Guia de Configurações de Boas Práticas de Segurança e Outras Recomendações Laserway

Histórico de revisões do documento:

Data	Revisão	Motivo da Revisão
20/01/2025	0	Entrega inicial

Sumário

1 OBJETIVO

A segurança da rede é uma categoria que envolve proteção da infraestrutura da rede e dos dados que por ela trafegam. Para isso, boas práticas de configuração, administração e operação são empregadas para manter as redes protegidas contra possíveis ataques internos ou externos e violações de dados.

Para que a operação e manutenção da rede se torne mais fácil e ágil, bem com a percepção de vulnerabilidades, devem ser observados os requisitos mínimos de segurança e boas práticas a serem aplicados desde o início do projeto.

Este documento trata de um conjunto de configurações e recomendações mínimas a serem aplicadas ao se implantar ou revisar uma rede.

2 CONFIGURAÇÕES DE SEGURANÇA

As configurações a seguir devem ser customizadas por projeto Laserway como forma de melhorar a segurança e monitoramento dos equipamentos GPON.

2.1 Acesso Remoto a OLT

Por questões de segurança, recomenda-se bloquear o acesso telnet ao equipamento e habilitar o serviço de servidor SSH para acesso remoto.

2.1.1 Configuração do servidor de SSH

Modelo G2500	Descrição
configure terminal ssh server enable !	Habilita o ssh server

Modelos LD3008, LW3008C, LD3016, LD3032, 3096	Descrição
configure terminal service ssh	Habilita o ssh server

Modelos 3508/3516	Descrição
configure terminal service ssh enable	Habilita o ssh server

2.1.2 Desabilitar conexões telnet

Modelos 3508/3516	Descrição
configure terminal service telnet disable	Desabilita o serviço telnet

2.1.3 Limite de conexões simultâneas

O equipamento possui um limite padrão de 8 conexões simultâneas. Coloque um número entre 1 e 8, conforme necessidade.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal login connect 5 !	Comandos para restrição de usuários simultâneos (neste caso, 5)

Modelos 3508/3516	Descrição
configure terminal no line vty 5 39 !	Comandos para restrição de usuários simultâneos (neste caso, 5)

2.1.4 Bloqueio de acesso SNMPv2

O protocolo SNMPv2 possui uma série de vulnerabilidades conhecidas sendo recomendada a utilização do protocolo SNMPv3 quando necessário. Para o bloqueio do protocolo SNMPv2, deve-se remover as comunidades padrão de leitura e escrita conforme abaixo:

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal no snmp community ro public no snmp community rw private !	Remoção das comunidades de leitura e escrita, para bloquear o acesso SNMPv2

O protocolo SNMPv3 endereça as questões de segurança através da combinação de autenticação e criptografia de pacotes pela rede.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal snmp user <user> md5 <password> smp group admin v3 <user> snmp access admin v3 auth all all all !	Configuração do SNMPv3

Modelos 3508/3516	Descrição
configure terminal snmp-server users create <user> rw priv <privacy> sha <user_password>	Configuração do SNMPv3

2.2 Controle de acesso remoto a OLT

As funcionalidades Admin Flow e Admin Policy permitem classificar e controlar o acesso ao equipamento tal qual uma lista de acesso administrativa. Recomenda-se a criação de regras para permitir o tráfego SSH e SNMP somente de fontes confiáveis (source IP).

2.2.1 Controle de conexões SSH

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal flow admin SSH_BLOCK create ip any <IP_GERENCIA_OLT> tcp any 22 apply !	Cria uma nova regra de fluxo chamada SSH_BLOCK, e a definição de regra para bloquear qualquer conexão TCP na porta 22 (SSH) de qualquer ip de origem para o ip de gerenciamento da OLT
flow admin SSH_PERMIT create ip <IP_DE_ORIGEM> <IP_GERENCIA_OLT> tcp any 22 apply !	Configura a permissão de acesso SSH
policy admin SSH_BLOCK create include-flow SSH_BLOCK priority medium action match deny apply !	Cria uma nova política de firewall chamada "SSH_BLOCK". Inclui a regra de fluxo "SSH_BLOCK" na política. Define a prioridade da política como média. Especifica que a ação a ser tomada quando a regra for correspondida é negar o tráfego.
policy admin SSH_PERMIT create include-flow SSH_PERMIT priority high action match permit	Cria uma nova política de firewall chamada "SSH_PERMIT". Inclui a regra de fluxo "SSH_PERMIT" na política. Define a prioridade da política como alta. Especifica que a ação a ser tomada quando a regra for correspondida é permitir o tráfego.

apply !	

