BUENAS PRÁCTICAS PARA EVITAR INDISPONIBILIDAD DE SERVICIO EN REDES GPON

1 Situaciones de Riesgo de *Loop*

Una situación de vulnerabilidad comun a que están sujetas redes de datos es el *loop* de paquetes. Un *loop* se caracteriza por la existencia de dos caminos físicos distintos en la interconexión entre elementos de red y que causan un flujo indeseado de paquetes ingresando y retornando al mismo camino de origen de manera constante. Este flujo puede llegar al punto de causar una indisponibilidad total en la rede.

La utilización de la tecnología *Gigabit Passive Optical Network* (GPON) en redes *enterprise* minimiza la posibilidad de ocurrencia de *loops Layer* 2 (L2) en la red, dada la cantidad reducida de equipos activos y funciones bien definidas de los equipos *Optical Line Termination* (OLT) y *Optical Network Unit* (ONU). A los equipos terminales de la red PON, ONUs, se recomienda, por ejemplo, que sean conectados solamente equipos terminales de usuarios, condición que, si seguida, no resultaría en *loops* L2.

Todavía, una rede GPON no está libre de errores de conexión o conexiones no autorizadas de *Access Points* (*Rogue APs*) o *switches* L2 a los ONUs. Para estes casos, es importante que los proyectos de solución Laserway consideren la configuración de un protocolo de *loop avoidance* conforme recomendaciones y consideraciones descriptas en este documento.

En topologías GPON usando las OLTs de Furukawa existen dos situaciones donde se está vulnerable a *loops*: Ligación entre puertas de ONTs conectadas a la misma OLT y ligación entre puertas de ONTs conectadas a puertas de OLT distintas.

1.1 Misma puerta de OLT

Un *loop* lógico podrá ser causado por la conexión entre puertas de dos ONTs conectadas en la misma OLT (figura 1), o por la conexión entre dos puertas de la misma ONT (figura 2) si, y solamente si, las interfaces conectadas pertenencieran a la misma VLAN y la puerta de OLT presentar la funcionalidad de *port-bridge* habilitada.

La funcionalidad de *port-bridge* es normalmente utilizada en redes empresariales y permite la comunicación entre computadores o teléfonos IP que trabajan en ONTs perteneciendo a la misma OLT.

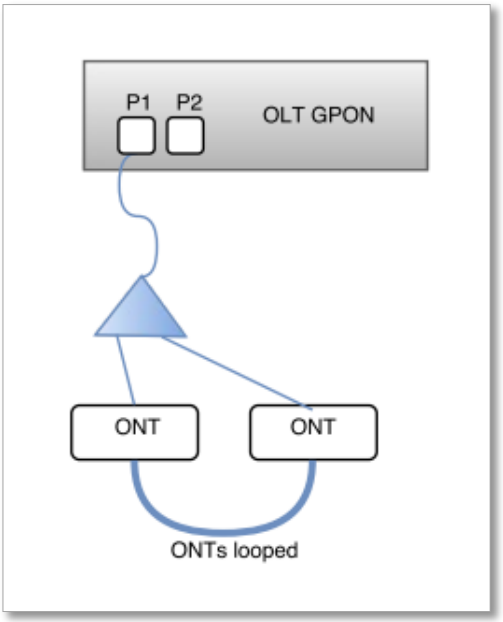

Figura 1 – ONTs conectadas entre si perteneciendo a una misma puerta de OLT (P1).

