Security Best Practices Configuration Guide and Laserway Recommendations

Document Revision History:

Date	Revision	Reasoning
20/01/2025	0	First version

Summary

1 OBJECTIVE

Network security involves protecting the network infrastructure and the data that flows through it. To achieve this, good practices in configuration, administration, and operation are employed to keep networks protected against potential internal or external attacks and data breaches.

To ensure easier and faster network operation and maintenance, as well as improved vulnerability detection, the minimum security requirements and best practices must be considered from the beginning of the project.

This document addresses a set of minimum configurations and recommendations to be applied when implementing or reviewing a network.

2 SECURITY CONFIGURATIONS

The following configurations must be customized for each Laserway project to enhance security and monitoring.

2.1 Remote Access to the OLT

For security reasons, it is recommended to block Telnet access to the OLT and enable the SSH server service for remote access.

2.1.1 SSH Server Configuration

Model G2500	Description
configure terminal ssh server enable !	Enables the SSH server.

Models: LD3008, LW3008C, LD3016, LD3032, 3096	Description
configure terminal service ssh	Enables the SSH server.

Models: 3508/3516	Description
configure terminal service ssh enable	Enables the SSH server.

2.1.2 Disable Telnet Connections

Models: 3508/3516	Description
configure terminal service telnet disable	Disable the Telnet service.

2.1.3 Limit Simultaneous Connections

The OLT has a default limit of 8 simultaneous connections. Set a number between 1 and 8 as needed.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal login connect 5 !	Restricts simultaneous users (in this case, to 5).

Models: 3508/3516	Description
configure terminal no line vty 5 39 !	Restricts simultaneous users (in this case, to 5).

2.1.4 Disable SNMPv2

The SNMPv2 protocol has several known vulnerabilities, so it is recommended to use the SNMPv3 protocol when necessary. To disable the SNMPv2 protocol, the default read and write communities should be removed as follows:

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal no snmp community ro public no snmp community rw private !	Removes the read and write communities to disable SNMPv2.

The SNMPv3 protocol addresses security issues by combining authentication and packet encryption over the network.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal snmp user <user> md5 <password> smp group admin v3 <user> snmp access admin v3 auth all all all !	SNMPv3 configuration example.

Models: 3508/3516	Description
configure terminal snmp-server users create <user> rw priv <privacy> sha <user_password>	SNMPv3 configuration example.

2.2 Remote Access Control to the OLT

The Admin Flow and Admin Policy features allow classification and control for accessing the OLT, similar to an administrative access list. It is recommended to create rules to allow SSH and SNMP traffic only from trusted sources (source IP).

2.2.1 SSH Connection Control

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal flow admin SSH_BLOCK create ip any <OLT_MGMT_IP> tcp any 22 apply !	Creates a new flow rule called SSH_BLOCK, and defines a rule to block any TCP connection on port 22 (SSH) from any source IPs to the OLT's management IP.
flow admin SSH_PERMIT create ip <SOURCE_IP> <OLT_MGMT_IP> tcp any 22 apply !	Configures SSH access permission.
policy admin SSH_BLOCK create include-flow SSH_BLOCK priority medium action match deny apply !	Creates a new firewall policy called "SSH_BLOCK." Includes the flow rule "SSH_BLOCK" in the policy. Sets the policy priority to medium. Specifies the action to be taken when the rule is matched to deny the traffic.
policy admin SSH_PERMIT create include-flow SSH_PERMIT priority high action match permit apply	Creates a new firewall policy called "SSH_PERMIT." Includes the flow rule "SSH_PERMIT" in the policy. Sets the policy priority to high. Specifies the action to be taken when the rule is matched to allow the traffic.

