Guía de configuración de buenas prácticas de seguridad y otras recomendaciones Laserway

Historial de revisión del documento:

Fecha	Revisión	Motivo de la revisión
20/01/2025	0	Entrega inicial

Sumário

1 OBJETIVO

La seguridad de las redes es una categoría que implica la protección de la infraestructura de red y de los datos que viajan a través de ella. Para ello, se emplean buenas prácticas de configuración, administración y funcionamiento para mantener las redes a salvo de posibles ataques internos o externos y de la violación de datos.

Para facilitar y agilizar la operación y el mantenimiento de la red, así como para detectar vulnerabilidades, es necesario respetar los requisitos mínimos de seguridad y las buenas prácticas que deben aplicarse desde el inicio del proyecto.

Este documento trata de un conjunto de configuraciones mínimas y recomendaciones que deben aplicarse al desplegar o revisar una red.

2 AJUSTES DE SEGURIDAD

Las siguientes configuraciones deben ser personalizadas por proyecto Laserway para mejorar la seguridad y monitorización de los equipos GPON.

2.1 Acceso Remoto a la OLT

Por razones de seguridad, recomendamos bloquear el acceso telnet al dispositivo y habilitar el servicio de servidor SSH para el acceso remoto.

2.1.1 Configuración del servidor SSH

Modelo G2500	Descripción
configure terminal ssh server enable !	Habilitar servidor ssh

Modelos LD3008, LW3008C, LD3016, LD3032, 3096	Descripción
configure terminal service ssh	Habilitar servidor ssh

Modelos 3508/3516	Descripción
configure terminal service ssh enable	Habilitar servidor ssh

2.1.2 Desactivar las conexiones telnet

Modelos 3508/3516	Descripción
configure terminal service telnet disable	Desactivar el servicio telnet

2.1.3 Límite de conexiones simultáneas

El dispositivo tiene un límite por defecto de 8 conexiones simultáneas. Introduzca un número entre 1 y 8 según sea necesario.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal login connect 5 !	Comandos para restringir los usuarios simultáneos (en este caso, 5)

Modelos 3508/3516	Descripción
configure terminal no line vty 5 39 !	Comandos para restringir los usuarios simultáneos (en este caso, 5)

2.1.4 Bloqueo del acceso SNMPv2

El protocolo SNMPv2 tiene una serie de vulnerabilidades conocidas y se recomienda utilizar el protocolo SNMPv3 cuando sea necesario. Para bloquear el protocolo SNMPv2, las comunidades de lectura y escritura predeterminadas deben eliminarse del siguiente modo:

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal no snmp community ro public no snmp community rw private !	Eliminación de comunidades de lectura y escritura para bloquear el acceso SNMPv2

El protocolo SNMPv3 aborda los problemas de seguridad combinando la autenticación y el cifrado de paquetes a través de la red.

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

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

2.2 Control de acceso remoto OLT

Las funcionalidades Admin Flow y Admin Policy permiten clasificar y controlar el acceso al equipo como si se tratara de una lista de acceso administrativo. Recomendamos crear reglas para permitir el tráfico SSH y SNMP sólo desde fuentes de confianza (IP de origen)..

2.2.1 Control de las conexiones SSH

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal flow admin SSH_BLOCK create ip any <IP_GERENCIA_OLT> tcp any 22 apply !	Cree una nueva regla de flujo llamada SSH_BLOCK y configure la regla para bloquear cualquier conexión TCP en el puerto 22 (SSH) desde cualquier ip de origen a la ip de administración de la OLT.
flow admin SSH_PERMIT create ip <IP_DE_ORIGEM> <IP_GERENCIA_OLT> tcp any 22 apply !	Establecer el permiso de acceso SSH
policy admin SSH_BLOCK create include-flow SSH_BLOCK priority medium action match deny apply !	Cree una nueva política de firewall llamada «SSH_BLOCK». Incluye la regla de flujo «SSH_BLOCK» en la política. Establece la prioridad de la política en media. Especifica que la acción que se llevará a cabo cuando coincida la regla es denegar el tráfico.
policy admin SSH_PERMIT create include-flow SSH_PERMIT priority high action match permit	Crea una nueva política de firwewall denominada «SSH_PERMIT». Incluye la regla de flujo «SSH_PERMIT» en la política. Establece la prioridad de la política en alta.

apply !	Especifica que la acción que se llevará a cabo cuando coincida la regla es permitir el tráfico.