Modelos 3508 - 3516
Não suporta

2.3 Autenticação de acesso à OLT

2.3.1 Alteração de senha padrão no primeiro login

Recomenda-se alterar a senha padrão dos equipamentos durante o primeiro login de acesso utilizando a configuração de senha forte baseada nos seguintes critérios:

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	
• Mínimo de 10 caracteres, máximo de 16 caracteres (exceto "?"); • Conter ao menos 1 caractere alfabético maiúsculo e 1 minúsculo (A-Z, a-z); • Conter ao menos 1 número (0-9); • Conter ao menos 1 caractere especial; • Não utilizar senha em branco; • Conter ao menos 4 caracteres diferentes da senha atual.	
Comandos	**Descrição**
configure terminal passwd <user> Changing password for <user> Enter the new password (maximum of 16 characters) Please use a combination of upper and lower case letters and numbers.	Inicia o processo de alteração de senha para o usuário especificado. Mensagem indicando que a senha do usuário está sendo alterada. Solicita que você insira a nova senha, com um máximo de 16 caracteres. Recomenda o uso de uma combinação de letras maiúsculas, minúsculas e números para maior segurança. Solicita que você insira a nova senha.

Enter the new password: Re-enter the new password: Password changed. !	Solicita que você insira novamente a nova senha para confirmação. Mensagem confirmando que a senha foi alterada com sucesso.

Modelos 3508/3516	
• Mínimo de 6 caracteres, máximo de 8 caracteres (exceto "?"); • Conter ao menos 1 caractere alfabético maiúsculo e 1 minúsculo (A-Z, a-z); • Conter ao menos 1 número (0-9); • Conter ao menos 1 caractere especial; • Não utilizar senha em branco; • Conter ao menos 4 caracteres diferentes da senha atual.	
Comandos	**Descrição**
configure terminal username admin password ********	Configuração de senha

Observação: Caso seja necessário restaurar o acesso de usuário e senha padrão, o procedimento de recuperação pode ser encontrado nos Manuais dos produtos, e na parte de suporte do site da Furukawa:

https://www.furukawalatam.com/pt-br/recursos/-/Guias

2.3.2 Autenticação centralizada utilizando protocolo AAA

A utilização de base de dados centralizada de usuários para autenticação facilita o gerenciamento e aumenta o nível de segurança de acesso ao equipamento.

O protocolo AAA (Authentication, Authorization, and Accounting) oferece mais vantagens importantes para a segurança e gerenciamento de redes, e será utilizado para logar na OLT.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
Autenticação utilizando servidor RADIUS configure terminal login local radius enable login remote radius enable login local radius primary login remote radius primary login local host auto-enable login remote host auto-enable login radius interface <MGMT_BRXX> login radius server <IP_ADD_1> <KEY> login radius server move <IP_ADD_1> 1 login radius server <IP_ADD_2> <KEY> login radius server move <IP_ADD_2> 2 ! *O privilégio do user é definido no arquivo "users" do radius server. Por exemplo, para user com privilégio admin, utilizar somente o parâmetro cisco-avpair = "shell:priv-lvl=15", e não mencionar Service-Type.*	Ativação da autenticação RADIUS, definição de servidores RADIUS primários, habilita hosts, especificação da interface de gerenciamento para comunicação com os servidores RADIUS
Autenticação utilizando servidor TACACS configure terminal login local tacacs enable login remote tacacs enable login local tacacs primary login remote tacacs primary	

login local host auto-enable login remote host auto-enable login tacacs interface <MGMT_BRXX> login tacacs server <IP_ADD_1> <KEY> login tacacs server move <IP_ADD_1> 1 login tacacs server <IP_ADD_2> <KEY> login tacacs server move <IP_ADD_2> 2 !	Ativação da autenticação TACAS+, definição de servidores TACACS+ primários, habilita hosts, especificação da interface de gerenciamento para comunicação com os servidores TACACS+

Dependendo da disponibilidade de servidor, pode-se utilizar tanto autenticação baseada em servidor RADIUS quanto servidor TACACS.

Observação: A configuração "login local/remote host auto-enable" permite que a tentativa de autenticação com usuário local (e.g. admin) ocorra somente se não existir conexão com o RADIUS SERVER. Caso exista conexão, mas a autenticação falhe (senha ou usuário inválidos), a autenticação local não ocorrerá. Esta configuração é preferida em relação a desabilitar permanentemente a autenticação de usuário local via "login local/remote host disable'.