Models: 3508 - 3516
Not supported

2.3 Configuring authentication

2.3.1 Change Default Password on First Login

It is recommended to change the default password of the OLT during the first login, using a strong password configuration based on the following criteria:

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	
• Minimum of 10 characters, maximum of 16 characters (excluding "?"); • Must contain at least 1 uppercase alphabetical letter and 1 lowercase alphabetical letter (A-Z, a-z); • Must contain at least 1 number (0-9); • Must contain at least 1 special character; • Do not use a blank password; • Must contain at least 4 characters different from the current password.	
Commands	**Description**
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. Enter the new password:	Initiates the password change process for the specified user. Prompt indicating that the user's password is being changed. Prompt to enter the new password, with a maximum of 16 characters. It is recommended to use a combination of uppercase letters, lowercase letters, and numbers for added security.

Re-enter the new password: Password changed.	Prompt to enter the new password. Prompt to re-enter the new password for confirmation. Prompt confirming that the password has been successfully changed.

Models: 3508/3516	
• Minimum of 6 characters, maximum of 8 characters (except "?"); • Must contain at least 1 uppercase alphabetical letter and 1 lowercase alphabetical letter (A-Z, a-z); • Must contain at least 1 number (0-9); • Must contain at least 1 special character; • Do not use a blank password; • Must contain at least 4 characters different from the current password.	
Commands	**Description**
configure terminal username admin password ********	Password configuration

Note: If it is necessary to restore default username and password access, the recovery procedure can be found in the Product Manuals and in the support section of the Furukawa website:

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

2.3.2 Centralized Authentication Using AAA Protocol

The use of a centralized user database for authentication simplifies management and increases the security level for OLT access.

The AAA protocol (Authentication, Authorization, and Accounting) provides significant advantages for network security and management and can be used for logging into the OLT.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
RADIUS Server authentication 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 ! *The user's privilege is defined in the "users" file of the RADIUS server. For example, for a user with admin privilege, use only the parameter cisco-avpair = "shell:priv-lvl=15". It is not necessary to mention the Service-Type.*	Enables RADIUS authentication. Defines primary RADIUS servers. Enables host and specifies the management interface for communication with the RADIUS servers.
TACACS Server authentication configure terminal login local tacacs enable login remote tacacs enable login local tacacs primary login remote tacacs primary	Enables TACACS+ authentication. Defines primary TACACS+ servers. Enables hosts, and Specifies the management interface for communication with the TACACS+ servers.

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 !	

Depending on server availability, either RADIUS server-based authentication or TACACS server-based authentication can be used.

Note: The configuration "login local/remote host auto-enable" ensures that authentication attempts with local users (e.g., admin) occur only if there is no connection to the RADIUS server. If a connection exists but authentication fails (e.g., invalid username or password), local authentication will not occur. This configuration is preferred over permanently disabling local user authentication with "login local/remote host disable."

Models: 3508, 3516	Description
On the OLT, it is both possible and recommended to implement Authentication, Authorization, and Accounting/Auditing configurations using TACACS, as detailed below: 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	Authentication, Authorization, and Accounting/Auditing configuration on TACACS.

aaa accounting command default group tacacs ! *Note: Currently, the OLT only supports authentication via the RADIUS server and does not support authorization or accounting/auditing.* If a RADIUS server is used, the configuration applies only to authentication: configure terminal radius-server host <IP_ADDR> key <KEY> aaa new-model aaa authentication login default group radius local aaa authentication login console local !	RADIUS server Configuration

2.3.3 Temporary Lockout Against Unauthorized Access Attempts

The OLT should be configured to temporarily block repeated unauthorized user authentication attempts as a form of brute force access prevention. It is recommended to configure a maximum of 3 attempts with a block time of at least 5 minutes.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal login attempts 3 delay 10 !	Configuration for temporary lockout against failed access attempts.

Models: 3508, 3516
Not supported

2.3.4 Inactive Session Timeout (Timeout)

Another form of preventing unauthorized access is configuring session timeout for inactivity. It is recommended to set the timeout to 5 minutes.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal exec-timeout 5 !	Timeout configuration based on inactivity time (in this case, 5 minutes).

Models: 3508, 3516	Description
configure terminal line vty 0 39 exec-timeout 5	Timeout configuration based on inactivity time (in this case, 5 minutes).

