Security for PON Business Services

White paper

To be successful in offering business services, security is key. As a shared medium, PON uses multiple methods to separate, encrypt and secure data on the network to provide mission critical security on a par with dedicated point-to-point connections. This paper explains the various methods involved.

Authors: Yannick Sillis, Aravindan Jagannathan

Contents

Introduction

The commercial availability of high capacity 10G PON and 25G PON technologies presents fiber broadband network operators with new opportunities in wholesaling, convergence and especially business services.

A single high capacity PON infrastructure can comfortably support requirements for business services with guaranteed SLAs alongside mobile backhaul and premium tier residential services. This allows operators to significantly reduce costs and create a competitive advantage through more attractive pricing.

Security considerations

To be successful in offering business services, providing secure connectivity is key.

PON has a point-to-multipoint architecture, where one fiber is split to serve multiple users. But if multiple users share one fiber, how secure are point-to-multipoint networks? The PON standards have put a lot of effort in defining the features that will ensure the security of data transferred over a PON. This enables operators to benefit from a more cost-efficient solution to connect everyone, while at the same time offering mission critical security for their customers.

Let's explore possible security concerns, and how PON technology solves them.

In the upstream direction (from user to the network), a user's modem (called an ONU) sends the traffic only in one direction—to the fiber access node (called the OLT). The signal is not reflected back into the network, for example from splitters or OLTs, because these devices are designed and manufactured to reflect almost no light. So, it is not possible for traffic sent by one ONU to be intercepted by another ONU.

In the downstream direction, which is from the network to the user, the OLT sends traffic towards all ONUs. But it doesn't mean that ONUs can read the data intended for other users. In a PON, every packet is labeled, and an ONU can take in only the packages that are intended for it.

In order to interfere with traffic on a PON (either to intercept or transmit), a malicious user would need to insert an ONU (or other listening device) either before or after the splitter, or replace the splitter itself with a highly reflective one that would reflect back to malicious or legitimate ONU.

All of this is extremely difficult to do undetected because of the physical nature of a fiber optic network. Any device introduced on the network needs a physical connection, which will disrupt signals in the network and should trigger an alarm. In addition, even if it were possible to manufacture a highly reflective splitter, their locations (typically underground or in hard-to-reach sites) are not publicly known.

However, "extremely difficult" is not the same as "impossible", hence PON networks use multiple methods to separate, encrypt and secure data on the network to provide end-to-end, mission critical security on a par with dedicated point-to-point connections (which, of course, have the same susceptibility to maliciously inserted listening devices).

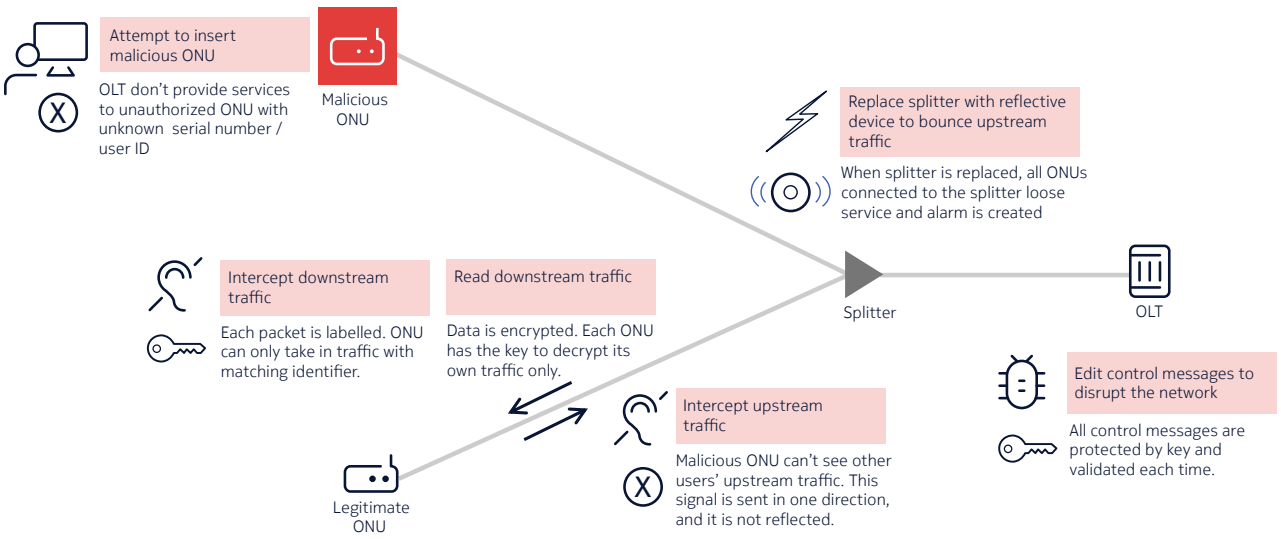
PON security features

PON networks use multiple security features to:

- Isolate traffic for each user
- Encrypt data traffic
- Prevent unauthorized devices being connected
- Validate control messages

These security features rely on the packet structure used in PON data transmission. Each packet of data is comprised of the payload (the user information being transmitted) and a header comprising information about the transmission (such as its length, origin, and destination) and security information (encryption keys, timeslot codes, etc.).

Figure 1. PON security features ensure mission critical data protection



User isolation

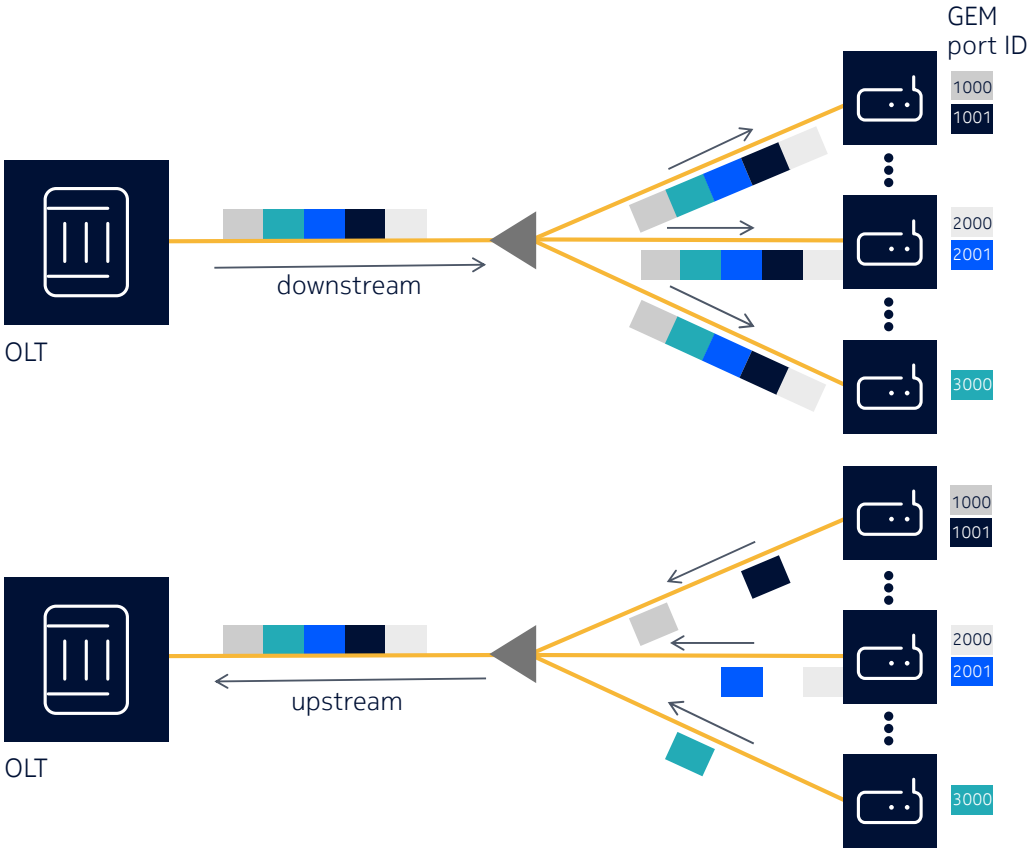
Every ONU receives all downstream data from the OLT. This raises the potential of someone attempting to read the downstream traffic meant for another user.

PON technology uses the Gigabit Encapsulation Method (GEM), which is a label in the header, to isolate traffic for each user. For downstream traffic, GEM tells ONUs which packet is for it, and for upload traffic it tells the OLT from which user or service that packet originates.

In downstream transmission, while an ONU will receive data packets for all subscribers, it is only able to take in those packets in a matching identifier in the GEM. A malicious ONU on the network will not have been provisioned with a recognized GEM identifier and, therefore, is unable to take in any packets.

