast recebidos na interface. Esse objeto é uma versão de 64 bits de ifInBroadcastPkts. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Transmitted Bytes	O número total de octetos transmitidos pela interface, incluindo caracteres de enquadramento. Esse objeto é uma versão de 64 bits de ifOutOctets. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Transmitted Unicast Packets	O número total de pacotes unicast transmitidos. Esse objeto é uma versão de 64 bits de ifOutUcastPkts. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Transmitted Multicast Packets	O número total de pacotes multicast transmitidos, incluindo endereços de Grupos. Esse objeto é uma versão de 64 bits de ifOutMulticastPkts. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Transmitted Broadcast Packets	O número total de pacotes broadcast transmitidos. Esse objeto é uma versão de 64 bits de ifOutMulticastPkts. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Received Discards	O número de pacotes recebidos que foram escolhidos para descarte, mesmo sem apresentar erro. Um possível motivo para descarte de tais pacotes poderia ser liberação de espaço no buffer. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Received Errors	O número de pacotes recebidos com erro. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.

Received Unknown Protocols	O número de pacotes recebidos que foram descartados devido a um protocolo desconhecido ou não suportado pela interface. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Transmitted Discards	O número de pacotes de saída escolhidos para descarte, mesmo sem apresentar erro que impossibilitasse a sua transmissão. Um possível motivo para descarte de tais pacotes poderia ser liberação de espaço no buffer. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Transmitted Errors	O número de pacotes de saída com erro que não puderam ser transmitidos. Descontinuidades no valor dessa contagem podem ocorrer durante o reinício do sistema de gerenciamento e em outros momentos, como indicado pelo valor de ifCounterDiscontinuityTime.
Speed Bits per Second	Uma estimativa da largura de banda atual da interface em bits por segundo. Para interfaces com largura de banda fixa ou aquelas onde não é possível fazer uma estimativa precisa, esse objeto deve conter a largura de banda nominal. Se a largura de banda da interface é superior ao valor máximo relatável por esse objeto, então esse objeto deverá relatar o valor máximo (4.294.967.295) e ifHighSpeed deve ser utilizado para relatar a velocidade da interface. Para uma sub-camada sem conceito de largura de banda, esse objeto deve ter valor zero.
Speed Megabits per Second	Uma estimativa da largura de banda atual da interface em unidades de 1.000.000 bits por segundo. Para interfaces com largura de banda fixa ou aquelas onde não é possível fazer uma estimativa precisa, esse objeto deve conter a largura de banda nominal. Para uma sub-camada sem conceito de largura de banda, esse objeto deve ter valor zero.

Estatísticas aprimoradas da porta Ethernet da OLT 8820 G

15.6. Estatísticas PON

As estatísticas PON são as estatísticas da OLT ou ONU coletadas e relatadas pela OLT 8820 G.

As estatísticas de downstream são as estatísticas enviadas pela OLT 8820 G para a ONU, e as estatísticas de upstream são as estatísticas enviadas da ONU para a OLT 8820 G.

Visualização das estatísticas da OLT

A OLT 8820 G pode reportar os seguintes tipos de estatísticas em uma interface OLT (porta PON): estatísticas da camada física GPON (ex. gpon), estatísticas da camada Ethernet (ex. rmon) e estatísticas da camada de interface (ex. intf). As estatísticas da camada física GPON somente estão disponíveis em interfaces OLT (porta PON).

A OLT 8820 G pode reportar os seguintes tipos de estatísticas para as interfaces ONU: estatísticas da camada física da ONU (ex. onu), estatísticas da camada de interface (ex. intf). As estatísticas da camada física da ONU somente estão disponíveis em interfaces ONU.

Colete e exiba estatísticas da OLT e ONU com o comando *port statistics* ao especificar uma interface OLT ou ONU no campo em ifName/Type.

```
Sintaxe: port stats ifName/Type StatsType
```

- **ifName**

  Nome da interface, no formato shelfID-SlotID-OLTID-ONUID.

- **Type**

  Tipo de interface, ex. gponolt, gpononu, eth, linegroup, etc.

  Para exibir as estatísticas da interface OLT ou ONU, deve-se utilizar o tipo de interface como *gponolt* ou *gpononu*.

- **StatsType**

  Tipo de estatísticas. Os tipos possíveis de estatísticas são:

  - **intf**

    Refere-se a estatísticas de interface mib2. intf é o valor padrão, e se não há um tipo de estatística especificado, o sistema exibe as estatísticas intf. é válido para todos os tipos de interface.

  - **rmon**

    Refere-se às estatísticas de monitoramento remoto ethernet. É válido para as interfaces ethernet ou gponolt.

  - **eth**

    Refere-se às estatísticas ethernet dot3.

  - **olt**

    Refere-se às estatísticas de controle de tráfego GPON OLT. É valido somente para interfaces *gponolt*.

» **onu**

Refere-se a estatísticas de erro GPON ONU relatadas pela OLT 8820 G. é válido somente para interfaces *gpononu.*

» **all**

Refere-se a todas as estatísticas relevantes para o tipo de interface.