Modelos 3508 - 3516
No soporta

2.3 Autenticación de acceso OLT

2.3.1 Cambiar la contraseña default en el primer acceso

Se recomienda cambiar la contraseña predeterminada de los dispositivos durante el primer inicio de sesión de acceso utilizando la configuración de contraseña segura basada en los siguientes criterios:

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	
• Mínimo 10 caracteres, máximo 16 caracteres (excepto «?»); • Contener al menos 1 carácter alfabético en mayúscula y 1 carácter alfabético en minúscula (A-Z, a-z); • Contener al menos 1 número (0-9); • Contener al menos 1 carácter especial; • No utilice una contraseña en blanco; • Contener al menos 4 caracteres diferentes de la contraseña actual.	
Comandos	**Descripción**
configure terminal passwd <user> Changing password for <user> Enter the new password (maximum of 16 characters)	Inicia el proceso de cambio de contraseña del usuario especificado. Mensaje indicando que se está cambiando la contraseña del usuario. Pide que se introduzca la nueva contraseña, con un máximo de 16 caracteres.

Please use a combination of upper and lower case letters and numbers. Enter the new password: Re-enter the new password: Password changed. !	Recomienda utilizar una combinación de mayúsculas, minúsculas y números para mayor seguridad. Le pide que introduzca la nueva contraseña. Le pide que vuelva a introducir la nueva contraseña para confirmarla. Mensaje de confirmación de que la contraseña se ha modificado correctamente..

Modelos 3508/3516	
• Mínimo de 6 caracteres, máximo de 8 caracteres (excepto "?"); • Contener al menos 1 carácter alfabético en mayúscula y 1 en minúscula (A-Z, a-z); • Contener al menos 1 número (0-9); • Contener al menos 1 carácter especial; • No utilizar una contraseña en blanco; • Contener al menos 4 caracteres diferentes de la contraseña actual.	
Comandos	**Descripción**
configure terminal username admin password ********	Configuración de contraseña

Observación: En caso de que sea necesario restaurar el acceso de usuario y contraseña predeterminados, el procedimiento de recuperación se puede encontrar en los Manuales de los productos y en la sección de soporte del sitio web de Furukawa:

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

2.3.2 Autenticación centralizada utilizando el protocolo AAA

El uso de una base de datos centralizada de usuarios para la autenticación facilita la gestión y aumenta el nivel de seguridad en el acceso al equipo.

El protocolo AAA (Authentication, Authorization, and Accounting) ofrece ventajas importantes para la seguridad y la gestión de redes, y será utilizado para iniciar sesión en la OLT.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
Autenticación 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 ! *El privilegio del usuario se define en el archivo "users" del servidor RADIUS. Por ejemplo, para un usuario con privilegio de administrador, utilice únicamente el parámetro cisco-avpair = "shell:priv-lvl=15" y no mencione el Service-Type.*	Activación de la autenticación RADIUS, definición de servidores RADIUS primarios, habilitación de hosts, especificación de la interfaz de gestión para la comunicación con los servidores RADIUS.
Autenticación 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 !	Activación de la autenticación TACACS+, definición de servidores TACACS+ primarios, habilitación de hosts, especificación de la interfaz de gestión para la comunicación con los servidores TACACS+.

Dependiendo de la disponibilidad del servidor, se puede utilizar tanto la autenticación basada en un servidor RADIUS como en un servidor TACACS..

Observación: La configuración "login local/remote host auto-enable" permite que el intento de autenticación con un usuario local (por ejemplo, admin) ocurra solo si no existe conexión con el SERVIDOR RADIUS. Si existe conexión, pero la autenticación falla (contraseña o usuario inválidos), la autenticación local no se realizará. Esta configuración se prefiere en lugar de deshabilitar permanentemente la autenticación de usuario local mediante "login local/remote host disable"..