2.4 ONUs access control

For security reasons, each ONU should have its default access password changed, either via web page (for ONU models that have one) or via the ONU's CLI. It is also recommended, for ONUs configured in Router mode – Home Gateway Unit (HGU) – to disable access to the ONU via the LAN interface, allowing access only through the WAN interface.

The password change for the ONU may vary between models. Some ONUs have more complex and detailed requirements for password creation, but generally, the minimum recommended password change requirement should be:

- At least 8 characters
- At least one uppercase letter and one lowercase letter
- Contain numbers from 0 to 9
- At least one special character

2.5 Disable LLDP

The LLDP protocol should not be enabled on GPON interfaces, as it represents a DoS vulnerability on the OLT.

2.5.1 Disable LLDP in the GPON interfaces

By default, this functionality is disabled on the OLTs.

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge no lldp <FIRST_PORT-LAST_PORT>	Disables LLDP on the interfaces.

Models: LD3032, 3096	Description
configure terminal interface gpon <1> lldps disable !	Disables LLDP on the interfaces. In this case, interface GPON 1.

Models: 3508, 3516	Description
configure terminal interface gpon <1> no lldp !	Disables LLDP on the interfaces. In this case, interface GPON 1.

2.6 Local and Remote Syslog

It is recommended to configure a remote syslog server for backup and centralization of network messages. The syslog server is a system that collects and stores logs from different network devices, such as routers and switches, in a central location. This facilitates the analysis and correlation of log messages, aiding in issue identification and resolution.

Additionally, it is important to adjust the log levels. Log levels determine the amount and type of information that is recorded. Customizing these levels helps avoid logging unnecessary information, focusing only on data relevant to network administration and security.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
The Syslog server function is enabled by default in the OLT to permit log registration in the system. **Remote Syslog server and logging level Configuration.** configure terminal syslog output info remote <SERVER_IP> syslog output info local volatile syslog output notice local non-volatile	Configures log output to a remote server and local storage, both volatile and non-volatile.

Models: 3508 / 3516	Description
Syslog level configuration is made by modules and can be altered as shown below. **Logging level configuration (by modules)** configure terminal logging level ? all Set logging level for all messages	Logging level configuration by modules.

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	
Logging level 4 configuration example: configure terminal logging level gpon 4	Configures logging level 4 for GPON messages.

Note: In normal network operation, it is recommended to set the maximum logging level to 4. Higher logging levels should only be used occasionally for troubleshooting purposes.	
Local Syslog server configuration The local syslog server function is disabled by default on the OLT. To enable local logging, use the commands below. configure terminal logging logfile 4 !	Local Syslog configuration
Remote Syslog server configuration configure terminal logging server 4 <server_ip>	Remote Syslog Server configuration

2.7 VLANs and port description

To facilitate network management, it is recommended to assign descriptions to the GPON interfaces, Ethernet interfaces, VLANs, and link aggregation (LAG) on the OLT.

2.7.1 Ethernet port description configuration

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge port description <ETH_PORT> <REMOTE_HOSTNAME> <REMOTE_PORT>	Adds a description to Ethernet ports.

Models: LD3032, 3096	Description
configure terminal interface tengigabitethernet <0/1> Description <REMOTE_HOSTNAME> !	Adds a description to Ethernet ports. In this case, port 1. Adds a description for the port.

Models: 3508, 3516	Description
configure terminal interface <gpon1> description <DESCRIPTION> !	Adds a description to Ethernet ports. In this case, GPON interface number 1.

2.7.2 GPON ports description configuration

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge port description <PORT_NUMBER> <DESCRIPTION>	GPON port description configuration

Models: LD3032, 3096	Description
configure terminal interface gpon <1/1> description <DESCRIPTION>	GPON port description configuration. In this case, port 1/1.

Models: 3508 / 3516	Description
configure terminal interface <gpon1> description <DESCRIPTION> !	GPON port description configuration. In this case, interface 1.