Visualização das estatísticas da OLT

1. Visualize as interfaces da OLT. Esse passo é opcional;

```
iSH> list if-translate
Processing list of 874
if-translate          1-1-1-0/rs232
if-translate          1-1-1-0/eth
if-translate          1-1-1-0-eth/linegroup
if-translate          1-1-2-0/eth
if-translate          1-1-2-0-eth/linegroup
if-translate          1-1-3-0/eth
if-translate          1-1-3-0-eth/linegroup
if-translate          1-1-4-0/eth
if-translate          1-1-4-0-eth/linegroup
if-translate          1-1-5-0/eth
if-translate          1-1-5-0-eth/linegroup
if-translate          1-1-6-0/eth
if-translate          1-1-6-0-eth/linegroup
if-translate          1-1-7-0/eth
if-translate          1-1-7-0-eth/linegroup
if-translate          1-1-8-0/eth
if-translate          1-1-8-0-eth/linegroup
if-translate          1-1-9-0/eth
if-translate          1-1-9-0-eth/linegroup
if-translate          1-1-6-0/ipobridge
if-translate          ipobridge/linegroup
if-translate          1-1-1-0/gponolt
if-translate          1-1-1-0-gponolt/linegroup
if-translate          1-1-2-0/gponolt
if-translate          1-1-2-0-gponolt/linegroup
if-translate          1-1-3-0/gponolt
if-translate          1-1-3-0-gponolt/linegroup
if-translate          1-1-4-0/gponolt
if-translate          1-1-5-0/gponolt
if-translate          1-1-5-0-gponolt/linegroup
if-translate          1-1-6-0/gponolt
if-translate          1-1-7-0/gponolt
if-translate          1-1-7-0-gponolt/linegroup
if-translate          1-1-8-0/gponolt
if-translate          1-1-8-0-gponolt/linegroup
if-translate          1-1-1-1/gpononu
...
874 entries found.
```

2. Ao especificar o tipo de estatísticas como *all*, as estatísticas rmon, OLT e de interface são exibidas para essa interface OLT (porta PON);

```
iSH> port stats 1-1-3-0/gponolt all
****** rmon ******
Total Dropped Events                                0
Total Dropped Frames                                0
Total Bytes                                         0
Total Packets                                       0
Transmitted Packets                                 0
Received Packets                                    0
Transmitted Multicast Bytes                         0
Received Multicast Bytes                            0
Received Multicast Dropped Bytes                    0
Transmitted Average Throughput                      0
Received Average Throughput                         0
Transmitted Bandwidth Occupancy                     0
Received Bandwidth Occupancy                        0
Total Broadcast Packets                             0
Total Multicast Packets                             0
CRC Align Errors                                    0
Undersize Packets                                   0
Oversize Packets                                    0
Transmitted Oversize Packets                        0
Received Oversize Packets                           0
Fragments                                           0
Jabbers                                             0
Collisions                                          0
Transmitted No Errors                               0
Received No Errors                                  0
IPMC Bridged Packets                                0
IPMC Routed Packets                                 0
Transmitted IPMC Dropped Packets                    0
Received IPMC Dropped Packets                       0
Total Packets 0 to 64 Bytes                         0
Total Packets 65 to 127 Bytes                       0
Total Packets 128 to 255 Bytes                      0
Total Packets 256 to 511 Bytes                      0
Total Packets 512 to 1023 Bytes                     0
Total Packets 1024 to 1518 Bytes                    0
Total Packets 1519 to 2047 Bytes                    0
Total Packets 2048 to 4095 Bytes                    0
Total Packets 4095 to 9216 Bytes                    0
Received Packets 0 to 64 Bytes                      0
Received Packets 65 to 127 Bytes                    0
Received Packets 128 to 255 Bytes                   0
Received Packets 256 to 511 Bytes                   0
Received Packets 512 to 1023 Bytes                  0
Received Packets 1024 to 1518 Bytes                 0
Received Packets 1519 to 2047 Bytes                 0
Received Packets 2048 to 4095 Bytes                 0
Received Packets 4095 to 9216 Bytes                 0
```

```
Transmitted Packets 0 to 64 Bytes                       0
Transmitted Packets 65 to 127 Bytes                     0
Transmitted Packets 128 to 255 Bytes                    0
Transmitted Packets 256 to 511 Bytes                    0
Transmitted Packets 512 to 1023 Bytes                   0
Transmitted Packets 1024 to 1518 Bytes                  0
Transmitted Packets 1519 to 2047 Bytes                  0
Transmitted Packets 2048 to 4095 Bytes                  0
Transmitted Packets 4095 to 9216 Bytes                  0
****** olt ******
Upstream Valid Gem Frames                               0
Upstream Discarded Frames                               0
Upstream Gem Frames                                     0
Upstream Omci Frames                                    0
Upstream Ploam Frames                                   0
Upstream Idle Ploam Frames                              0
Downstream Valid Gem Frames                             0
Downstream Discarded Frames                             0
Downstream Gem Frames                                   0
Downstream Omci Frames                                  0
Downstream Ploam Frames                                 0
Downstream Idle Ploam Frames                            0
Downstream Pon Valid Ethernet Packtes                   0
Downstream Pon Cpu Packets                              0
Downstream Transmitted Bytes                            0
Upstream Pon Valid Packets                              0
Upstream Pon Valid Not Idle Ploams                      0
Upstream Pon Error Ploams                               0
Upstream Pon Invalid Packets                            0
Upstream Dropped Packets                                0
Upstream Dropped Ploams Fifo Full                       0
Downstream TM Valid Packets                             0
Downstream TM Crc Packets                               0
Downstream TM Dropped Cpu Packets                       0
Downstream TM MAC Lookup Miss                           0
Downstream TM Packets Forwarded From Hm To Pon          0
Downstream TM Packets Dropped Gem Pid Not Enabled       0
Downstream TM Q0 Valid Packets                          0
Downstream TM Q0 Dropped Packets                        0
Downstream TM Q1 Valid Packets                          0
Downstream TM Q1 Dropped Packets                        0
Downstream TM Q2 Valid Packets                          0
Downstream TM Q2 Dropped Packets                        0
Downstream TM Q3 Valid Packets                          0
Downstream TM Q3 Dropped Packets                        0
Downstream TM Q4 Valid Packets                          0
Downstream TM Q4 Dropped Packets                        0
Downstream TM Q5 Valid Packets                          0
Downstream TM Q5 Dropped Packets                        0
Downstream TM Q6 Valid Packets                          0
Downstream TM Q6 Dropped Packets                        0
```

```
Downstream TM Q7 Valid Packets                          0
Downstream TM Q7 Dropped Packets                        0
Upstream TM Dropped Cpu Packets                         0
Upstream TM Dropped Packets Crc Error                   0
Upstream TM Dropped Packets Security                    0
****** intf ******
Interface Name                                          1-4-4-0
Operational Status                                      Down
Received Bytes                                          0
Received Packets                                        0
Received Multicast Packets                              0
Received Broadcast Packets                              0
Transmitted Bytes                                       0
Transmitted Unicast Packets                             0
Transmitted Multicast Packets                           0
Transmitted Broadcast Packets                           0
Received Discards                                       0
Received Errors                                         0
Received Unknown Protocols                              0
Transmitted Discards                                    0
Transmitted Errors                                      0
Speed Bits per Second                                   *** n/a ***
Speed Megabits per Second                               2400
```