Modelos 3508, 3516	Descripción
En la OLT es posible y se recomienda utilizar las configuraciones de autenticación, autorización y contabilidad/auditoría en TACACS, como se indica a continuación: 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	Configuraciones de autenticación, autorización y contabilidad/auditoría en TACACS

aaa accounting login-session default group tacacs aaa accounting command default group tacacs ! ***Obs.:*** *Actualmente, la OLT solo soporta la autenticación en servidor RADIUS, no soportando la autorización ni la contabilidad/auditoría.*	
En caso de utilizarse un servidor RADIUS, la configuración se realiza solo para la autenticación: configure terminal radius-server host <IP_ADDR> key <KEY> aaa new-model aaa authentication login default group radius local aaa authentication login console local !	Configuraciones para servidor RADIUS

2.3.3 Bloqueo temporal contra intentos de acceso no autorizado

Los equipos deben ser configurados para bloquear temporalmente los intentos repetidos de autenticación de usuarios no autorizados como una forma de mitigación contra ataques de fuerza bruta. Se recomienda configurar 3 intentos con un tiempo de bloqueo de al menos 5 minutos..

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal login attempts 3 delay 10 !	Configuración para bloqueo temporal contra intentos de acceso no exitosos

Modelos 3508, 3516
No soportado

2.3.4 Cierre de sesiones inactivas (timeout)

Otra forma de mitigación de accesos no autorizados es la configuración del cierre de sesiones por tiempo de inactividad. Se recomienda configurar 5 minutos..

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal exec-timeout 5 !	Configuración de timeout por tiempo de inactividad (en este caso, 5 minutos)

Modelos 3508, 3516	Descripción
configure terminal line vty 0 39 exec-timeout 5	Configuración de timeout por tiempo de inactividad (en este caso, 5 minutos)

2.4 Configuración de tiempo de espera por inactividad (en este caso, 5 minutos)

Por razones de seguridad, cada ONU debe tener su contraseña de acceso predeterminada modificada, ya sea a través de la página web (para los modelos que la tengan) o mediante la CLI de la ONU. También se recomienda, para las ONUs configuradas en modo Router – Home Gateway Unit (HGU) – deshabilitar el acceso a la ONU a través de la interfaz LAN, manteniendo solo el acceso a través de la WAN del equipo.

El cambio de contraseña de la ONU puede variar según los modelos. Algunos equipos tienen requisitos más complejos y elaborados para la creación de contraseñas, pero en general, el requisito mínimo para el cambio de contraseña que se debe recomendar es el siguiente:

- Tener al menos 8 caracteres
- Tener al menos una letra mayúscula y una letra minúscula
- Tener números del 0 al 9
- Tener al menos 1 carácter especial

2.5 Bloqueo de LLDP en el acceso GPON

El protocolo LLDP no debe ser habilitado en las interfaces GPON; representa una vulnerabilidad de DoS en el equipo.

2.5.1 Desactivar el LLDP en las interfaces

Por defecto, esta funcionalidad está deshabilitada en las OLTs.

Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge no lldp <PRIMERO_PUERTA-ULTIMA_PUERTA>	Desactiva LLDP en las interfaces

Modelos LD3032, 3096	Descripción
configure terminal interface gpon <1> lldps disable !	Desactiva LLDP en las interfaces. En este caso, la interface 1

Modelos 3508, 3516	Descripción
configure terminal interface gpon <1> no lldp !	Desactiva LLDP en las interfaces. En este caso, la interface 1

2.6 Syslog interno y externo

Se recomienda configurar un servidor syslog remoto para respaldo y centralización de los mensajes de red. El servidor syslog es un sistema que recopila y almacena los registros de diferentes dispositivos de red, como routers y switches, en un lugar central. Esto facilita el análisis y la correlación de los mensajes de registro, ayudando en la identificación y resolución de problemas.

Además, es importante ajustar los niveles de logs. Los niveles de logs determinan la cantidad y el tipo de información registrada. Personalizar estos niveles ayuda a evitar el registro de información innecesaria, centrándose solo en los datos relevantes para la administración y seguridad de la red..

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
La función de servidor syslog está habilitada por defecto en la OLT para permitir la generación de registros locales en el sistema. **Configuración de servidor de syslog remoto y niveles locales** configure terminal syslog output info remote <SERVER_IP> syslog output info local volatile syslog output notice local non-volatile	Configuración de la salida de logs a un servidor remoto y almacenamiento local, tanto volátil como no volátil.