2.7.3 VLANs description configuration

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal bridge vlan description <VLAN_ID> <VLAN_ DESCRIPTION>	VLAN description configuration

Models: LD3032, 3096	Description
configure terminal interface vlan <VLAN_ID> description <VLAN_DESCRIPTION> !	VLAN description configuration

Models: LD3032, 3096	Description
configure terminal vlan database vlan <VLAN_ID> bridge 1 name <VLAN_DESCRIPTION> !	VLAN description configuration

2.8 Clock sync

Clock synchronization using NTP (Network Time Protocol) is essential for controlling and correlating network logs. Therefore, the entire client network must use the same NTP server reference. It is recommended to configure the OLT as follows:

2.8.1 Timezone configuration

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal show time-zone time-zone	Displays all time zones. Choose the correct time zone.

Models: 3508 / 3516	Description
configure terminal clock timezone <TIMEZONE> !	Time zone Configuration.
It is possible to navigate through the timezone configuration by selecting the continent, country, and state using the command below: configure terminal clock timezone select	Time zone configuration navigation.

2.8.2 NTP server configuration

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal ntp <SERVER1_IP>	NTP server configuration Enter the IP of the NTP server. Example: 200.160.7.186

Models: 3508 / 3516	Description
configure terminal	NTP server configuration

ntp server <SERVER1_IP/HOSTNAME>	Enter the NTP server's IP. Example: 200.160.7.186

3 OTHER CONFIGURATIONS AND GOOD SECURITY PRACTICES

The following recommendations are considered best practices for network design aimed at enhancing security, performance, and scalability issues in GPON access networks.

3.1 Private Management IP Addresses

It is recommended to use private IP addresses for OLT and ONU management, as specified in RFC 1918. Using public IP addresses should be avoided, as they represent a higher risk of external attacks on the equipment if not properly protected by a firewall.

3.2 Broadcast Domains Size

The design of the GPON access network should consider the correct sizing of the broadcast domain, properly segmenting the service VLANs whenever possible. Excessive broadcast frames in the GPON access network can interfere with network performance and may also cause DoS on the network devices' CPUs. As an example, it is suggested that the Internet access service use segmentation into different VLANs and IP networks per GPON port, thereby limiting the broadcast domain to the number of devices connected to the ONUs of each GPON port.

Additionally, it is recommended to avoid enabling the bridge configuration between the OLT GPON ports whenever possible. Some OLT models support the bridge configuration between PON ports by VLAN, allowing direct communication between ONUs only for the services where such communication is necessary. This helps minimize unnecessary network traffic and improves security by limiting interactions between ONUs.

3.3 Avoid using VLAN 1

VLAN 1 is commonly used in network devices as the default or native VLAN for all interfaces and often has control protocols like spanning-tree (STP) enabled by default. Using VLAN 1 in production environments poses a significant security risk as it reverses the logic of network design, where configurations are planned and applied on-demand to interfaces, assuming by default that all interfaces on the device are members of this service VLAN 1.

To change the native VLAN of an interface:

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge	

vlan create <VID> vlan <VID> <port> untagged !	Change the native VLAN of an interface.

Models: 3032, 3096	Description
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 !	Change the native VLAN of an interface.

Models: 3508 / 3516	Description
configure terminal vlan <VID> bridge 1 interface <port> switchport mode trunk switchport trunk allowed vlan add <VID> switchport trunk native vlan <VID> switchport trunk allowed vlan remove 1	Change the native VLAN of an interface

3.4 Storm Control

The Storm Control feature allows limiting the rate of Broadcast, multicast, and Destination Lookup Failure (DLF) packets per second (pps) to be received on an interface, preventing network congestion. When the number of packets exceeds the configured rate, the system discards the excess rate. The rates below serve as an example of proportional sizing based on the interface's capacity, but they should be adjusted according to the traffic characteristics expected for each project/application.

The storm control configuration for the following OLT models is done by configuring the packets per second rate.

An example of a recommended configuration:

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

OLTs Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge storm-control broadcast <RATE> [PORTS] storm-control multicast <RATE> [PORTS] storm-control dlf <RATE> [PORTS] !	Storm Control configuration

The storm control configuration for the following OLT models is done by configuring the packets per second rate.

