GOOD PRACTICES TO AVOID UNAVAILABILITY OF SERVICES IN GPON NETWORKS

1 *Loop* Risk Situations

A common vulnerability situation which data networks are subjected to is packets *loop.* A *loop* is characterized by the existence of two distinct physical pathways at the interconnection between network elements that causes an unwanted flow of packets by constantly entering and returning to the original path. This flow may reach a point that causes a total unavailability of the network.

The utilization of the *Gigabit Passive Optical Network* (GPON) technology in *enterprise* networks minimizes the possibility of *loops Layer* 2 (L2) occurrences in the network, given the reduced quantity of active equipment and well-defined functions of the *Optical Line Termination* (OLT) and *Optical Network Unit* (ONU). To the network termination equipment PON, ONUs, it is recommended, for example, connecting only user's terminal equipment, condition that, if followed, would not result in L2 *loops*.

However, a GPON network is not free of connection errors or unauthorized *Access Points* (*Rogue APs*) connections or *switches* L2 to the ONUs. For these cases, it is important that the Laserway projects solution consider the configuration of a loop *avoidance* protocol according to the recommendations and considerations described in this document.

In GPON topologies using Furukawa's OLTs, there are two situations where there is a *loop* vulnerability: connection between ONTs ports connected to the same OLT and connection between ONTs ports connected to distinct OLT ports.

1.1 Same OLT port

A logical *loop* may be caused by the connection between two ONTs ports connected in the same OLT (figure 1), or by the connection between two ports of the same ONT (figure 2) if, and only if, the connected interfaces belong to the same VLAN and the OLT port have the *port*-bridge functionality enabled.

The *port-bridge* functionality is normally used in enterprise networks and allows the communication between computers or IP telephones that work in ONTs that belong to the same OLT.

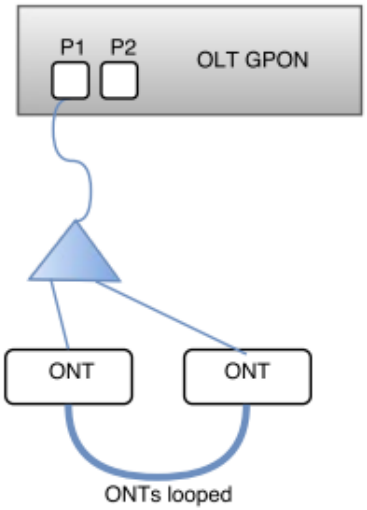

Figure 1 – ONTs connected between themselves belonging to the same OLT port (P1)

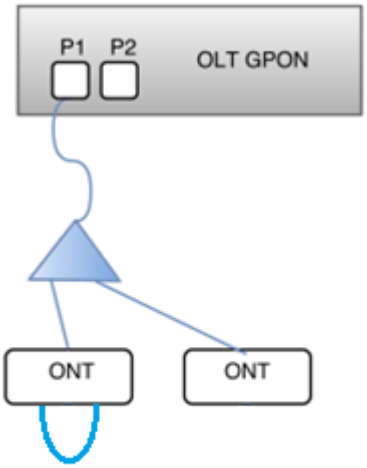

Figure 2 – ONT ports connected between them

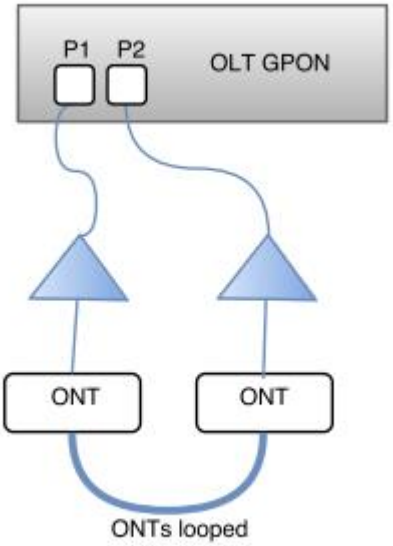

Figure 2 - ONTs connected between them belonging to distinct OLT port (P1 and P2)

1.1.1 Port-bridge

The Furukawa's GPON OLTs support the *port-bridge* layer 2 functionality (L2), which allows the forwarding of packets to the same interface that originated it. When the destination MAC address is found, the packet is forwarded normally, even if in the same origin OLT port.

An alternative to the *port-bridge* is the configuration of the *ARP alias* functionality.

1.1.2 ARP alias

To allow communication between specific *hosts* that are connected to the same OLT port, Furukawa's GPON OLTs support the *arp alias* command, which makes the concentration switch to respond to the OLT clients ARP requests.

1.2 Distinct OLT ports

The formation of a *loop* is possible connecting ONTs that belong to distinct OLT ports but are working under the same VLAN scheme. In this case, the *loop* occurs between the OLT port and it is recommended to enable a *spanning-tree* mode to avoid the phenomenon.

1.3 *Loop* Identification

The first register that must be checked for identifying any problem (*troubleshooting*) with the GPON OLTs is the equipment *syslog*.