3. Ao especificar o tipo de estatísticas como *olt*, somente as estatísticas da camada física GPON OLT são exibidas para essa interface OLT (porta PON).

```
iSH> port stats 1-1-3-0/gponolt olt
Upstream Valid Gem Frames                               1390778452
Upstream Discarded Frames                               0
Upstream Gem Frames                                     1390766390
Upstream Omci Frames                                    12062
Upstream Ploam Frames                                   2773259552
Upstream Idle Ploam Frames                              2772149075
Upstream Pon Invalid Packets                            0
Upstream Dropped Packets Inactive Ports                 0
Upstream Dropped Ploams Fifo Full                       0
Downstream TM Valid Packets                             1408605259
Downstream TM Crc Packets                               0
Downstream TM Dropped Cpu Packets                       0
Downstream TM MAC Lookup Miss                           0
Downstream TM Packets Forwarded From Hm To Pon          1005110436
Downstream TM Packets Dropped Gem Pid Not Enabled       3416
Upstream TM Dropped Cpu Packets                         0
Upstream TM Dropped Packets Crc Error                   0
Upstream TM Dropped Packets Security                    0
Upstream TM Learn Failures                              0
Upstream TM Q0 Valid Packets                            1390766390
Upstream TM Q0 Dropped Packets                          0
Upstream TM Q1 Valid Packets                            0
Upstream TM Q1 Dropped Packets                          0
Upstream TM Q2 Valid Packets                            0
Upstream TM Q2 Dropped Packets                          0
```

```
Upstream TM Q3 Valid Packets                    0
Upstream TM Q3 Dropped Packets                  0
Upstream TM Q4 Valid Packets                    0
Upstream TM Q4 Dropped Packets                  0
Upstream TM Q5 Valid Packets                    0
Upstream TM Q5 Dropped Packets                  0
Upstream TM Q6 Valid Packets                    0
Upstream TM Q6 Dropped Packets                  0
Upstream TM Q7 Valid Packets                    0
Upstream TM Q7 Dropped Packets                  0
```

A tabela a seguir define as estatísticas de camada física GPON OLT exibidas no comando *port stats ifName/gponolt*.

Lembre que as estatísticas de downstream são as estatísticas enviadas pela OLT 8820 G para a ONU, e as estatísticas de upstream são as estatísticas enviadas da ONU para a OLT 8820 G.

Atributo	Descrição
Upstream Valid Gem Frames	O número de quadros GEM válidos enviados na direção upstream.
Upstream Discarded Frames	O número total de quadros GEM descartados enviados na direção upstream.
Upstream Gem Frames	O número de quadros GEM enviados na direção upstream.
Upstream Omci Frames	O número de quadros OMCI enviados na direção upstream.
Upstream Ploam Frames	Número total de quadros PLOAM (Operações, Gerenciamento e Manutenção da Camada Física) enviados na direção upstream. Isso inclui: Número total de mensagens PLOAM incluindo PLOAM inativos. Número total de mensagens PLOAM (sem incluir PLOAM inativos). Número total de mensagens PLOAM perdidas devido a erros de Cyclic Redundancy Check (CRC).
Upstream Idle Ploam Frames	O número total de quadros PLOAM inativos enviados na direção upstream.
Downstream Valid Gem Frames	O número total de quadros GEM válidos enviados na direção downstream.
Downstream Discarded Frames	O número de pacotes descartados devido a erros CRC, falhas de busca no MAC, congestionamento, etc.
Downstream Gem Frames	O número total de quadros GEM enviados na direção downstream.
Downstream Omci Frames	O número total de quadros OMCI enviados na direção downstream.
Downstream Ploam Frames	O número total de quadros PLOAM enviados na direção downstream.
Downstream Idle Ploam Frames	O número total de quadros PLOAM inativos enviados na direção downstream.
Downstream Pon Valid Ethernet Packets	O número total de pacotes ethernet válidos enviados na direção downstream.
Downstream Pon Cpu Packets	O número de pacotes downstream gerados pela CPU (MIPS).
Downstream Transmitted Bytes	O número total de bytes enviados na direção downstream.
Upstream Pon Valid Packets	O número total de pacotes PON válidos enviados na direção upstream.
Upstream Pon Valid Not Idle Ploams	O número total de mensagens PLOAM não ociosos enviadas na direção upstream.
Upstream Pon Error Ploams	O número total de mensagens PLOAM com erro PON enviadas na direção upstream.
Upstream Pon Invalid Packets	O número total de pacotes upstream com erros.
Upstream Dropped Packets Inactive Ports	Número total de pacotes de upstream descartados devido à falta de configuração da ID da GEM Port.
Upstream Dropped Ploams Fifo Full	Número total de PLOAM upstream perdidos devido ao buffer FIFO cheio.
Downstream TM Valid Packets	O número total de pacotes válidos enviados na direção downstream.
Downstream TM Crc Packets	O número total de pacotes de downstream perdidos devido a erros CRC.
Downstream TM Dropped Cpu Packets	O número de pacotes de downstream descartados gerados pela CPU (MIPS).
Downstream TM MAC Lookup Miss	O número de eventos de falha na busca MAC de downstream.
Downstream TM Packets Forwarded From Hm To Pon	O número de pacotes de downstream enviados durante a etapa de modificação do cabeçalho ao PON.
Downstream TM Packets Dropped Gem Pid Not Enabled	Número total de pacotes de upstream perdidos devido à configuração incorreta da ID da GEM Port.
Downstream TM QN Valid Packets (N=0 até 7)	O número de pacotes de downstream enviados de acordo com a prioridade de pedido de envio [0 até 7] ao PON. A ordem 0 é a maior prioridade, e a ordem 7 é a menor prioridade. Os pacotes na prioridade mais baixa são entregues primeiro. Quando o link PON está inativo, essa contagem não irá incrementar.