Modelos 3508 / 3516	Descripción
La configuración del nivel de logging se realiza por módulos y puede ser modificada según las opciones a continuación. **Configuración de niveles de logging por módulos** configure terminal logging level ? all Set logging level for all messages 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	Configuración de niveles de logging por módulos

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	
Ejemplo de configuración de nivel de logging 4 para GPON: configure terminal logging level gpon 4 *Observación: En una operación normal de red, se recomienda que el nivel máximo de logging a ser utilizado en la OLT sea 4. Niveles de logging superiores deben ser utilizados puntualmente en casos de troubleshooting..*	Configuración de nivel de logging 4 para GPON.
Configuración de servidor de syslog local. La función de servidor de syslog local está deshabilitada por defecto en la OLT. Para permitir la generación de logs locales en el sistema, es necesario habilitarla mediante configuración.. configure terminal logging logfile 4 !	Configuración de servidor de Syslog local.
Configuración de servidor de Syslog remoto. configure terminal logging server 4 <server_ip>	Configuración de servidor de Syslog remoto.

2.7 Descripción de puertos y VLANs.

Con el fin de facilitar la gestión de la red, se recomienda asignar descripciones a las interfaces GPON, Ethernet, VLANs y la agregación de enlaces (LAG) del equipo OLT.

2.7.1 Configuración de la descripción de puertos Ethernet

Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge port description <PORTA_ETH> <HOSTNAME_REMOTO> <PORTA_REMOTA>	Configuración para agregar descripción de puertos Ethernet.

Modelos LD3032, 3096	Descripción
configure terminal interface tengigabitethernet <0/1> Description <HOSTNAME_REMOTO> !	Configuración para agregar descripción a puertos Ethernet. En este caso, puerto 1. Añadir descripción para el puerto

Modelos 3508, 3516	Descripción
configure terminal interface <gpon1> description <DESCRIÇÃO> !	Configuración para agregar descripción a puertos Ethernet. En este caso, interfaz GPON número 1

2.7.2 Configuración de la descripción de puertos GPON.

Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge port description <NUMERO_DA_PORTA> <DESCRIÇÃO>	Configuración de la descripción de puertos GPON.

Modelos LD3032, 3096	Descripción
configure terminal interface gpon <1/1> description <DESCRIÇÃO>	Configuración de la descripción de puertos GPON. En este caso, puerto 1/1

Modelos 3508 / 3516	Descripción
configure terminal interface <gpon1> description <DESCRIÇÃO> !	Configuración de la descripción de puertos GPON. En este caso, interfaz 1

2.7.3 Configuración de la descripción de VLANs.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal bridge vlan description <ID_DA_VLAN> <DESCRIÇÃO_DA_VLAN>	Configuración de la descripción de VLANs.

Modelos LD3032, 3096	Descripción
configure terminal interface vlan <ID_DA_VLAN> description <DESCRIÇÃO_DA_VLAN> !	Configuración de la descripción de VLANs.

Modelos LD3032, 3096	Descripción
configure terminal vlan database vlan <ID_DA_VLAN> bridge 1 name <DESCRIÇÃO_DA_VLAN> !	Configuración de la descripción de VLANs.

2.8 Sincronización del reloj.

Las configuraciones NTP para la sincronización del reloj son importantes para el control y la correlación de los registros de la red, por lo que es fundamental que toda la red del cliente utilice la misma referencia de servidor NTP. Se recomienda configurar la OLT de la siguiente manera:

2.8.1 Configuración de la zona horaria (time zone).

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal show time-zone time-zone	Visualización de todas las zonas horarias y selección de una de ellas.

Modelos 3508 / 3516	Descripción
configure terminal clock timezone <TIMEZONE> !	Configuración de la zona horaria.
Es posible navegar por la configuración de zona horaria, eligiendo continente, país y estado mediante el siguiente comando: configure terminal clock timezone select	Navegación de las opciones de zona horaria.

2.8.2 Configuración del servidor NTP.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal ntp <SERVER1_IP>	Configurando el servidor NTP Solo es necesario ingresar la dirección IP del servidor NTP. Ejemplo: SP 200.160.7.186

Modelos 3508 / 3516	Descripción
configure terminal ntp server <SERVER1_IP/HOSTNAME>	Configurando el servidor NTP Solo es necesario ingresar la dirección IP del servidor NTP. Ejemplo: SP 200.160.7.186

3 OTRAS CONFIGURACIONES Y BUENAS PRÁCTICAS DE SEGURIDAD

Las siguientes recomendaciones se consideran buenas prácticas en el diseño de redes, que buscan mitigar problemas de seguridad, rendimiento y escalabilidad en las redes de acceso PON.