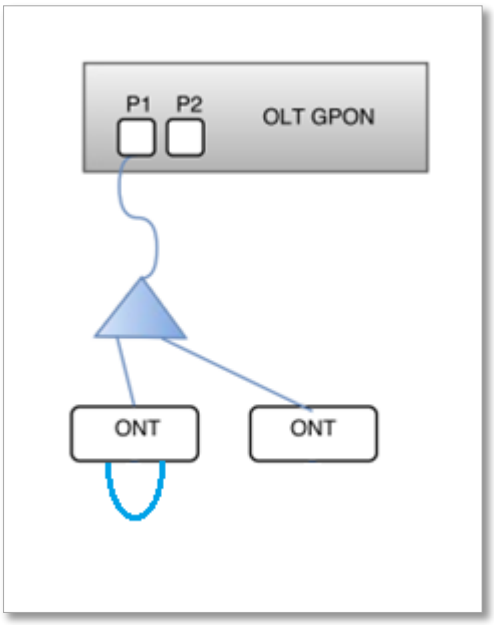

Figura 2 – Puertas de una ONT conectadas entre si.

1.1.1 Port-bridge

Las OLTs GPON Furukawa soportan la funcionalidad *port bridge* de capa 2 (L2), que permite el encaminamiento de paquetes para la misma interfaz que los originó. Cuando la dirección MAC de destino es encontrada, el paquete es encaminado normalmente, aunque en la misma puerta OLT de origen.

Una alternativa al *port-bridge* es la configuración de la funcionalidad *ARP alias*.

1.1.2 ARP alias

Para permitir la comunicación entre *hosts* específicos que están conectados a una misma puerta de OLT, las OLTs GPON Furukawa soportan el comando *arp alias*, que hace con que el switch de concentración responda las requisiciones ARP de los clientes de esta OLT.

1.2 Puertas de OLT distintas

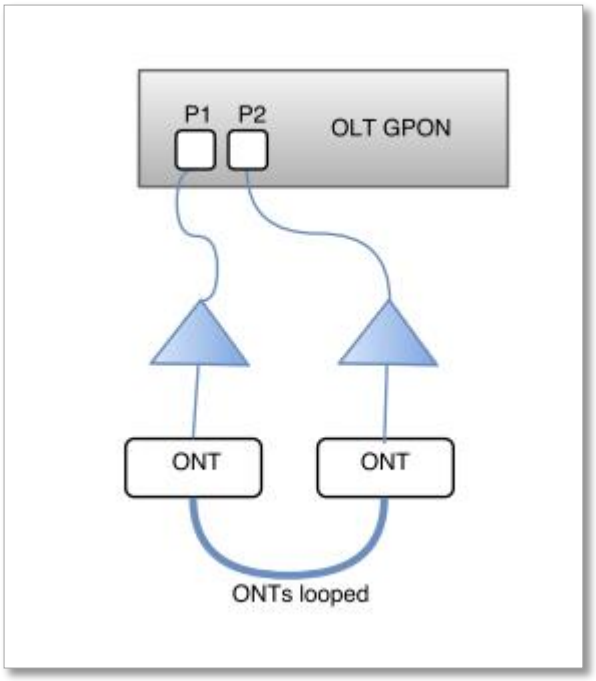

Figura 3 - ONTs conectadas entre si pertenecen a puertas de OLT distintas (P1 y P2)

Es posible la formación de un *loop* conectando ONTs que pertenezcan a puertas de OLT distintas pero que trabajan en el mismo segmento de VLANs. En este caso el *loop* ocurre entre las puertas de OLT y se recomenda habilitar un modo de *spanning-tree* para evitar tal fenómeno.

1.3 Identificación del *Loop*

El primer registro que debe ser consultado para identificación de problemas (*troubleshooting*) con las OLTs GPON es el *syslog* del equipo.

Verifique el syslog de la OLT a través del siguiente comando:

```
SWITCH(config)# show syslog local non-volatile reverse
```

Eventos de loop pueden ser identificados por entradas en el syslog como las siguientes:

```
Jun 23 15:54:47  GPON[278]: ONU(2/2,13)
Found afflict Mac(00:24:21:fe:52:ba).
Stats(TC:4999,IC:2527, MC:2443)

Jun 23 15:54:47  GPON[278]: ONU(2/2,14)
Found afflict Mac(00:24:21:fe:52:ba).
Stats(TC:4999,IC:2527, MC:2443)
```

2 Configuraciones Recomendadas

Para disminuir los efectos indeseables causados por *loop* se recomenda agregar al sistema las configuraciones que siguen en este capítulo.