Check the OLT syslog through the following command:

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

Loop events may be identified by syslog entries such as the following:

```
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 Recommended configuration

To diminish the undesirable effects caused by the *loop* it is recommended to aggregate to the system the configurations that follows in this chapter.

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

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

The functionality *Source MAC address Monitoring* (SRC-MAC-MON) allows the OLT to identify problematic ONUs through analysis of the source MAC address of the received frames (SRC-MAC). In case the OLT identifies a frame which the SRC-MAC is equal to the OLT system MAC, characterizing a L2 *loop*, the ONU that sent the *frame* is then blocked.

The unblocking of a *looped* ONU may be configured to occur in an administrative way or automatically, based in temporization (*expire-timeout*). In case the unblock automatic mode is used, it is recommended to set the timing to at least 300 seconds in order to allow the removal of the physical *loop*:

srcmac-monitor configuration in the interfaces PON 1 and 2 of the OLT: automatic unblock in 300s:

```
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
```

Configuration of the srcmac-monitor in the interfaces PON 1 and 2 of the OLT: manual unblock:

```
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
```

Verification and manual unblock of the ONU:

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

The efficiency of the functionality SRC-MAC-MON on the identification and blocking of loops depends on the generation of frames by the OLT, capable or circulating the entire L2 network. The functionality *Loop Detection* described below needs to be configured in the PON interfaces that needs to be protected in order to assure the periodic generation of *frames* for MAC monitoring.

2.2 *Loop Detection* (LD)

The functionality *Loop Detection* (LD) allows the configured interfaces to send *broadcast loop-detect frames* periodically, which the SRC-MAC is the OLT

system MAC address. The interfaces, then, monitor the reception of these *frames* also identifying the *loop* condition, but not blocking, by *default*, the involved interfaces. This way, it is possible to combine the SRC-MAC-MON and LD functionalities in the PON interfaces in order to identify and block selectively just the ONUs involved in the L2 loop condition.

By using f*rames broadcast*, the LD does not depend on any additional configuration on connected equipment to the ONU access; STP for example. The *broadcast loop-detect frames* are sent to all associated *bridges* to the OLT PON interfaces, including *untagged frames* in case the interface is configured to do so.

In order to assure the *loop* detection efficiency, the period to send the *loop-detect* frames (*period*) must be tuned to 3 seconds.

The LD functionality, even configured only to identify a *loop*, despite not blocking the interface, utilizes a timing to initiate a new *loop* detection (*timer*). This way, considering the *loop* detection in the PON interface, the detection time controls the minimal interval between *loop* detections in ONUs on the same PON interface. Due to this, the detection time must be set to 5 seconds.

loop-detect configuration on the PON 1 and 2 interfaces of the OLT: send interval of 3s and detection time of 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 Monitoring and locating *loops*

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

Example of log showing a loop between the 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
```

Example of log of the automatic blocking of the ONUs (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* may be redirected to a remote *Syslog* server through the below command.

Redirecting of the log to a remote Syslog server:

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

Example of log in the Syslog 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 possible to verify the blocking state of the ONU through a CLI command.

Blocked ONU (1,2) verification:

```
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 Scenarios of loop protection supported by the SRC-MAC-MON and LD

As mentioned, the LD does not depend on any additional configuration in the equipment connected to the ONU access for *loop* detection, as it uses *broadcast* frames. This way, there are no known scenarios where the combination SRC-MAC-MON and LD cannot identify and block ONUs with access in *loop*. This recommendation does not consider redundant architecture of connection in the OLT uplink, being necessary to evaluate the usage of xSTP or *Link Aggregation Group* (*LAG*) in these conditions.

2.5 Broadcast storm-control

This functionality allows controlling the effect of massive transmission of broadcast and multicast packets.

It is possible establishing a maximum rate of packets to be processed per second in a specific OLT interface.

2.6 Spanning-tree

Check the session “Spanning-tree protocol (STP)” of the user manual to configure the desired spanning-tree mode and avoid the logical loop of packets between OLT ports.

2.7 Serial access

In some situations, an event of denial of service (DoS) like the ones generated by *loops* may stop the network management access of the equipment (telnet / SSH) and prevent the collection of information and configuration.

In this case, the only way to access the equipment is through the console interface (serial connection).

It is recommended always to keep a computer with access to Furukawa’s OLT console available for emergencies.

A few console concentrators in the market allow remote serial access to network equipment through an administration LAN (*out-of-band*).

2.8 Configuration of a syslog server

It is recommended to also configure a syslog server in the administration network to keep the system's health information updated and identify more easily situations of risk.

Linux operational systems already possess embedded syslog servers; therefore do not need extra applications for the implementation of the syslog server.

For Windows operational systems, we recommend:

1 – KIWI Syslog Server for Windows

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

Payed software. There is a free version but for only five equipment.

2 – Aonaware Syslog Daemon

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

Free software. It is necessary to install the Microsoft SQL Server 2005 or superior in the server where the syslog will be installed. It is very simple and does not have tools to filter/analyze the information, however it is a robust solution in the logs storage in databases point of view.

3 – Syslog Server

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

Free software.

3 Conclusion

The presented information in this Technical Note intend to help to identify and mitigate the undesired effects in the GPON network when submitted to a flood of data packets.

The combined use of the Source MAC address Monitoring and Loop Detection is indicated as an efficient mechanism of detection, blocking and localization of L2 loops in the GPON network user interfaces using OLTs GPON FK-OLT-G2500, FK-OLT-G8S or FK-OLT-G4S.

For more information about the presented functionalities or clarification of technical doubts, search the product documentation or open a ticket in the address below:

http://suporte.furukawa.com.br/formulario