Modelos 3508, 3516	Descrição
Na OLT é possível e recomendado utilizar as configurações de autenticação, autorização e contabilidade/auditoria no TACACS, conforme abaixo: configure terminal tacacs-server host <IP_ADD> key <KEY> aaa new-model aaa authentication login default group tacacs local aaa authentication login console local aaa authorization login-session default group tacacs local aaa accounting login-session default group tacacs aaa accounting command default group tacacs	Configurações de autenticação, autorização e contabilidade/auditoria no TACACS

! *Obs.: Atualmente a OLT suporta apenas a autenticação em servidor RADIUS, não suportando a autorização e contabilidade/auditoria* Caso seja utilizado servidor RADIUS, a configuração ocorre apenas para a autenticação: configure terminal radius-server host <IP_ADDR> key <KEY> aaa new-model aaa authentication login default group radius local aaa authentication login console local !	Configurações para servidor RADIUS

2.3.3 Bloqueio temporário contra tentativas de acesso não autorizado

Os equipamentos devem ser configurados para bloquear temporariamente tentativas repedidas de autenticação de usuário não autorizadas como forma de mitigação de acesso de força bruta. Recomenda-se a configuração de 3 tentativas com tempo de bloqueio de no mínimo 5 minutos.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal login attempts 3 delay 10 !	Configuração para bloqueio temporário contra tentativas de acesso não sucedidas

Modelos 3508, 3516
Não suportado

2.3.4 Encerramento de sessões inativas (timeout)

Outra forma de mitigação de acessos indevidos é a configuração do encerramento de sessões por tempo de inatividade. Recomenda-se a configuração de 5 minutos.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal exec-timeout 5 !	Configuração de timeout por tempo de inatividade (neste caso, 5 minutos)

Modelos 3508, 3516	Descrição
configure terminal line vty 0 39 exec-timeout 5	Configuração de timeout por tempo de inatividade (neste caso, 5 minutos)

2.4 Controle de acesso das ONUs

Por questões de segurança, cada ONU deve ter sua senha de acesso default alterada seja através da página WEB (para os modelos que possuírem) ou seja pelo CLI da ONU. Também é recomendado, para ONUs configuradas em modo Router – Home Gateway Unit (HGU) – desabilitar o acesso à ONU via interface LAN, mantendo apenas o acesso pela WAN do equipamento.

A alteração de senha da ONU pode sofrer variações entre os modelos. Alguns equipamentos possuem requisitos mais complexos e elaborados para a formação da senha, mas em geral, o requisito mínimo na mudança de senha que deve ser recomendado a ser utilizado é:

- Ter no mínimo 8 caracteres
- Ter pelo menos uma letra maiúscula e uma letra minúscula
- Ter números de 0 a 9
- Ter no mínimo 1 caractere especial

2.5 Bloqueio de LLDP no acesso GPON

O protocolo LLDP não deve ser habilitado nas interfaces GPON; Ele representa uma vulnerabilidade de DoS no equipamento.

2.5.1 Desabilitar o LLDP nas interfaces

Por padrão, esta funcionalidade está desabilitada nas OLTs

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge no lldp <PRIMEIRA_PORTA-ULTIMA_PORTA>	Desabilita LLDP nas interfaces

Modelos LD3032, 3096	Descrição
configure terminal interface gpon <1> lldps disable !	Desabilita LLDP nas interfaces. Neste caso, interface 1

Modelos 3508, 3516	Descrição
configure terminal interface gpon <1> no lldp !	Desabilita LLDP nas interfaces. Neste caso, interface 1

2.6 Syslog interno e externo

Recomenda-se configurar um servidor syslog remoto para backup e centralização das mensagens de rede. O servidor syslog é um sistema que coleta e armazena logs de diferentes dispositivos de rede, como roteadores e switches, em um local central. Isso facilita a análise e correlação das mensagens de log, ajudando na identificação e resolução de problemas.

Além disso, é importante ajustar os níveis de logs. Os níveis de logs determinam a quantidade e o tipo de informações registradas. Customizar esses níveis ajuda a evitar o registro de informações desnecessárias, focando apenas nos dados relevantes para a administração e segurança da rede.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
A função de syslog server é habilitada por default na OLT para permitir a geração de logs locais no sistema. **Configuração de servidor de syslog remoto e níveis locais** configure terminal syslog output info remote <SERVER_IP> syslog output info local volatile syslog output notice local non-volatile	Configuração da saída de logs para um servidor remoto e armazenamento local, tanto volátil quanto não volátil

Modelos 3508 / 3516	Descrição
A configuração do nível de logging é feita por módulos e pode ser alterado de acordo com as opções abaixo **Configuração de níveis de logging por módulos** configure terminal logging level ? all Set logging level for all messages	Configuração de níveis de logging por módulos

auth Set logging level for auth messages cethlen Set logging level for cethlend messages ectp Set logging level for ectpd messages gpon Set logging level for gpon messages hsl Set logging level for hsl messages imi Set logging level for imi messages l2mrib Set logging level for l2mrib messages lagd Set logging level for lagd messages misc Set logging level for misc messages mrib Set logging level for mrib messages mstp Set logging level for mstp messages ndd Set logging level for ndd messages nsm Set logging level for nsm messages onm Set logging level for onm messages ospf Set logging level for ospf messages ospf6 Set logging level for ospf6 messages rib Set logging level for rib messages rip Set logging level for rip messages ripng Set logging level for ripng messages rmon Set logging level for rmon messages vlog Set logging level for vlog messages	
Exemplo de configuração de nível de logging 4 para gpon: configure terminal logging level gpon 4	Configuração de nível de logging 4 para gpon