2.1 Source MAC address Monitoring (SRC-MAC-MON) y Loop Detection (LD)

2.1.1 Source MAC address Monitoring (SRC-MAC-MON)

La funcionalidad *Source MAC address Monitoring* (SRC-MAC-MON) permite que la OLT identifique ONUs problemáticas a través del análisis de la dirección MAC de origen de los frames recibidos (SRC-MAC). Caso la OLT identifique un frame lo cual el SRC-MAC sea igual al MAC de sistema de la OLT, caracterizando un *loop* L2, es realizado el bloqueo de la ONU que envió el *frame*.

El desbloqueo de una ONU en *loop* puede ser configurado para ocurrir de forma administrativa o de forma automática, basado en una temporización (*expire-timeout*). Caso sea utilizado el modo automático de desbloqueo, se recomenda utilizar temporización de por lo menos 300 segundos a fin de permitir la remoción del *loop* físico:

Configuración de srcmac-monitor en las interfaces PON 1 y 2 de la OLT: desbloqueo automático en 300s:

```
configure terminal
gpon
 !
gpon-olt 1/1
olt srcmac-monitor enable auto-onu-block
expire-timeout 300
 gpon-olt 1/2
olt srcmac-monitor enable auto-onu-block
expire-timeout 300
```

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

```
configure terminal
 gpon
  !
  gpon-olt 1/1
   olt srcmac-monitor enable auto-onu-block
  gpon-olt 1/2
   olt srcmac-monitor enable auto-onu-block
```

Verificación y desbloqueo manual de ONU

```
show onu block status OLT-ID [ONU-ID]
!
configure terminal
gpon
 !
 gpon-olt OLT-ID
  onu unblock ONU-ID
```

La eficiência de la funcionalidad SRC-MAC-MON en la identificación y bloqueo de *loops* depende de la creación de frames por la OLT capazes de circular por toda la red L2. La funcionalidad *Loop Detection* descripta en seguida necesita ser configurada en las interfaces PON que se desea proteger a fin de garantir la creación periódica de *frames* para monitoreo de MAC.

2.2 *Loop Detection* (LD)

La funcionalidad de *Loop Detection* (LD) permite que las interfaces configuradas envien periódicamente *frames broadcast loop-detect* lo cual SRC-MAC es la dirección MAC de sistema de la OLT.

Las interfaces, entonces, monitorean el recibimiento de estes *frames* identificando también la condición de *loop*, pero no bloqueando, por *default*, las interfaces involucradas. De esta forma, es posible combinar las funcionalidades SRC-MAC-MON y LD en las interfaces PON a fin de identificar y bloquear de forma selectiva apenas las ONUs involucradas en la condición de *loop* L2.

Por utilizar *frames broadcast*, el LD no depende de cualquier configuración adicional en equipos conectados al acceso ONU; STP por ejemplo. Los *frames broadcast loop-detect* son enviados en todas las *bridges* asociadas a las interfaces PON de la OLT, incluyendo *frames untagged* caso la interfaz esté configurada para tal.

A fin de garantir la eficiencia en la detección de *loop*, el periodo de envio de los frames *loop-detect* (*period*) debe ser ajustado en 3 segundos.

La funcionalidad LD, aunque configurada para apenas identificar un *loop*, no bloquea la interfaz, utiliza una temporización para iniciar una nueva detección de *loop* (*timer*). Así, considerando la detección de *loop* en la interfaz PON, el tiempo de detección controla el intervalo mínimo entre detecciones de *loop* en ONUs de una misma interfaz PON. Por eso, el tiempo de detección debe ser sintonizado en 5 segundos.