Downstream TM QN Dropped Packets (N=0 até 7)	O número de pacotes de downstream descartados de acordo com a prioridade de pedido de envio [0 até 7] devido a congestionamento. A ordem 0 é a maior prioridade, e a ordem 7 é a menor prioridade. Os pacotes na prioridade mais baixa são entregues primeiro. Quando o link PON está inativo, essa contagem não irá incrementar.
Upstream TM Dropped Cpu Packets	O número de pacotes de upstream descartados pela CPU(MIPS), não enviados para a interface SGMI.
Upstream TM Dropped Packets Crc Error	O número de pacotes de upstream descartados devido a erros CRC.
Upstream TM Dropped Packets Security	Número total de pacotes de upstream descartados devido a que não passaram nas normas de segurança.
Upstream TM Learn Failures	Falhas no endereçamento MAC devido a tráfego de envio na direção upstream atrasado por falta de espaço no buffer FIFO.
Upstream TM QN Valid Packets (N=0 até 7)	O número de pacotes de upstream enviados de acordo com a prioridade de pedido de envio [0 até 7] a OLT 8820 G. A ordem 0 é a maior prioridade, e a ordem 7 é a menor prioridade. Os pacotes na prioridade mais baixa são entregues primeiro. Quando o link PON está inativo, essa contagem não irá incrementar.
Upstream TM QN Dropped Packets (N=0 até 7)	O número de pacotes de upstream descartados de acordo com a prioridade de pedido de envio [0 até 7] devido a congestionamento. A ordem 0 é a maior prioridade, e a ordem 7 é a menor prioridade. Os pacotes na prioridade mais baixa são entregues primeiro. Quando o link PON está inativo, essa contagem não irá incrementar.

Atributos das estatísticas de camada física GPON OLT

Visualização das estatísticas da ONU

Visualização das estatísticas ONU

1. Visualize as interfaces ONU. Esse passo é opcional;

```
iSH> list if-translate
Processing list of 874
if-translate          1-1-1-0/rs232
if-translate          1-1-1-0/eth
if-translate          1-1-1-0-eth/linegroup
if-translate          1-1-2-0/eth
if-translate          1-1-2-0-eth/linegroup
if-translate          1-1-3-0/eth
if-translate          1-1-3-0-eth/linegroup
if-translate          1-1-4-0/eth
if-translate          1-1-4-0-eth/linegroup
if-translate          1-1-5-0/eth
if-translate          1-1-5-0-eth/linegroup
if-translate          1-1-6-0/eth
if-translate          1-1-6-0-eth/linegroup
if-translate          1-1-7-0/eth
if-translate          1-1-7-0-eth/linegroup
if-translate          1-1-8-0/eth
if-translate          1-1-8-0-eth/linegroup
if-translate          1-1-9-0/eth
if-translate          1-1-9-0-eth/linegroup
if-translate          1-1-6-0/ipobridge
if-translate          ipobridge/linegroup
if-translate          1-1-1-0/gponolt
if-translate          1-1-1-0-gponolt/linegroup
if-translate          1-1-2-0/gponolt
if-translate          1-1-2-0-gponolt/linegroup
if-translate          1-1-3-0/gponolt
if-translate          1-1-3-0-gponolt/linegroup
if-translate          1-1-4-0/gponolt
```

```
if-translate          1-1-5-0/gponolt
if-translate          1-1-5-0-gponolt/linegroup
if-translate          1-1-6-0/gponolt
if-translate          1-1-7-0/gponolt
if-translate          1-1-7-0-gponolt/linegroup
if-translate          1-1-8-0/gponolt
if-translate          1-1-8-0-gponolt/linegroup
if-translate          1-1-1-1/gpononu
if-translate          1-1-1-2/gpononu
...
874 entries found.
```