Observação: Em uma operação normal de rede, recomenda-se que o nível de logging máximo a ser utilizado na OLT seja 4, níveis de logging maiores devem ser utilizados pontualmente em casos de troubleshooting.	
Configuração de servidor de syslog local A função de syslog server local é desabilitada por default na OLT, para permitir a geração de logs locais no sistema é necessário habilitar via configuração. configure terminal logging logfile 4 !	Configuração de servidor de syslog local
Configuração de servidor de syslog remoto configure terminal logging server 4 <server_ip>	Configuração de servidor de syslog remoto

2.7 Descrição de portas e VLANs

A fim de facilitar o gerenciamento da rede, recomenda-se atribuir descrição a interfaces GPON, ethernet, VLANs e agregação de links (LAG) do equipamento OLT.

2.7.1 Configuração da descrição de portas ethernet

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge port description <PORTA_ETH> <HOSTNAME_REMOTO> <PORTA_REMOTA>	Configuração para adicionar descrição de portas ethernet

Modelos LD3032, 3096	Descrição
configure terminal interface tengigabitethernet <0/1> Description <HOSTNAME_REMOTO> !	Configuração para adicionar descrição de portas ethernet. Neste caso, porta 1. Adiciona descrição para a porta

Modelos 3508, 3516	Descrição
configure terminal interface <gpon1> description <DESCRIÇÃO> !	Configuração para adicionar descrição de portas ethernet. Neste caso, interface gpon número 1

2.7.2 Configuração da descrição de portas GPON

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge port description <NUMERO_DA_PORTA> <DESCRIÇÃO>	Configuração da descrição de portas GPON

Modelos LD3032, 3096	Descrição
configure terminal interface gpon <1/1> description <DESCRIÇÃO>	Configuração da descrição de portas GPON. Neste caso, porta 1/1

Modelos 3508 / 3516	Descrição
configure terminal interface <gpon1> description <DESCRIÇÃO> !	Configuração da descrição de portas GPON. Neste caso, interface 1

2.7.3 Configuração da descrição de VLANs

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal bridge vlan description <ID_DA_VLAN> <DESCRIÇÃO_DA_VLAN>	Configuração da descrição de VLANs

Modelos LD3032, 3096	Descrição
configure terminal interface vlan <ID_DA_VLAN> description <DESCRIÇÃO_DA_VLAN> !	Configuração da descrição de VLANs

Modelos LD3032, 3096	Descrição
configure terminal vlan database vlan <ID_DA_VLAN> bridge 1 name <DESCRIÇÃO_DA_VLAN> !	Configuração da descrição de VLANs

2.8 Sincronismo do relógio

As configurações NTP para sincronismo de relógio são importantes para controle e correlação de logs da rede, por isso, é importante que toda a rede do cliente esteja usando a mesma referência de servidor NTP. É recomendado configurar a OLT conforme abaixo:

2.8.1 Configuração do fuso horário (time zone)

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal show time-zone time-zone	Visualização de todos os fusos, e escolha de um deles.

Modelos 3508 / 3516	Descrição
configure terminal clock timezone <TIMEZONE> !	Configuração do fuso horário
É possível navegar pela configuração de timezone, escolhendo continente, país e estado através do commando abaixo: configure terminal clock timezone select	Navegação das opções de timezone

2.8.2 Configuração do servidor NTP

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal ntp <SERVER1_IP>	Configurando servidor NTP. Basta colocar o IP do servidor NTP. Exemplo: SP 200.160.7.186

Modelos 3508 / 3516	Descrição
configure terminal ntp server <SERVER1_IP/HOSTNAME>	Configuração do servidor NTP Basta colocar o IP do servidor NTP. Exemplo: SP 200.160.7.186

3 OUTRAS CONFIGURAÇÕES E BOAS PRÁTICAS DE SEGURANÇA

As recomendações abaixo são consideradas boas práticas de desenho de rede que visam mitigar problemas de segurança, desempenho e escalabilidade das redes de acesso PON.

3.1 Endereços IP de gerência privados

Recomenda-se utilizar endereços IP privados na rede de gerência dos equipamentos OLT e ONUs conforme especificado na RFC 1918. A utilização de endereços IP públicos deve ser evitada uma vez que representa um risco maior aos equipamentos a ataques externos quando não protegidos adequadamente por Firewall.