An example of a recommended configuration:

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

OLTs Models: LD3032, 3096	Description
configure terminal interface gpon/tengigabitethernet <PORT> storm-control broadcast <RATE> storm-control multicast <RATE> storm-control dlf <RATE>	Storm Control Configuration

The storm control configuration for the following OLT models is done by configuring traffic type percentage.

An example of a recommended configuration:

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

Models: 3508 / 3516	Description
configure terminal interface x storm-control broadcast level 1 storm-control multicast level 1 storm-control dlf level 1 !	Storm Control configuration

3.5 CPU Protection (Only for OLTs LD3008, LW3008C, LD3016, G2500, LD3032, 3096)

The CPU protection feature allows limiting the packets per second rate processed by the CPU, so that, in the event of a packet flood in the network, the OLT's CPU is not affected, preventing management loss to the OLT.

The rates below are a recommendation to keep the CPU processing capacity at acceptable levels:

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge cpu-flood-guard enable cpu-flood-guard <GPON_PORTS> 500 cpu-flood-guard<GPON_PORTS> timer 300 !	Enables protection against CPU flooding. Sets a limit of 500 packets per second for the specified GPON ports. Configures a 300-second timer for protection on the GPON ports.

Models: LD3032, 3096	Description
configure terminal cpu-flood-guard enable interface gpon <GPON_PORTS> cpu-flood-guard 100 cpu-flood-guard timer 1800 !	 Enables protection against CPU flooding. Selects the GPON interface. Sets a limit of 100 packets per second for the selected interface. Configures an 1800-second (30-minute) timer for protection on the interface.

3.6 OLT Configuration Backup

Having periodic OLT configuration backups is important in case of database loss or configuration change failures. This practice can save time in restoring network operation.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
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]:	 Starts downloading the specified configuration file. Requests the IP address or name of the TFTP server. Requests the name of the file to be downloaded.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
copy tftp <SERVER> config export running-config !	Copies the current equipment configuration to the specified TFTP server.

3.7 Stored Passwords Encryption

Local user passwords can be viewed on plain text through the "show running-config" command. It is recommended to use password encryption to prevent passwords from being exposed.

Models: LD3008, LW3008c, LD3016, G2500, LD3032, 3096	Description
configure terminal service password-encryption	Encrypts the passwords stored on the OLT.

4 L2 LOOP DETECTION

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

The Source MAC address Monitoring (SRC-MAC-MON) feature allows the OLT to identify problematic ONUs by analyzing the source MAC address of received frames (SRC-MAC).

If the OLT detects a frame with a SRC-MAC matching the OLT's system MAC address, indicating an L2 loop, the ONU that sent the frame is blocked.

The unlocking of a looped ONU can be configured to occur manually or automatically, based on a timeout (expire-timeout).

It is recommended to always use manual ONU unlocking.

Configuration of srcmac-monitor on PON interfaces 1 and 2 of the OLT:

Commands	Description
configure terminal gpon	

gpon-olt 1 olt srcmac-monitor enable auto-onu-block gpon-olt 2 olt srcmac-monitor enable auto-onu-block	Configuration for manual unlocking of ONUs

Commands	Description
show on block status [OLT-ID] [ONU-ID] ! configure terminal gpon gpon-olt [OLT-ID] onu unblock ONU-ID	Verification and manual unlocking of ONU

The effectiveness of the SRC-MAC-MON functionality in identifying and blocking loops depends on the generation of frames by the OLT that are capable of traveling throughout the entire L2 network.

The Loop Detection functionality described in the following chapter needs to be configured on the PON interfaces that are to be protected to ensure the periodic generation of frames for MAC monitoring.

4.2 Loop Detection

The Loop Detection (LD) functionality allows configured interfaces to periodically send loop-detect broadcast frames, where the SRC-MAC is the OLT system's MAC address. The interfaces then monitor the receipt of these frames, also identifying the loop condition. Since it uses broadcast frames, LD does not rely on any additional configuration in devices connected to the ONU access; for example, STP. The loop-detect broadcast frames are sent across all bridges associated with the OLT's PON interfaces, including untagged frames if the interface is configured for such.