3.1 Direcciones IP de gestión privadas.

Se recomienda utilizar direcciones IP privadas en la red de gestión de los equipos OLT y ONUs, conforme lo especificado en la RFC 1918. El uso de direcciones IP públicas debe ser evitado, ya que representa un mayor riesgo para los equipos frente a ataques externos si no están adecuadamente protegidos por un firewall.

3.2 Limitación de los dominios de Broadcast

El diseño de la red de acceso GPON debe considerar el dimensionamiento adecuado del dominio de Broadcast de los servicios, segmentando correctamente las VLANs de servicio siempre que sea posible. El exceso de tramas Broadcast en la red de acceso GPON puede interferir con el rendimiento de la red, y también puede representar un ataque DDoS a la CPU de los equipos en algunas situaciones. Como ejemplo, se sugiere que el servicio de acceso a Internet utilice segmentación en diferentes VLANs y redes IP por puerto PON del equipo OLT, limitando así el dominio Broadcast a la cantidad de dispositivos conectados a las ONUs de cada puerto.

Adicionalmente, se debe evitar habilitar la configuración de puente entre los puertos GPON de la OLT siempre que sea posible. Algunos modelos de OLT soportan la configuración de puente entre los puertos PON por VLAN, permitiendo limitar la comunicación directa entre las ONUs únicamente a los servicios en los que esta comunicación sea necesaria.

3.3 No utilización de la VLAN 1.

La VLAN 1 es comúnmente utilizada en los dispositivos de red como la VLAN predeterminada o nativa de todas las interfaces y, a menudo, tiene protocolos de control como spanning-tree (STP) habilitados por defecto en esta VLAN. El uso de la VLAN 1 en entornos de producción implica un gran riesgo de seguridad, ya que invierte la lógica del diseño de la red, en la que las configuraciones son planificadas y aplicadas según sea necesario a las interfaces, asumiendo por defecto que todas las interfaces del equipo son miembros de esta VLAN 1 de servicio..

Para realizar el cambio de la VLAN nativa de una interfaz:

Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge vlan create <VID> vlan <VID> <port> untagged !	Cambio de la VLAN nativa de una interfaz

Modelos 3032, 3096	Descripción
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 !	Cambio de la VLAN nativa de una interfaz.

Modelos 3508 / 3516	Descripción
configure terminal vlan <VID> bridge 1	Cambio de la VLAN nativa de una interfaz.

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

3.4 Storm Control

La funcionalidad Storm Control permite limitar la tasa de paquetes por segundo (pps) de Broadcast, multicast y Destination Lookup Failure (DLF) recibidos en una interfaz, evitando la congestión en la red. Cuando el número de paquetes excede la tasa configurada, el sistema descarta el exceso. Las tasas mencionadas a continuación son un ejemplo de dimensionamiento proporcional a la capacidad de la interfaz, pero deben ajustarse según las características del tráfico esperado de cada proyecto/aplicación..

La configuración de Storm Control para estos modelos de OLT se realiza mediante la configuración de limitación de paquetes por segundo.

Un ejemplo de recomendación y configuración:

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

OLTs Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge	

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

La configuración de Storm Control para estos modelos de OLT se realiza mediante la limitación de paquetes por segundo.

Un ejemplo de recomendación y configuración:

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

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

La configuración de Storm Control para estos modelos de OLT se realiza mediante la configuración de limitación del porcentaje de tráfico.

Un ejemplo de recomendación y configuración:

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

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

3.5 Protección de la CPU (Solo OLTs LD3008, LW3008C, LD3016, G2500, LD3032, 3096)

La funcionalidad de protección de la CPU permite limitar la tasa de paquetes por segundo que son procesados por la CPU, de manera que, en caso de un posible flood de paquetes en la red, la CPU de la OLT no se vea afectada y no se pierda el acceso a la OLT.

Las tasas a continuación son una recomendación para mantener la capacidad de procesamiento de la CPU en valores aceptables:

Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge cpu-flood-guard enable cpu-flood-guard <PORTAS_GPON> 500 cpu-flood-guard<GPON_PORTS> timer 300 !	Activa la protección contra inundación de la CPU. Define un límite de 500 paquetes por segundo para los puertos GPON especificados. Configura un temporizador de 300 segundos para la protección en los puertos GPON.

