Global Information Assurance Certification Paper

Comparative Risk Analysis Between GPON Optical LAN and Traditional LAN Technologies

GIAC (GSEC) Gold Certification

Author: Jason Young, jason.n.young@silverbulletsecurity.com
Advisor: Antonios Atlasis

Accepted: 24 October, 2013

Abstract

Today's digital frontier can be described as the new Wild West with untested cutting-edge technologies finding their way into the public domain. With increased interest in Gigabit Passive Optical Networks (GPON) to provide LAN access, one question must be asked. What is the risk? Risks associated with traditional Ethernet LAN technologies are well known and documented. As is common with new technologies, risk from failures or exploits may not be realized until after implementation is complete. In many cases, risk assessments are pushed to the side with focus on quick implementation and costs savings as they take precedence. Using a traditional Cisco Ethernet LAN Infrastructure to provide a baseline, we will compare known risks to a comparable set of GPON systems provided by Envistacom.

1. Introduction

Gigabit Passive Optical Networks or "GPON" as promoted by vendors like Tellabs and Zhone Technologies operates quite differently from traditional Ethernet when providing LAN communications in a fiber to the desktop (FTTD) architecture (Tellabs, n.d.b). These differences will determine increases or decreases in risk to LAN environments. As GPON has been used in many other applications, the most commonly known would be Verizon's FIOS. Verizon's FIOS is a fiber to the home (FTTH) architecture which provides basic voice, video and data services via direct fiber communications links (BroadbandSoHo, n.d.). In initial research, it became apparent that comparisons between GPON FTTD implementations and traditional LAN technologies focused mainly on Cisco and Tellabs (Lippis, 2012; Tellabs, n.d.a). As is normal in information technology, many of these comparisons were biased towards one vendor, and generated favorable outcomes by choosing certain models and configurations. With that in mind, this risk assessment will not address issues such as performance or cost analysis, but analyze risk to systems in their basic configurations. It must be understood that this analysis will raise as many questions as it answers, and these questions should be pursued, tested, and validated to appropriate conclusions.

This evaluation will focus on risk posed to basic enterprise LAN communications from the distribution layer to the access layer for the GPON FTTD architecture. This risk assessment will not analyze risks to individual vendor systems, such as those that would be normally provided by a security scan, or a penetration test. This is meant to provide the initial look at the technology laying the groundwork for those types of activities to begin.

2. GPON FTTD Architecture

In GPON, there are three main components that provide communications from the distribution layer to access layer in a basic FTTD LAN configuration. This would be the Optical Line Terminal (OLT), Optical Distribution Network (ODN), also called the Optical Network Unit (ONU) in some cases, and Optical Network Terminal (ONT)

(Hoover, 2012). A GPON FTTD example, starting from the distribution layer to the access layer, would be the use of a Tellabs 1150 OLT and a Tellabs 120W ONT connected via 2:32 ODN as seen in Figure 1.

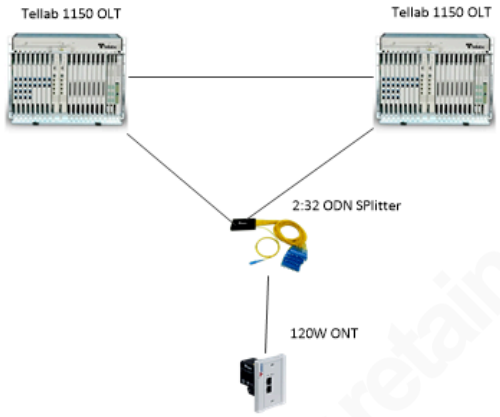

Figure 1. GPON FTTD LAN. Adapted from "Tellabs GPON Optical LAN," by Michael S. LaVallee & Jerry Stilp, (2012), p. 29. Copyright 2012 by Envistacom LLC. Adapted with permission.