Configuración de loop-detect en las interfaces PON 1 y 2 de la OLT: intervalo de envio de 3s y tiempo de detección de 5s:

```
configure terminal
bridge
 loop-detect enable
 loop-detect 1-2
 loop-detect 1-2 period 3
 loop-detect 1-2 timer 5
```

2.3 Monitoreo y localización de loops

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

Ejemplo de log evidenciando 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 encaminados para un servidor *Syslog remote* a través del comando abajo.

Redirecionamento de log para servidor Syslog remoto:

```
configure terminal
syslog output info remote SERVER_IPV4_ADDR
!
```

Ejemplo de log en el servidor Syslog

```
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 ONU a través de comando CLI.

Verificación 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)
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
```

2.4 Escenarios de protección de loops soportados por el SRC-MAC-MON y LD

Conforme citado, el LD no depende de cualquier configuración adicional en equipos conectados al acceso ONU para detección de *loops*, ya que utiliza frames *broadcast*. De esta forma, no existen escenarios conocidos en que la combinación SRC-MAC-MON y LD no logre identificar y bloquear ONUs con acceso en *loop*. Esta recomendación no considera arquitecturas redundantes de conexión en el uplink de la OLT, siendo necesario avaliar el uso de xSTP o *Link Aggregation Group* (*LAG*) en estas condiciones.

2.5 Broadcast storm-control

Esta funcionalidad permite controlar el efecto de la transmisión masiva de paquetes broadcast y multicast.

Es posible establecer una tasa máxima de paquetes broadcast a ser procesados por segundo en una determinada interfaz de OLT.

2.6 Spanning-tree

Verifique la sesión “Spanning-tree protocol (STP)” del manual de usuario para configurar el modo deseado de spanning-tree y evitar el *loop* lógico de paquetes entre puertas de la OLT.

2.7 Acceso serial

En algunas situaciones, un evento de negación de servicio (DoS) como los generados por *loop* pueden impedir el acceso a la gestión del equipo por red (telnet / SSH) e impiden la colecta de información y configuraciones.

En este caso, la única forma de acceder al equipo es a través de la interfaz consola (conexión serial).

Se recomenda mantener siempre un computador con acceso a la consola de la OLT Furukawa disponible para situaciones de emergencia.

Existen algunos concentradores de consola en el mercado que permiten el acceso serial a equipos de

red de forma remota a través de una LAN de gestión (*out-of-band*).

2.8 Configuración de un servidor de syslog

Se recomenda también configurar un servidor de *syslog* en la red de gestión para mantener actualizadas las informaciones de salud del sistema e identificar más fácilmente situaciones de riesgo.

Los sistemas operacionales Linux ya poseen servidores de *syslog* embarcados, por lo tanto no necesitan de aplicaciones extras para implementación del servidor de syslog.

Para los sistemas operacionales Windows recomendamos:

1 – KIWI Syslog Server for Windows

http://www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx

Software pago. Existe una versión gratuita pero para apenas 5 equipos.

2 – Aonaware Syslog Daemon

http://www.aonaware.com/syslog.htm

Software libre. Es necesario instalar el Microsoft SQL Server 2005 o superior en el servidor que tendrá el servidor de *syslog* instalado. Es bastante simple y no posee herramientas para filtrar/analisar las informaciones, todavía es una solución robusta del punto de vista de almacenamiento de los logs en base de datos.

3 – Syslog Server

https://sourceforge.net/projects/syslog-server/

Software libre.

3 Conclusión

Las informaciones presentadas en esta Nota Técnica visam auxiliar en la identificación y en la mitigación de efectos indeseados en redes GPON cuando sometidas a inundación de paquetes de datos.

El uso combinado de las funcionalidades Source MAC address Monitoring y Loop Detection es indicado como mecanismo eficiente de detección, bloqueo y localización de *loops* L2 en las interfaces de usuarios de redes GPON utilizando OLTs GPON FK-OLT-G2500, FK-OLT-G8S o FK-OLT-G4S.

Para mayores informaciones sobre las funcionalidades presentadas ou aclareo de dudas técnicas pesquise la documentación del producto o abra un ticket por la liga abajo:

http://suporte.furukawa.com.br