Modelos LD3032, 3096	Descripción
configure terminal cpu-flood-guard enable interface gpon <PORTA_GPON> cpu-flood-guard 100 cpu-flood-guard timer 1800 !	Activa la protección contra inundación de la CPU. Selecciona la interfaz GPON específica.. Define un límite de 100 paquetes por segundo para la interfaz seleccionada.. Configura un temporizador de 1800 segundos (30 minutos) para la protección en la interfaz.

3.6 Backup de las configuraciones de la OLT

Tener copias de seguridad periódicas de las configuraciones de la OLT es importante en caso de pérdida de la base de datos o fallos en las modificaciones de configuración. Esta práctica puede ahorrar tiempo para restablecer la operación de la red.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
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 el proceso de descarga del archivo de configuración especificado. Solicita la dirección IP o el nombre del servidor TFTP. Solicita el nombre del archivo a ser descargado.

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
copy tftp <SERVER> config export running-config !	Copia la configuración actual del equipo al servidor TFTP especificado..

3.7 Cifrado de contraseñas almacenadas.

Las contraseñas de los usuarios locales pueden ser vistas mediante el comando "show running-config". Para evitar que las contraseñas estén expuestas, se recomienda utilizar cifrado de contraseñas.

Modelos LD3008, LW3008c, LD3016, G2500, LD3032, 3096	Descripción
configure terminal service password-encryption	Configuración para criptografia de contraseñas almacenadas en el dispositivo

4 DETECCIÓN Y CONTROL DE LOOPS L2.

4.1 Monitoreo de la dirección MAC de origen (SRC-MAC-MON – Solo OLTs LD3008, LW3008C, LD3016, G2500, LD3032, 3096).

La funcionalidad de Monitoreo de la Dirección MAC de Origen (SRC-MAC-MON) permite que la OLT identifique ONUs problemáticas mediante el análisis de la dirección MAC de origen de los frames recibidos (SRC-MAC).

Si la OLT identifica un frame cuyo SRC-MAC sea igual al MAC del sistema de la OLT, lo que caracteriza un loop L2, se procederá al bloqueo de la ONU que envió el frame

El desbloqueo de una ONU en loop puede ser configurado para ocurrir de forma manual o de forma automática, basado en un tiempo de expiración (expire-timeout)..

Se recomienda utilizar siempre el desbloqueo manual..

Configuración de srcmac-monitor en las interfaces PON 1 y 2 de la OLT.:

Comandos	Descripción
configure terminal gpon gpon-olt 1 olt srcmac-monitor enable auto-onu-block gpon-olt 2 olt srcmac-monitor enable auto-onu-block	Configuración para el desbloqueo manual de las ONUs.

Comandos	Descripción
show on block status [OLT-ID] [ONU-ID] ! configure terminal gpon gpon-olt [OLT-ID] onu unblock ONU-ID	Verificación y desbloqueo manual de ONU.

La eficiencia de la funcionalidad SRC-MAC-MON en la identificación y bloqueo de loops depende de la generación de frames por parte de la OLT capaces de circular por toda la red L2..

La funcionalidad de Detección de Loops descrita en el siguiente capítulo necesita ser configurada en las interfaces PON que se desean proteger, a fin de garantizar la generación periódica de frames para la monitorización de MAC..

4.2 Loop Detection

La funcionalidad de Detección de Loops (LD) permite que las interfaces configuradas envíen periódicamente frames de broadcast loop-detect, cuyo SRC-MAC es la dirección MAC del sistema de la OLT. Las interfaces, entonces, monitorean la recepción de estos frames, identificando también la condición de loop. Al utilizar frames de broadcast, el LD no depende de ninguna configuración adicional en los equipos conectados al acceso ONU, como el STP, por ejemplo. Los frames de broadcast loop-detect se envían en todos los bridges asociados a las interfaces PON de la OLT, incluidos los frames untagged, en caso de que la interfaz esté configurada para ello.

Para garantizar la eficiencia en la detección de loops, el período de envío de los frames loop-detect (period) debe ser ajustado a 1 segundo.