In upstream transmission, each ONU transmits directly to the OLT in assigned timeslots. The upstream data is not reflected back from the OLT or the passive optical splitter, so other ONUs cannot listen in to upstream traffic. If a malicious ONU is somehow inserted in the network without triggering an alarm, it will still not be recognized in the OLT's provisioning database and will not be granted timeslots to send its data.

Figure 2. User Isolation on a PON



Traffic encryption

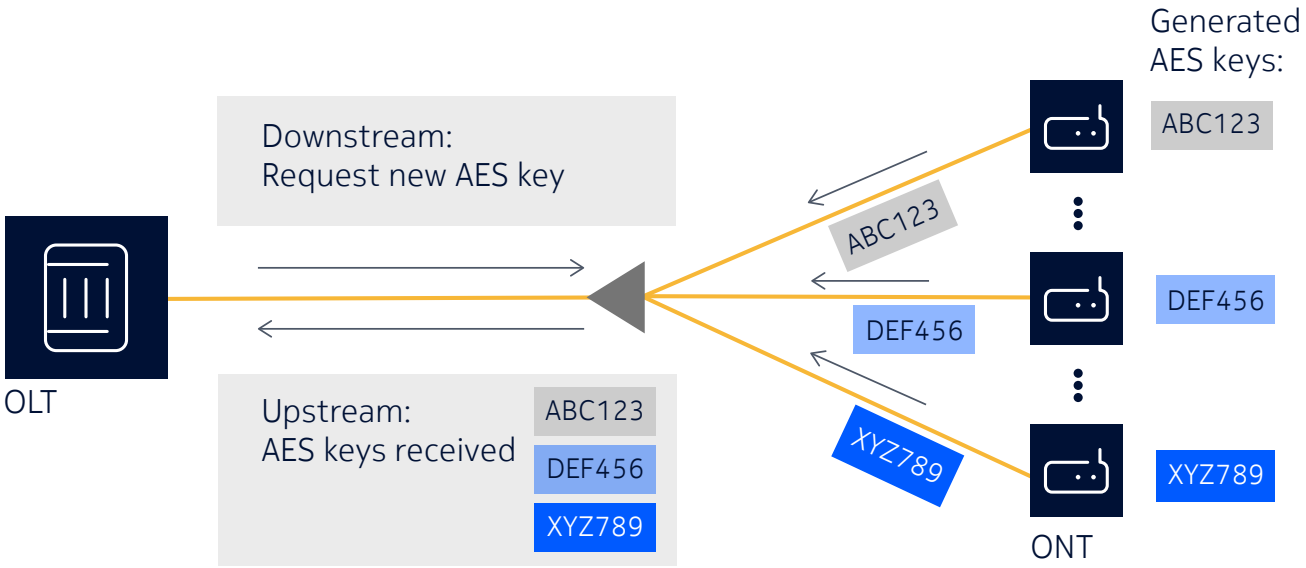
In addition to separating the data for each user, the data itself is protected by encryption.

PON networks use the well-known Advanced Encryption Standard (AES) security algorithm to encrypt data packets. All packets coming from or to an ONU are encrypted with the key, which is only known by that ONU and the OLT.

Encryption keys are generated by each ONU and sent upstream to the OLT. They are periodically refreshed (e.g., hourly, daily) depending on the network configuration. As previously mentioned, traffic is not mirrored back into the network, so other ONUs cannot intercept the keys (also the encryption keys are themselves encrypted when sent).

Encryption is applied to both the data payload and the GEM payload, providing an additional level of security, so GEM frames cannot be read even if intercepted.

Figure 3. AES Encryption prevents eavesdropping



User activation

PON has a user activation procedure that prevents unauthorized devices being connected. Each ONU has a unique serial number and registration ID. The serial number is set in the factory and is hard-coded in the ONU hardware; the registration ID for each new subscriber is assigned by the operator and set in the ONU when it is installed.