3.2 Limitação dos domínios de Broadcast

O projeto da rede de acesso GPON deve considerar o correto dimensionamento do domínio de Broadcast dos serviços, segmentando corretamente as VLANs de serviço sempre que possível. O excesso de frames Broadcast na rede de acesso GPON pode interferir no desempenho da rede, podendo também representar um ataque DDoS à CPU de equipamentos em algumas situações. Como exemplo, pode-se sugerir que o serviço de acesso Internet utilize segmentação em diferentes VLANs e redes IP por porta PON do equipamento OLT, limitando, assim, o domínio Broadcast à quantidade de dispositivos conectados às ONUs de cada porta.

Adicionalmente, deve-se evitar habilitar a configuração de bridge entre as portas GPON da OLT sempre que possível. Alguns modelos de OLT suportam a configuração de bridge entre as portas PON por VLAN, 16 permitindo limitar a comunicação direta entre ONUs somente aos serviços em que essa comunicação seja necessária.

3.3 Não utilização da VLAN 1

A VLAN 1 é comumente utilizada nos dispositivos de rede como a VLAN padrão ou nativa de todas as interfaces e tendo, muitas vezes, protocolos de controle como spanning-tree (STP) habilitados por padrão nessa VLAN. O uso da VLAN 1 em ambientes de produção implica em um grande risco de segurança uma vez que inverte a lógica de desenho de rede, em que as configurações são planejadas e aplicadas sob demanda às interfaces, assumindo por padrão todas as interfaces do equipamento como membros dessa VLAN 1 de serviço.

Para realizar alteração da vlan nativa de uma interface:

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge vlan create <VID> vlan <VID> <port> untagged !	Alteração da VLAN nativa de uma interface

Modelos 3032, 3096	Descrição
configure terminal vlan database vlan <VID> interface tengigabitethernet <port> switchport mode trunk switchport trunk allowed vlan add <VID> switchport trunk native vlan <VID> switchport trunk allowed vlan remove 1 !	Alteração da VLAN nativa de uma interface

Modelos 3508 / 3516	Descrição
configure terminal vlan <VID> bridge 1 interface <port>	Alteração da VLAN nativa de uma interface

switchport mode trunk switchport trunk allowed vlan add <VID> switchport trunk native vlan <VID> switchport trunk allowed vlan remove 1 !	

3.4 Storm Control

A funcionalidade Storm Control permite limitar a taxa de pacotes por segundo (pps) Broadcast, multicast e Destination Lookup Failure (DLF) recebidos em uma interface, evitando o congestionamento na rede. Quando o número de pacotes excede a taxa configurada, o sistema descarta a taxa excedente. As taxas abaixo são um exemplo de 17 dimensionamento proporcional à capacidade da interface, mas devem ser dimensionados de acordo com a característica de tráfego esperada de cada projeto/aplicação.

A configuração de storm control para estes modelos de OLT é feita através da configuração de limitação de pacotes por segundo.

Um exemplo de recomendação e configuração:

Interface	BCAST	MCAST	DLF
GPON	100	100	100
ETH 1G	1000	1000	1000
ETH 10G	10000	10000	10000

OLTs Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge storm-control broadcast <RATE> [PORTS]	

storm-control multicast <RATE> [PORTS] storm-control dlf <RATE> [PORTS] !	Configuração de Storm Control

A configuração de storm control para estes modelos de OLT é feita através da configuração de limitação de pacotes por segundo.

Um exemplo de recomendação e configuração:

Interface	BCAST	MCAST	DLF
GPON	1080	2000	2000
ETH 1G	1080	2000	2000
ETH 10G	10000	20000	20000

OLTs Modelos LD3032, 3096	Descrição
configure terminal interface gpon/tengigabitethernet <PORT> storm-control broadcast <RATE> storm-control multicast <RATE> storm-control dlf <RATE>	Configuração de Storm Control

A configuração de storm control para estes modelos de OLT é feita através da configuração de limitação de percentual de tráfego.

Um exemplo de recomendação e configuração:

Interface	BCAST	MCAST	DLF
GPON	1%	1%	1%
ETH 1G	1%	1%	1%
ETH 10G	1%	1%	1%

Modelos 3508 / 3516	Descrição
configure terminal interface x storm-control broadcast level 1 storm-control multicast level 1 storm-control dlf level 1 !	Configuração de Storm Control

3.5 Proteção de CPU (Somente OLTs LD3008, LW3008C, LD3016, G2500, LD3032, 3096)

A funcionalidade para proteção de CPU permite limitar a taxa de pacotes por segundo que são processadas pelo CPU, para que em um eventual flood de pacotes na rede, o CPU da OLT não seja afetado para não ocorrer uma perda de acesso a OLT.

As taxas abaixo são uma recomendação para manter a capacidade de processamento da CPU em valores aceitáveis:

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge cpu-flood-guard enable cpu-flood-guard <PORTAS_GPON> 500 cpu-flood-guard<GPON_PORTS> timer 300 !	Ativa a proteção contra inundação de CPU. Define um limite de 500 pacotes por segundo para as portas GPON especificadas. Configura um temporizador de 300 segundos para a proteção nas portas GPON.