2. Ao especificar o tipo de estatísticas *onu*, somente as estatísticas de camada física da ONU são exibidas para a referida ONU;

```
iSH> port stats 1-1-1-1/gpononu onu
Upstream BIP8 Errors                          0
Upstream FEC Corrected Bytes                  0
Upstream FEC Corrected Code-words             0
Upstream FEC Uncorrectable Code-words         0
Upstream Received Code-words                  0
Upstream Unreceived Bursts                    0
Downstream Remote BIP8 Errors                 0
Upstream Remote BIP8 Errors                   0
Drift Of Window Indications                   0
Message Error Message                         0
```

3. Ao especificar o tipo de estatísticas *all*, somente as estatísticas da ONU estará disponível e será exibida para a referida ONU.

```
iSH> port stats 1-1-1-1/gpononu all
******    onu       ******
Upstream BIP8 Errors                          0
Upstream FEC Corrected Bytes                  0
Upstream FEC Corrected Code-words             0
Upstream FEC Uncorrectable Code-words         0
Upstream Received Code-words                  0
Upstream Unreceived Bursts                    0
Downstream Remote BIP8 Errors                 0
Upstream Remote BIP8 Errors                   0
Drift Of Window Indications                   0
Message Error Message                         0
```

A tabela a seguir define as estatísticas de camada física GPON ONU exibidas no comando *port stats ifName/gpononu*.

Atributo	Descrição
Upstream BIP8 Errors	Número total de erros BIP8 (Bit-Interleaved Parity 8) de upstream por ONU-ID.
Upstream FEC Corrected Bytes	Número total de bytes FEC de upstream corrigidos por ONU-ID.
Upstream FEC Corrected Code-words	Número total de palavras de código FEC de upstream corrigidas por ONU-ID.
Upstream FEC Uncorrectable Code-words	Número total de palavras de código FEC de upstream não corrigidas por ONU-ID.
Upstream Received Code-words	Número total de palavras de código de upstream transmitidas por ONU-ID.
Upstream Unreceived Bursts	Número total de rajadas de upstream não recebidos por ONU-ID.
Downstream Remote BIP8 Errors	Número total de erros remotos BIP8 de downstream por ONU-ID.
Upstream Remote BIP8 Errors	Número total de erros remotos BIP8 de upstream por ONU-ID.
Drift Of Window Indications	O número de vezes que o desvio de janela médio da ONU excede o limiar de desvio.
Message Error Message	O número de mensagen de erro enviadas pela ONU.

Atributos das estatísticas de camada física GPON ONU

15.7. Manutenção do sistema

Alteração das configurações da porta serial

Para alterar as configurações padrão da porta serial da OLT deve-se alterar o perfil *rs232-profile*. Altere esse perfil somente se necessário.

As configurações padrão do perfil da porta serial da OLT 8820 G são as seguintes:

- 9600 bps.
- 8 data bits.
- Sem paridade.
- 1 stop bit.
- Sem controle de fluxo.

> ⚠ **Cuidado:** a porta serial somente suporta velocidades de 9600 e 57600 bps. Não altere a velocidade para um valor não suportado. Ao realizar uma configuração incorreta pode impossibilitar o acesso a porta serial

Alterar o perfil *rs232-profile:*

```
iSH> update rs232-profile 1-1-1-0/rs232
Please provide the following: [q]uit.
rs232PortInSpeed: ------------->     {9600}: 57600
rs232PortautSpeed: ------------>     {9600}: 57600
rs232PortInFlowType: ---------->     {none}:
rs232PortautFlowType: -------->      {none}:
rs232AsyncPortBits: ----------->     {8}:
rs232AsyncPortStopBits: ------>      {one}:
rs232AsyncPortParity: --------->     {none}:
rs232AsyncPortAutobaud: ---->        {disabled}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
Record created.
```

Essas configurações serão aplicadas após o perfil ser gravado.

> ☑ **Observação:** se o perfil *rs232-profile* for removido, a velocidade da porta será determinada com o último valor configurado

Redefinindo o nome das interfaces

A OLT 8820 G suporta a personalização (até 32 caracteres) do nome das interfaces. A interface com o nome customizado é exibida nos comandos de estatísticas e em outras saída de comandos que exibem o nome da interface.

Para customizar um nome de interface, modifique o parâmetro *ifName* do perfil de configuração *if-translate*.

```
iSH> update if-translate 1-1-1-0/gponolt
if-translate       1-1-1-0/gponolt
Please provide the following:[q]uit.
ifIndex: ---------------->     {23}:
shelf: ------------------>     {1}:
slot: -------------------->     {1}:
port: -------------------->     {1}:
subport: ----------------->     {0}:
type: -------------------->     {other}:
adminstatus: ------------>     {up}:
physical-flag: ---------->     {true}:
iftype-extension: ------->     {gponolt:
ifName: ----------------->     {1-1-1-0}:[novo nome da interface com até 32 caracteres]
```

```
redundancy-param1: ----->     {0}:
description-index: ----->     (0):    **ready-only**
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Ativando ou desativando interfaces da OLT 8820 G

As interfaces físicas da OLT 8820 G estão associadas ao perfil *if-translate* e podem ser ativadas ou desativadas conforme necessidade. Para alterar o estados operacional de uma interface pode-se modificar o parâmetro *adminstatus* do perfil *if-translate* associada a interface ou utilizar o comando *port up | down | bounce ifIndex/type.*

Por exemplo, para desativar uma interface GPON da OLT 8820 G através do perfil if-translate:

```
iSH> update if-translate 1-1-1-0/gponolt
if-translate       1-1-1-0/gponolt
Please provide the following: [q]uit.
ifIndex: ---------------->   {23}:
shelf: ------------------>   {1}:
slot: -------------------->   {1}:
port: -------------------->   {1}:
subport: ----------------->   {0}:
type: --------------------->   {other}:
adminstatus: ------------>   {up}:down
physical-flag: ----------->   {true}:
iftype-extension: ------>   {gponolt}:
ifName: ------------------>   {1-1-1-0}:
redundancy-param1: ----->   {0}:
description-index: ----->   {0}:     ** read-only **
.....................
Save changes? [s]ave, [c]hange or [q]uit:s
```

Ou utilizar o comando *port down:*

```
iSH> port down 1-1-1-0/gponolt
```

Salvar e restaurar as configurações da OLT 8820 G

Os comandos *dump* e *restore* possibilitam salvar e restaurar a configuração da OLT. É possível salvar a configuração no console, localmente e em um arquivo na rede.

O comando utiliza a seguinte sintaxe:

```
dump [console] [network host filename]
```

As senhas são criptografadas quando são salvas no arquivo de configuração. As senhas criptografadas são utlizadas para restaurar a senha correta, mas não podem ser utilizadas para realização do login.

☑	**Observação:** os comandos *dump* e *restore* utilizam TFTP para a transferencia dos arquivos para a rede. Defina para 5 segundos o intervalo de tempo para o encerramento da sessão do servidor TFTP e pelo menos 5 tentativas para a recuperação da conexão
☑	**Observação:** os comandos *dump* e *restore* utilizam *Secure FTP (SFTP)* quando o parâmetro *secure* é habilitado no perfil *system 0*

Para salvar a configuração em um console

1. Configure o software de emulação de terminal conforme informações a seguir:
   - » 9600 bps.
   - » 8 bits de dado.
   - » Sem paridade.

» 1 bit de parada.
» Sem controle de fluxo.
» VT100.

2. Ative a função de captura de seu software de emulação de terminal;
3. Salve as configurações, insira o comando a seguir, porém não pressione o ENTER:

```
iSH> dump console
```

4. Inicie a função de captura em seu software de emulação de terminal, insira um nome para o arquivo (utilize uma extensão *.txt*);
5. Pressione a tecla *Enter;*

O arquivo de configuração será exibido na tela.

6. Quando o arquivo de configuração estiver pronto, pare a função de captura.

Para salvar a configuração localmente

1. Para criar um arquivo de backup e deixar armazenado localmente para uma futura exportação, insira o comando a seguir. Neste comando estaremos atribuindo como device.cfg o nome do arquivo de backup.

```
iSH> dump file device.cfg
```

Para salvar a configuração através da rede

1. Crie o arquivo de backup (com permissão de leitura e escrita) no local de destino do servidor TFTP;
2. Utilize o comando a seguir para salvar as configurações da OLT. Este exemplo assume que o arquivo de backup será chamado de device.cfg e o endereço IP do servidor TFTP é 192.168.8.21:

```
iSH> dump network 192.168.8.21 device.cfg
```

Restaurando as configurações

1. Para realizar a restauração das configurações da OLT é necessário colocar o arquivo de backup (criado previamente) dentro da pasta */card1/onreboot* utilizando o comando file download. *Sintaxe: file download <tftp_host> <tftp_file_path> <dest_path>;*
2. Deve-se renomear o arquivo de backup para restore, sem extensão;

```
iSH> file download 192.168.10.110 device.cfg /card1/onreboot/restore
```

3. Após o download do arquivo, fazer o reboot do sistema.

```
iSH> systemreboot
```

Configuração SNTP

Para configurar o sistema para utilizar servidors SNTP para a sincronização de relógio, deve modificar o perfil *ntp-client-config* e configurá-lo com as informações do servidor NTP desejado.

```
iSH> update ntp-client-config 0
Please provide the following: [q]uit.
primary-ntp-server-ip-address: --------->     {0.0.0.0}: 192.168.8.100
secondary-ntp-server-ip-address: ------->     {0.0.0.0}:
local-timezone: ------------------------>     {gmt}:brasilia
daylight-savings-time: ----------------->     {false}:
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Configurando data/hora de início e término do horário de verão

Para definir a data/hora de início e o término do horário de verão, modifique os parâmetros *daylight-savings-time-start e daylight-savings-time-end do perfil ntp-client-config*. Utilize o formato MM:DD:HH:MM (mês:dia:hora:minuto).

Por exemplo, atualize o *perfil ntp-client-config* conforme exibido a seguir.

» **Configurando horário de verão**

Este exemplo exibe como atualizar o perfil *update ntp-client-config 0* para definir o período de horário de verão para começar em 10 de março às 14h e terminar em 3 de novembro às 2h00.

Insira o comando *update ntp-client-config 0*.

```
iSH> update ntp-client-config 0

ntp-client-config   0
Please provide the following: [q]uit.
primary-ntp-server-ip-address: ------>     {172.16.1.53}:
secondary-ntp-server-ip-address: ---->     {0.0.0.0}:
local-timezone: ---------------------->     {pacific}:
daylight-savings-time: -------------->     {true}:
daylight-savings-time-start: -------->     {03:10:14:00}:
daylight-savings-time-end: ---------->     {11:03:02:00}:
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

> **Observação:** o parâmetro *primary-ntp-server-ip-address* deve ser diferente de zero para salvar as alterações no perfil *ntp-client-config*

> **Observação:** ao testar esta função, certifique-se de que há no mínimo um período de duas horas entre os horários de início e término do ciclo para a função operar corretamente

Status dos módulos SFP

Se precisar verificar o status de um SFP em uma porta Ethernet ou GPON, utilize o comando *sfp show*. Esse comando também exibe parâmetros dos SFP existentes para diagnóstico.

Para verificar as interfaces ethernet na OLT 8820 G, insira *list ether:*