The first device at the distribution layer is the OLT. The OLT is the brain of the GPON FTTD LAN, and provides the same functions of the layer three switches within the Cisco architecture plus more. This larger role is due to the nature of communications between the OLT and the ONT. All downstream communications from the OLT to the ONT is broadcast via TDM (Time Division Multiplexing), while communications upstream from the ONT to the OLT is TDMA (Time Division Multiple Access) (Cale, Salihovic & Ivekovic, 2007). The OLT not only routes all data between VLANs, but also manages communications between systems within the same VLAN. Failover, quality of service, port security and VLAN assignment are controlled at the OLT (Zhone Technologies, 2012a). There are exceptions to this as depending on the ONT which will be covered later. Generally speaking, the OLT centralizes all network activities including management and security to one central point. With these basic changes in network management, advantages and disadvantages will be discovered as analysis of communications between Cisco LAN and GPON FTTD are conducted.

The second device connecting the ONT to the OLT is the 2:32 ODN splitter. The ODN splitter is roughly the size of a cell phone and is a passive device which has no

management, switching or routing capabilities (ITU-T, 2008a). It serves the same function as a layer two switch at the access layer in the sense of providing a communications link from the distribution layer to the access layer. Think of the ODN splitter as connecting multiple access layer ONT systems to the distribution layer OLT systems.This could be a topic of discussion as one splitter can have more clients than a switch, or vice versa, but in theory they perform the same function.

The third system providing communications to the access layer is a Tellabs 120W ONT. ONT systems vary greatly depending on the type of Fiber to the x (FTTx) architecture used. Other examples not yet covered would be fiber to the premises (FTTP) or fiber to the node (FTTN) (Hayes, 2006), but the Tellabs 120W in Figure 1 represents a suitable ONT for FTTD LAN communications. FTTD architectures are different in that they provide a centralized end-to-end managed solution through the OLT and software like Panorama Integrated Network Manager (INM) (Tellabs, n.d.b). Other installations like a SOHO (Small Office Home Office) may implement an FTTH configuration using an ONT that operates independently from the OLT. For example a Zhone Technologies zNID-GPON-2426 ONT provides DHCP, wireless access point services, access control lists, and a few other services to local management (Zhone Technologies, 2012b). In short, requirements dictate the type of ONT used for network connectivity. For this evaluation of an FTTD LAN, the Tellabs 120W is a suitable device.

Other systems that support the GPON architecture in Figure 1 are the bulk rectifier and power distribution unit (PDU). Two bulk rectifiers are used with battery backup, and installed in a failover configuration to provide redundant power sources. Their main function is to provide power via the PDU to the ONT systems. The PDU in turn provides power to 32 ONT systems, and is 1 Rack Unit (1RU) in size. It is installed in the same location as the splitter typically in a ceiling zone box to save space. Finally ONT systems run on 48Vdc with power provided via a fiber/copper cable solution used by GPON (Hoover, 2012).

3. The Test Environment

For performing a comparative analysis, Cisco was chosen due to its large presence in the networking world. When deciding how to compare the two technologies, several questions were posed to create an appropriate test environment.

- Which equipment is comparable to the systems in Figure 1 for providing LAN services in an enterprise LAN environment?
- If Layer 2 communicatoins is done at the OLT, how does that impact the risk posed to the system?
- Does losing a 2:32 Splitter impact the network more than losing a Cisco access layer switch?
- Does the use of the ONT devices in areas accessible to unauthorized personnel greatly impact security?
- How intelligent are ONT devices, and what services or security do they provide to the end user?
- Given that an intruder has gained elevated access to an authorized system, what traffic will they see when sniffing using Tcpdump or Wireshark?

To create a comparable configuration to match our GPON systems from Figure 1, an example would be two Cisco 4500 series layer three switches providing services to clients at the access layer using Cisco 2960 series switches. The Cisco 4500 series switches at a minimum, but not limited to, would provide layer three routing of packets between VLANs, Hot Standby Router Protocol (HRSP), and serve as the VLAN Trunking Protocol (VTP) Servers. The Cisco 2960 series switches would provide access and extend security services such as port security to client systems (Odom, 2012).