Modelos LD3032, 3096	Descrição
configure terminal cpu-flood-guard enable interface gpon <PORTA_GPON> cpu-flood-guard 100 cpu-flood-guard timer 1800 !	Ativa a proteção contra inundação de CPU. Seleciona a interface GPON específica. Define um limite de 100 pacotes por segundo para a interface selecionada. Configura um temporizador de 1800 segundos (30 minutos) para a proteção na interface.

3.6 Backup das configurações da OLT

Possuir backup periódico das configurações da OLT é importante para casos de perda da base de dados, ou caso de falha em alterações de configuração. Esta prática pode economizar tempo para restabelecimento da operação da rede.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
copy running-config <filename> copy tftp config download <filename>.CFG	

To exit : press Ctrl+D --- IP address or name of remote host (TFTP): <tftp_server> Download File Name [teste.CFG]:	Inicia o processo de download do arquivo de configuração especificado. Solicita o endereço IP ou nome do servidor TFTP. Solicita o nome do arquivo a ser baixado.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
copy tftp <SERVER> config export running-config !	Copia a configuração atual do equipamento para o servidor TFTP especificado.

3.7 Criptografia de senhas armazenadas

As senhas dos usuários locais podem ser vistas através do comando "show running-config". Para evitar que as senhas fiquem expostas, recomenda-se utilizar criptografia de senhas.

Modelos LD3008, LW3008c, LD3016, G2500, LD3032, 3096	Descrição
configure terminal service password-encryption	Configuração para criptografia das senhas armazenadas no equipamento

4 DETECÇÃO E CONTROLE DE LOOPS L2

4.1 Source MAC address Monitoring (SRC-MAC-MON – Somente OLTs LD3008, LW3008C, LD3016, G2500, LD3032, 3096)

A funcionalidade Source MAC address Monitoring (SRC-MAC-MON) permite que a OLT identifique ONUs problemáticas através da análise do endereço MAC de origem dos frames recebidos (SRC-MAC).

Caso a OLT identifique um frame cujo SRC-MAC seja igual ao MAC de sistema da OLT, caracterizando um loop L2, é realizado o bloqueio da ONU que enviou o frame.

O desbloqueio de uma ONU em loop pode ser configurado para ocorrer de forma manual ou de forma automática, baseado em uma temporização (expire-timeout).

É recomendado utilizar sempre o desbloqueio manual.

Configuração de srcmac-monitor nas interfaces PON 1 e 2 da OLT:

Comandos	Descrição
configure terminal gpon gpon-olt 1 olt srcmac-monitor enable auto-onu-block gpon-olt 2 olt srcmac-monitor enable auto-onu-block	Configuração para desbloqueio manual das ONUs

Comandos	Descrição
show on block status [OLT-ID] [ONU-ID] ! configure terminal gpon gpon-olt [OLT-ID] onu unblock ONU-ID	Verificação e desbloqueio manual de ONU

A eficiência da funcionalidade SRC-MAC-MON na identificação e bloqueio de loops depende da geração de frames pela OLT capazes de circular por toda a rede L2.

A funcionalidade Loop Detection descrita no capítulo a seguir necessita ser configurada nas interfaces PON que se deseja proteger a fim de garantir a geração periódica de frames para monitoração de MAC.

4.2 Loop Detection

A funcionalidade de Loop Detection (LD) permite que as interfaces configuradas enviem periodicamente frames broadcast loop-detect cujo 20 SRC-MAC é o endereço MAC de sistema da OLT. As interfaces, então, monitoram o recebimento desses frames identificando também a condição de loop. Por utilizar frames broadcast, o LD não depende de qualquer configuração adicional em

equipamentos conectados ao acesso ONU; STP por exemplo. Os frames broadcast loop-detect são enviados em todas as bridges associadas às interfaces PON da OLT, incluindo frames untagged caso a interface esteja configurada para tal.

A fim de garantir a eficiência na detecção de loop, o período de envio dos frames loop-detect (period) deve ser sintonizado em 1 segundo.

A funcionalidade LD, mesmo configurada para apenas identificar um loop, apesar de não bloquear a interface, utiliza uma temporização para iniciar uma nova detecção de loop (timer). Assim, considerando a detecção de loop na interface PON, o tempo de detecção controla o intervalo mínimo entre detecções de loop em ONUs de uma mesma interface PON.

Por isso, o tempo de detecção deve ser sintonizado em 5 segundos.

4.2.1 Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096

Nestes modelos de OLTs, para ocorrer o bloqueio automático da ONU em que o loop foi detectado, é necessário combinar as funcionalidades SRC-MAC-MON e LD nas interfaces PON a fim de identificar e bloquear seletivamente apenas as ONUs envolvidas na condição de loop L2.