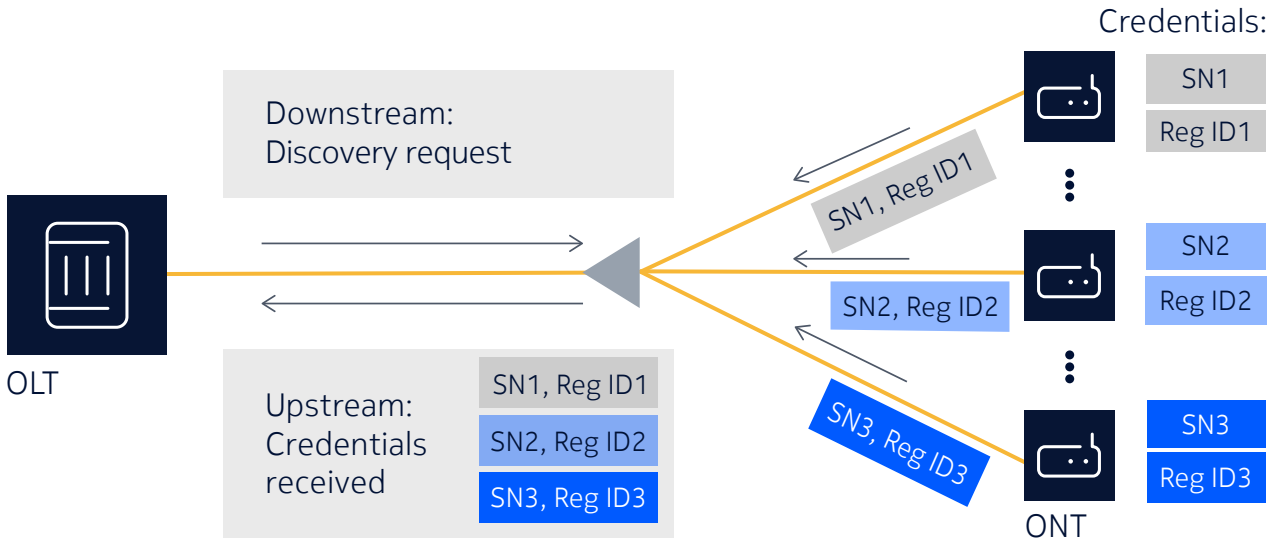
The serial number and registration ID are also programmed by the operator in the provisioning data, so the OLT knows upfront all the ONUs that are supposed to receive service.

When an ONU is introduced to the network, the provisioning process checks the authenticity of these codes: the OLT requests the codes from the ONU and checks that they match as expected. The codes are delivered upstream, so they cannot be intercepted by another ONU.

A maliciously introduced ONU will not have a correct combination of serial number and registration ID; therefore, the OLT will not provide any service to it.

As with any security mechanism, humans are the weakest link. It is possible that someone could get hold of the serial number and registration ID of a legitimate ONU in the network. However, this is as difficult as getting someone's password or other confidential information, because it requires physical access to the legitimate ONU to read the serial number, log in to ONU's local interface, or get hold of the letter or mail to retrieve the registration ID.

Figure 4. User Activation prevents unauthorized ONUs from accessing the PON



Message integrity

In a PON, an ONU is activated, configured, managed, and monitored by the OLT. A malicious user may attempt to generate, replicate, or edit control messages that could cause service disruption. For example, a malicious user may attempt to generate network alarms (e.g., a LAN loss alarm) that would trigger a service outage.

Message integrity checks (MIC) are used by OLT and ONUs to verify that the downstream and upstream control messages come from a legitimate source and that they have not been tampered with. In downstream, a MIC is generated and inserted by the OLT when a message is transmitted and checked by the ONU when received. In upstream, a MIC is generated and inserted by the ONU when the message is transmitted and checked by the OLT when received.

For every ONU there is a dedicated set of keys used to generate the MIC. These MIC keys are calculated by the OLT and ONU independently, based on information bidirectionally exchanged during the ONU activation process, such as the ONU serial number and registration ID. Hence, only the OLT and the ONU have all the information needed to generate and validate the MIC for control messages related to that ONU.

MICs are executed in the control layer and are a protection against a malicious user trying to disrupt a network, rather than steal data from it.

Conclusion

The four security features explained in this paper combine to deliver mission critical security in PON networks. User traffic is protected by AES encryption. Control messages are carried in the GEM code, so are also encrypted. On top of that, there are message integrity checks. Combined, they provide maximum protection against data being intercepted as well as maximum protection of the data itself.

The level of security in a PON is the equivalent of the security level provided in any SLA for a point-to-point broadband service. This clears the way for operators to confidently embrace PON to deliver business services and take advantage of 10G PON and 25G PON to converge services, reduce costs, and drive new revenues.

Abbreviations

AES	Advanced Encryption Standard
GEM	Gigabit Encapsulation Method
MIC	Message integrity check
OLT	Optical line terminal
ONU	Optical network unit
PON	Passive optical network
SLA	Service level agreement

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (February) CID210711