La funcionalidad LD, incluso configurada solo para identificar un loop, aunque no bloquee la interfaz, utiliza una temporización para iniciar una nueva detección de loop (temporizador). Así, considerando la detección de loop en la interfaz PON, el tiempo de detección controla el intervalo mínimo entre las detecciones de loop en ONUs de una misma interfaz PON..

Por ello, el tiempo de detección debe ser ajustado a 5 segundos.

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

En estos modelos de OLTs, para que se produzca el bloqueo automático de la ONU en la que se detectó el loop, es necesario combinar las funcionalidades SRC-MAC-MON y LD en las interfaces PON, con el fin de identificar y bloquear selectivamente solo las ONUs involucradas en la condición de loop L2.

Modelos LD3008, LW3008C, LD3016, G2500	Descripción
configure terminal bridge loop-detect enable loop-detect 1-2 loop-detect 1-2 period 1 loop-detect 1-2 timer 5	Configuración de loop-detect en las interfaces PON 1 y 2 de la OLT: intervalo de envío de 1 segundo y tiempo de detección de 5 segundos:
Modelos LD3032, 3096	**Descripción**
configure terminal loop-detect enable interface gpon <PORT>	Configuración de loop-detect en las interfaces PON 1 y 2 de la OLT: intervalo de envío de 1 segundo y tiempo de detección de 5 segundos:

loop-detect period 1 loop-detect timer 5	

4.2.2 Modelos 3508, 3516

Para estos modelos de OLT, solo se necesita una configuración para habilitar la detección de loop en las ONUs. Después de habilitar este comando, cuando ocurra cualquier incidencia de loop, es decir, si la OLT recibe nuevamente un paquete que fue enviado por ella, la OLT bloqueará inmediatamente la ONU por donde se recibió el paquete de loop.

El valor recomendado para el envío de paquetes para monitoreo de loop en estas OLTs es de 10 segundos.

Comandos	Descripción
configure terminal interface gponx keepalive 10 !	Configuración de loop-detect en la interfaz gponx. Ejemplo: interface gpon1

4.3 Monitoreo y localización de Loops

Como buenas prácticas, a continuación se ejemplifican las maneras de monitorear y localizar loops en la red:

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

Los logs generados por la funcionalidad SRC-MAC-MON permiten identificar las ONUs involucradas en el loop L2.

A continuación se muestra un ejemplo de loop entre las ONUs (1,1) y (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
```

Ejemplo de log del desbloqueo automático de las ONUs (1,1) y (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
```

Los logs pueden ser redirigidos a un servidor Syslog remoto a través de los siguientes comandos

```
configure terminal

syslog output info remote SERVER IPV4 ADDR
```

Ejemplo de log en el 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

Es posible también verificar el estado de bloqueo de una ONU mediante un comando CLI. Ejemplo de verificación de la 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

En caso de un loop, es posible verificar que la ONU involucrada entra en estado bloqueado a través de los logs y mediante el comando de "show", el cual se puede verificar de la siguiente manera:

```
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

Las siguientes recomendaciones son consideradas buenas prácticas de rendimiento de red que buscan mitigar problemas en escenarios de multicast

5.1 Bloqueo de tráfico multicast desconocido

Cuando un tráfico multicast llega a un puerto y la tabla MCFDB no tiene información de encaminamiento, el tráfico se envía a todas las interfaces de la OLT. Este comportamiento puede generar una sobrecarga de tráfico multicast en la OLT, además de inundar la red del cliente con reenvíos multicast.

Para evitar esto, se recomienda bloquear el tráfico multicast desconocido. De esta forma, la OLT descartará las direcciones que no tienen información de encaminamiento. Esta funcionalidad se puede configurar de manera general en la OLT o para la VLAN específica en uso..

Modelos LD3008, LW3008C, LD3016, G2500, LD3032, 3096	Descripción
configure terminal ip unknown-multicast [port <PORT>] block	Bloqueo de tráfico multicast desconocido

Modelos 3508 / 3516	Descripción
configure terminal 12 unknown mcast discard	Bloqueo de tráfico multicast desconocido

5.2 Definición del GEM multicast (Solo OLTs LD3008, LW3008C, LD3016, G2500)

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

Modelos 3032, 3096	Descripción
configure terminal olt multicast-gem 4094	Define el GEM Multicast