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal bridge loop-detect enable loop-detect 1-2 loop-detect 1-2 period 1 loop-detect 1-2 timer 5	Configuração de loop-detect nas interfaces PON 1 e 2 da OLT: intervalo de envio de 1s e tempo de detecção de 5s:
Modelos LD3032, 3096	**Descrição**
configure terminal loop-detect enable interface gpon <PORT> loop-detect period 1 loop-detect timer 5	Configuração de loop-detect nas interfaces PON 1 e 2 da OLT: intervalo de envio de 1s e tempo de detecção de 5s:

4.2.2 Modelos 3508, 3516

Para estes modelos de OLT, apenas uma configuração é necessária para habilitar a detecção de loop nas ONUs. Após habilitar este comando, quando houver qualquer ocorrência de loop, ou seja, se a OLT receber novamente um pacote que foi enviado por ela, a OLT vai imediamente bloquear a ONU por onde o pacote de loop foi recebido.

O valor recomendado de envio de pacotes para monitoramento de loop nestas OLTs é de 10 segundos.

Comandos	Descrição
configure terminal interface gponx keepalive 10 !	Configuração de loop-detect na interface gponx. Exemplo: interface gpon1

4.3 Monitoramento e localização de Loops

Como boas práticas, abaixo, estão exemplificadas as maneiras para se monitorar e localizar loops na rede:

4.3.1 Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096

Os logs gerados pela funcionalidade SRC-MAC-MON permitem apontar as ONUs envolvidas no loop L2.

Segue abaixo um exemplo de loop entre as ONUs (1,1) e (1,2):

```
Aug 4 15:03:39 system: port 1 is looping

Aug 4 15:03:39 GPON[121]: ONU(1,1) Found NEW MAC is System MAC

Aug 4 15:03:40 GPON[121]: notify_priority_function_call(3747) Receive updated Block Status of ONU(1,1)

Aug 4 15:03:40 GPON[121]: ONU(1,1) is Blocking Status

Aug 4 15:03:40 GPON[121]: ONU(1,2) Found NEW MAC is System MAC

Aug 4 15:03:40 GPON[121]: notify_priority_function_call(3747) Receive updated Block Status of ONU(1,2)

Aug 4 15:03:40 GPON[121]: ONU(1,2) is Blocking Status
```

```
Aug 4 15:03:41 GPON[121]: ONU(1,1) eth port 4 link off(operational)

Aug 4 15:03:42 GPON[121]: notify_priority_function_call ONU(1,1) MIb Sync Data 0

Aug 4 15:03:44 GPON[121]: ONU(1,1) eth port 4 link on(operational)

Aug 4 15:03:44 system: port 1 is moved to loop-detect detecting list by timeout

Aug 4 15:03:51 GPON[121]: ONU(1,1) eth port 4 link off(operational)

Aug 4 15:03:52 GPON[121]: notify_priority_function_call ONU(1,2) MIb Sync Data 0
```

Exemplo de log do desbloqueio automático das ONUs (1,1) e (1,2):

```
Aug 4 15:04:40 GPON[121]: ONU(1,2) Success to check the traffic profile

Aug 4 15:04:40 GPON[121]: notify_priority_function_call(3747) Receive updated Block Status of ONU(1,2)

Aug 4 15:04:40 GPON[121]: ONU(1,2) is Unblocking Status

Aug 4 15:04:41 GPON[121]: ONU(1,1) Success to check the traffic profile

Aug 4 15:04:41 GPON[121]: notify_priority_function_call(3747) Receive updated Block Status of ONU(1,1)

Aug 4 15:04:41 GPON[121]: ONU(1,1) is Unblocking Status

Aug 4 15:04:42 GPON[121]: notify_priority_function_call ONU(1,2) MIb Sync Data 73 Aug 4 15:04:43
GPON[121]: notify_priority_function_call ONU(1,1) MIb Sync Data 49
```

Os logs podem ser redirecionados para servidor Syslog remote através dos comandos abaixo:

```
configure terminal

syslog output info remote SERVER IPV4 ADDR

!
```

Exemplo de log no servidor:

configure terminal 08/08/2016 10:43:51 [363] From: (10.150.4.25) Fac:0

Sev:6 Msg >>> system: port 1 is looping

08/08/2016 10:43:52 [367] From: (10.150.4.25) Fac:0 Sev:6 Msg >>> system: port 2 is moved to loop-detect detecting list by timeout

08/08/2016 10:43:52 [364] From: (10.150.4.25) Fac:1 Sev:4 Msg >>> GPON[121]: ONU(1,2) Found NEW MAC is System MAC

08/08/2016 10:43:52 [365] From: (10.150.4.25) Fac:1 Sev:4 Msg >>> GPON[121]: ONU(1,2) is Blocking Status