```
iSH> list ether
ether    1-1-1-0/eth
ether    1-1-2-0/eth
ether    1-1-3-0/eth
ether    1-1-4-0/eth
ether    1-1-5-0/eth
ether    1-1-6-0/eth
ether    1-1-7-0/eth
ether    1-1-8-0/eth
ether    1-1-9-0/eth

9 entries found.
```

Para verificar as interfaces GPON na OLT 8820 G, insira *list gpon-olt-config:*

```
iSH> list gpon-olt-config
gpon-olt-config 1-1-1-0/gponolt
gpon-olt-config 1-1-2-0/gponolt
gpon-olt-config 1-1-3-0/gponolt
gpon-olt-config 1-1-4-0/gponolt
gpon-olt-config 1-1-5-0/gponolt
gpon-olt-config 1-1-6-0/gponolt
gpon-olt-config 1-1-7-0/gponolt
gpon-olt-config 1-1-8-0/gponolt

8 entries found.
```

Para visualizar os parâmetros de uma interface SFP, insira *sfp show interface/type:*

```
iSH> sfp show 1-1-1-0/gponolt
vendorName                                  FUJITSU
vendorOui                                   00-00-0e
vendorPartNumber                            FIM30538
vendorRevisionLevel                         03A
serialNumber                                02329    E36476
manufacturingDateCode                       091223
complianceCode                              unknown value (0x0000)
connectorType                               sc (1)
transceiverType                             sfp (3)
extendedIdentifier                          4
encodingAlgorithm                           nrz (3)
channelLinkLength                           unknown value (0x0000)
channelTransmitterTechnology                unknown value (0x0000)
channelTransmitterMedia                     unknown value (0x0000)
channelSpeed                                unknown value (0x0000)
nineTo125mmFiberLinkLengthkm                20
nineTo125mmFiberLinkLength100m              200
fiftyTo125mmFiberLinkLength10m              0
sixtyTwoDot5To125mmFiberLinkLength10m        0
nominalBitRate                              0
upperBitRateMarginPercentage                0
lowerBitRateMarginPercentage                0
copperLinkLength                            0
```

Para visualizar se há qualquer SFPs presente na OLT 8820 G, insira *sfp show all:*

```
iSH> sfp show all
SFP Data for interface 1-1-1-0/gponolt vendorName       FUJITSU
vendorOui                                               00-00-0e
vendorPartNumber                                        FIM30538
vendorRevisionLevel                                     03A
serialNumber                                            02329    E36476
manufacturingDateCode                                   091223
complianceCode                                          unknown value (0x0000)
connectorType                                           sc (1)
transceiverType                                         sfp (3)
extendedIdentifier                                      4
encodingAlgorithm                                       nrz (3)
channelLinkLength                                       unknown value (0x0000)
channelTransmitterTechnology                            unknown value (0x0000)
channelTransmitterMedia                                 unknown value (0x0000)
channelSpeed                                            unknown value (0x0000)
nineTo125mmFiberLinkLengthKm                            20
nineTo125mmFiberLinkLength100m                          200
fiftyTo125mmFiberLinkLength10m                          0
sixtyTwoDot5To125mmFiberLinkLength10m                    0
nominalBitRate                                          0
upperBitRateMarginPercentage                            0
lowerBitRateMarginPercentage                            0
copperLinkLength                                        0
```

```
SFP Data for interface 1-1-2-0/eth
** No SFP present **

SFP Data for interface 1-1-2-0/gponolt

vendorName                                              FUJITSU
vendorOui                                               00-00-0e
vendorPartNumber                                        FIM30538
vendorRevisionLevel                                     03A
serialNumber                                            02239     E36512
manufacturingDateCode                                   091222
complianceCode                                          unknown value (0x0000)
connectorType                                           sc (1)
transceiverType                                         sfp (3)
extendedIdentifier                                      4
encodingAlgorithm                                       nrz (3)
channelLinkLength                                       unknown value (0x0000)
channelTransmitterTechnology                            unknown value (0x0000)
channelTransmitterMedia                                 unknown value (0x0000)
channelSpeed                                            unknown value (0x0000)
nineTo125mmFiberLinkLengthKm                            20
nineTo125mmFiberLinkLength100m                          200
fiftyTo125mmFiberLinkLength10m                          0
sixtyTwoDot5To125mmFiberLinkLength10m                   0
nominalBitRate                                          0
upperBitRateMarginPercentage                            0
lowerBitRateMarginPercentage                            0
copperLinkLength                                        0

SFP Data for interface 1-1-3-0/eth
** No SFP present **
<SPACE> for next page, <CR> for next line, A for all, Q to quitq
```

Visualizar informações da OLT 8820 G

Os comandos a seguir exibem informações sobre o status do sistema:

Para visualizar o status geral do sistema, utilize o comando *shelfctrl monitor:*

```
iSH> shelfctrl monitor
Shelf                   Status
Uptime                  8 hours, 22 minutes
Temperature Sensor      Celsius(C)              Fahrenheit(F)
Card sensor             35                      95
Temperature reading     normal
Fans                    Status
Fan A                   failure
Fan B                   failure
Fan C                   failure
System Alarm            Status
System                  Critical alarm set
Alarm I/O Board
Alarm Active:           Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes
                        Yes  Yes  Yes  Yes
```

Para visualizar estatísticas gerais do sistema:

```
iSH> shelfctrl stats
Shelf Controller Message Statistics
-----------------------------------
Directory services: 2
Clock: 933
Info: 5
Receive errors: 2
```

Para verificar se o sistema está ativo:

```
iSH> shelfctrl show
Shelf Controller Address: 01:1:12
Shelf Registry Address: 01:1:1045
Lease ID: 0x02070000_00000034
State: active
Slot 1:
   prevState: CONFIGURING currentState: RUNNING
   mode: NONE startTime: 1428462509
```

Para visualizar informações sobre o dispositivo, utilize o comando slots:

```
iSH> slots 1
Type                : MXK 19x
Sub-Type            : MXK 198-10GE - 8 GPON OLT, 8 FE/GE, 2 10GE
Card Version        : 800-03112-01-K
EEPROM Version      : 2
Serial #            : 12185380
CLEI Code           : No CLEI
Card-Profile ID     : 1/1/10500
Shelf               : 1
Slot                : 1
ROM Version         : MX 2.2.1.211
Software Version    : MX 2.5.1.423
State               : RUNNING
Mode                : NONE
Heartbeat check     : enabled
Heartbeat resp      : 0
Heartbeat late      : 0
Hbeat seq error     : 0
Hbeat longest       : 0
Fault reset         : enabled
Power fault mon     : not supported
Uptime              : 7 hours, 49 minutes
```

O comando card stats exibe estatísticas em tempo de execução para a OLT 8820 G.

```
iSH> card stats
       -------------   cpu % utilization   ------------
slot   idle   usage   high   services   framework   low
====   ====   =====   ====   ========   =========   ===
1       89     11      5         5          0        0

------ memory (KB)---------------- Card Memory    uptime
```

```
% Used    Total    Peak    Avail    Status      ddd:hh:mm:ss    s/w version
======    =====    ====    =====    =========   =============   ============

 31.21    223453   69886   153703     1 - OK       0:07:49:58     MX 2.5.1.423
```

A tabela a seguir define os campos do comando *card stats*.

Seção	Campo
CPU % utilization (Utilização % de CPU)	*Slot* Descrição textual da unidade do dispositivo de acesso
	Idle Porcentagem de tempo que a CPU passou executando tarefas com prioridade 200 ou menor. Tarefas com prioridade 200 ou menor (quanto maior o número, menor a prioridade) são consideradas tarefas ociosas
	Usage Porcentagem de tempo que a CPU passou executando tarefas com prioridade de 199 ou maior
	High Porcentagem de tempo que a CPU passou executando tarefas com prioridade 001 a 099. Tarefas de alta prioridade estão principalmente relacionadas ao processamento de pacote e ao monitoramento crítico do sistema
	Services Porcentagem de tempo que a CPU passou executando tarefas com prioridade 100 a 179. Tarefas de serviços são principalmente tarefas de monitoramento do estado e de alarmes
	Framework Porcentagem de tempo que a CPU passou executando tarefas com prioridade 180 a 199. Tarefas de framework são principalmente atividades relacionadas ao sistema de gerenciamento de banco de dados e rede, como config synch e backup
	Low Porcentagem de tempo que a CPU passou executando tarefas com prioridade de 200 a 250
memory (KB)	*Used* Porcentagem de tempo que a CPU passou executando tarefas com prioridade de 199 ou mais
	Total Quantidade total de memória física contida no dispositivo
	Peak Memória física máxima alocada a qualquer momento pelo dispositivo
	Avail Quantidade de memória física não alocada e que não está em uso pelo dispositivo
Card Memory Status	Status da memória enviada com trap. Uma trap é enviada quando cada uma das condição ocorre 1. ramMemOK — Utilização da memória RAM inferior a 90% 2. ramMemLow — Utilização da memória RAM superior a 90% 3. flashMemOK — Memória FLASH suficiente para armazenamento máximo no banco de dados 4. flashMemLow — Memória FLASH insuficiente para armazenamento máximo no banco de dados 5. flashMemOut — Memória FLASH esgotada, os dados não são mais persistentes
uptime ddd:hh:mm:ss	O uptime é calculado como sysUpTime - ifLastChange (presumindo que o dispositivo está funcionando)
s/w version	Versão de software

Campos do comando card stats

Visualização e configuração de data e hora na OLT 8820 G

Visualizando e configurando data e hora na OLT 8820 G

Visualize a hora atual na OLT 8820 G, insira o comando *showdatetime:*

```
iSH> showdatetime

Current Time: TUE FEB 09 09:49:52 2010
```

Configurando data e hora na OLT

Configure a data e hora da OLT.

Pode utilizar o comando *setdatetime* ou utilizar o SNTP (o protocolo de horário da rede) para fornecer o horário a OLT ao invés de configurá-lo manualmente. Por exemplo:

```
iSH> setdatetime < month(mm) day(dd) year(yyyy) hour(hh) minute(mm) second(ss) >
```

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 3 (três) meses de garantia legal mais 21 (vinte e um) 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 gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. 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.
8. Após sua vida útil, o produto deve ser entregue a uma assistência técnica autorizada da Intelbras ou realizar diretamente a destinação final ambientalmente adequada evitando impactos ambientais e a saúde. Caso prefira, a pilha/bateria assim como demais eletrônicos da marca Intelbras sem uso, pode ser descartado em qualquer ponto de coleta da Green Eletron (gestora de resíduos eletroeletrônicos a qual somos associados). Em caso de dúvida sobre o processo de logística reversa, entre em contato conosco pelos telefones (48) 2106-0006 ou 0800 704 2767 (de segunda a sexta-feira das 08 ás 20h e aos sábados das 08 ás 18h) ou através do e-mail suporte@intelbras.com.br.

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

Importado no Brasil 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

01.20
Origem: Estados Unidos