To ensure efficient loop detection, the period for sending loop-detect frames (period) should be tuned to 1 second.

The LD functionality, even when configured only to identify a loop, does not block the interface but uses a timer to initiate a new loop detection. Therefore, considering loop detection on the PON interface, the detection time controls the minimum interval between loop detections on ONUs of the same PON interface.

Therefore, the detection time should be tuned to 5 seconds.

4.2.1 OLT Models LD3008, LW3008C, LD3016, G2500, LD3032, 3096

In these OLT models, for automatic blocking of the ONU where the loop was detected, it is necessary to combine the SRC-MAC-MON and LD functionalities on the PON interfaces to selectively identify and block only the ONUs involved in the L2 loop condition.

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal bridge loop-detect enable loop-detect 1-2 loop-detect 1-2 period 1 loop-detect 1-2 timer 5	Loop-detect configuration on PON 1 and 2 interfaces of the OLT: send interval of 1s and detection time of 5s.
Models: LD3032, 3096	**Description**
configure terminal loop-detect enable interface gpon <PORT> loop-detect period 1 loop-detect timer 5	Loop-detect configuration on PON 1 and 2 interfaces of the OLT: sending interval of 1s and detection time of 5s.

4.2.2 OLT Models 3508, 3516

For these OLT models, only one configuration is required to enable loop detection. After enabling this command, whenever a loop occurs, meaning if the OLT receives a packet that was sent by itself, the OLT will immediately block the ONU through which the loop packet was received.

The recommended packet transmission interval for loop monitoring on these OLTs is 10 seconds.

Commands	Description
configure terminal	

interface gponx keepalive 10 !	Loop-detect configuration on the GPON interface. Example: interface gpon1

4.3 Monitoring and Locating Loops

The best practices for monitoring and locating loops in the network are exemplified below:

4.3.1 OLT Models LD3008, LW3008C, LD3016, G2500, LD3032, 3096

The logs generated by the SRC-MAC-MON functionality allow identifying the ONUs involved in the L2 loop.

Here is an example of a loop between ONUs (1,1) and (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
```

Log example for automatic ONUs unlocking ((1,1) and (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
```

The logs can be redirected to a remote Syslog server using the following commands:

```
configure terminal

syslog output info remote SERVER IPV4 ADDR

!
```

Log example on the server:

```
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
```

It is also possible to check the ONU blocking status via CLI. Checking blocked ONU (1,2):

```
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 OLT Models 3508, 3516

In the event of a loop, it is possible to verify that the involved ONU enters a blocked status through logs and the "show" command, which can be checked as follows:

```
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

The following recommendations are considered best practices for network performance aimed at mitigating issues in multicast scenarios.

5.1 Blocking Unknown Multicast Traffic

When multicast traffic arrives at a port and the MCFDB (Multicast Forwarding Database) table does not have any forwarding information, the traffic is then forwarded to all interfaces of the OLT. This behavior can cause an overload of multicast traffic on the OLT, as well as flooding the customer's network with multicast traffic.

To avoid this, it is recommended to block unknown multicast traffic. This way, the OLT will drop multicast traffic that does not have any forwarding information. This functionality can be configured generally on the OLT or for the specific VLAN in use.

Models: LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Description
configure terminal ip unknown-multicast [port <PORT>] block	Blocking Unknown Multicast Traffic

Models: 3508 / 3516	Description
configure terminal 12 unknown mcast discard	Blocking Unknown Multicast Traffic

5.2 Multicast GEM Setting (Only for OLTs LD3008, LW3008C, LD3016, G2500)

Models: LD3008, LW3008C, LD3016, G2500	Description
configure terminal gpon olt multicast-gem 4094	Defines the GEM Multicast

Models: 3032, 3096	Description
configure terminal olt multicast-gem 4094	Defines the GEM Multicast