08/08/2016 10:43:52 [366] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> GPON[121]: ONU(2,2) eth port 3 link on(operational)

08/08/2016 10:43:57 [368] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> GPON[121]: ONU(2,2) eth port 3 link off(operational)

08/08/2016 10:43:59 [369] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> GPON[121]: ONU(2,2) eth port 3 link on(operational)

08/08/2016 10:43:59 [370] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> GPON[121]: ONU(1,2) eth port 4 link on(operational)

08/08/2016 10:44:11 [371] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> IMISH[2300]: show onu block status 1

08/08/2016 10:44:14 [372] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> IMISH[2300]: show onu block status 2

08/08/2016 10:44:37 [373] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> GPON[121]: ONU(2,2) eth port 3 link off(operational)

08/08/2016 10:44:37 [374] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> GPON[121]: ONU(1,2) eth port 4 link off(operational)

08/08/2016 10:44:48 [375] From: (10.150.4.25) Fac:1 Sev:4 Msg >>> GPON[121]: ONU(1,2) is Unblocking Status

08/08/2016 10:44:59 [376] From: (10.150.4.25) Fac:1 Sev:6 Msg >>> IMISH[2300]: show onu block status 1

É possível também verificar o estado de bloqueio de ONU através de comando CLI. Verificação de ONU (1,2) bloqueada:

```
Aug 8 10:44:14 system: port 1 is looping

Aug 8 10:44:14 GPON[121]: ONU(1,2) Found NEW MAC is System MAC

Aug 8 10:44:15 GPON[121]: notify_priority_function_call(3747) Receive updated Block Status of ONU(1,2)

Aug 8 10:44:15 GPON[121]: ONU(1,2) is Blocking Status

Aug 8 10:44:15 GPON[121]: ONU(2,2) eth port 3 link on(operational)

Aug 8 10:44:19 system: port 2 is moved to loop-detect detecting list by timeout

Aug 8 10:44:25 GPON[121]: ONU(2,2) eth port 3 link off(operational)

Aug 8 10:44:27 GPON[121]: ONU(2,2) eth port 3 link on(operational)

Aug 8 10:44:27 GPON[121]: ONU(1,2) eth port 4 link on(operational) 23

Aug 8 10:44:27 GPON[121]: notify_priority_function_call ONU(1,2) MIb Sync Data 0



SWITCH(config)# show onu block status 1

----------------------------------------

OLT | ONU | Block Status | Block Reason

----------------------------------------

1 | 1 | Unblock | None

1 | 2 | Auto Block | SRCMAC

1| 3 | Unblock | None

1 | 4 | Unblock | None

1 | 5 | Unblock | None

1 | 6 | Unblock | None
```

4.3.2 Modelos 3508, 3516

Na ocorrência de loop, é possível verificar que a ONU envolvida entrar em status bloqueada através de logs e através de comando de show, que pode ser verificado conforme abaixo:

```
2024 Oct 25 10:32:12 UTC OLT GPON-4 [2331]: [ONU] - ONU Blocked.

Interface: gpon3, ONU-ID: 1.


OLT# show onu table interface gpon3


-------------------------------------------------------------------------

|GPON | ONU | Serial number | Model name | Link status | Profile name | Profile status|

-------------------------------------------------------------------------

| 3 | 1 | FRKW298008b6 | 710-40B | Active | 200_acesso (B) | Uploaded |

-------------------------------------------------------------------------
```

5 MULTICAST

As recomendações abaixo são consideradas boas práticas de desempenho de rede que visam mitigar problemas em cenários de multicast.

5.1 Bloqueio de tráfego multicast desconhecido

Quando um tráfego multicast chega a uma porta e a tabela MCFDB não possui informações de encaminhamento, o tráfego é encaminhado para todas as interfaces da OLT. Esse comportamento pode gerar uma sobrecarga de tráfego multicast na OLT, além de inundar a rede do cliente com encaminhamentos multicast.

Para evitar isso, recomenda-se utilizar o bloqueio do tráfego multicast desconhecido. Dessa forma, a OLT irá dropar os endereços que não possuem informações de encaminhamento. Essa funcionalidade pode ser configurada de maneira geral na OLT ou para a VLAN específica em uso.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descrição
configure terminal ip unknown-multicast [port <PORT>] block	Bloqueio de tráfego multicast desconhecido

Modelos 3508 / 3516	Descrição
configure terminal 12 unknown mcast discard	Bloqueio de tráfego multicast desconhecido

5.2 Definição do GEM multicast (Somente OLTs LD3008, LW3008C, LD3016, G2500)

Modelos LD3008, LW3008C, LD3016, G2500	Descrição
configure terminal gpon olt multicast-gem 4094	Define o GEM Multicast

Modelos 3032, 3096	Descrição
configure terminal olt multicast-gem 4094	Define o GEM Multicast