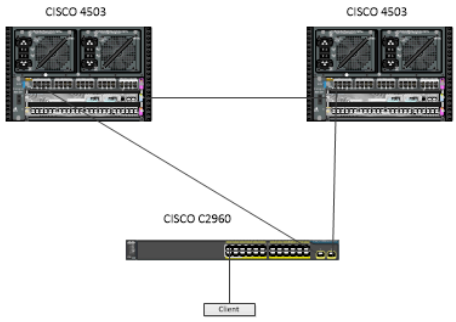

Figure 2. Cisco LAN

To simulate the environment for Figures 1 and 2, and answer our questions about layer 2 communications and ability to see network traffic with Wireshark or Tcpdump, the following test environments were created for GPON and Cisco: Two VLANs were created for capturing data traffic, VLAN 20 (172.16.2.0/24) and VLAN 30 (172.16.3.0/24). One final VLAN was created as a default gateway, VLAN 10 (172.16.1.0/24). GPON equipment used consisted of two Zhone MXK-194 OLTs, one N-Lightened NRMS-2-32 ODN splitter, and two Zhone zNID-GPON-2426-NA ONTs in the following configuration by Envistacom with the OLT providing network management.

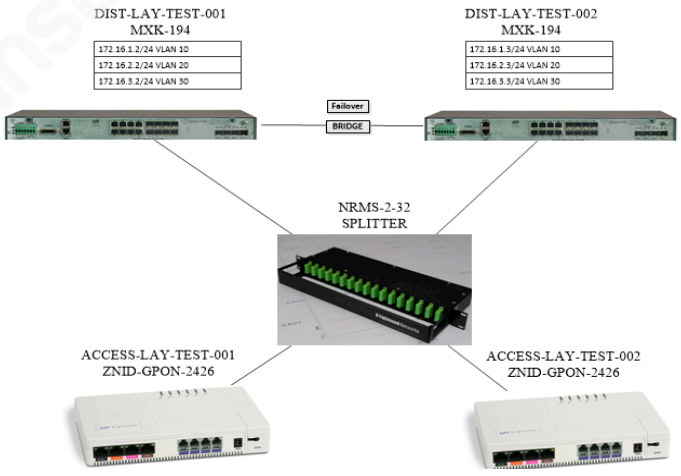

Figure 3. GPON Test Environment

The Cisco configuration consisted of two Cisco 3560 switches using HSRP standby for redundancy using ipservicesk9-m IOS to simulate the distribution layer. The access layer was simulated by two Cisco 2960 switches with a base IOS.

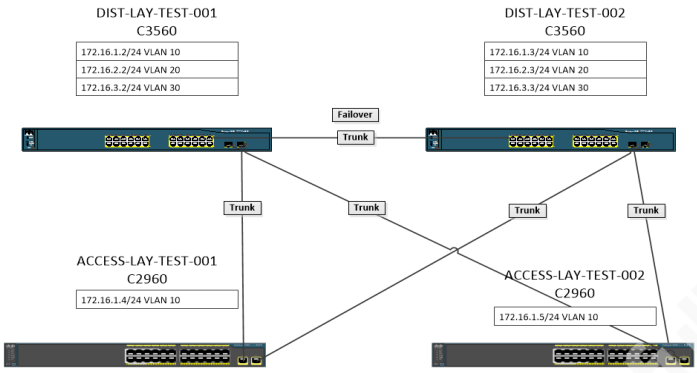

Figure 4. Cisco Test Enviroment

Three client systems were used within the test to generate, receive, and capture traffic for evaluation. Both systems used to generate and receive traffic were clean Windows 7 systems with Nmap installed for the test. The system used for the data capture was Ubuntu 12.04, and the following IP addresses were used for the three tests.

Client	Role	Test 1 IP	Test 2 IP	Test 3 IP
Client1	Generate traffic	172.16.2.4	172.16.2.4	172.16.2.4
Client2	Receive traffic	172.16.2.5	172.16.2.5	172.16.2.5
Client3	Capture traffic	172.16.2.6	172.16.3.4	No IP

Table 1. Client System Test Environment

These environments were created given a basic configuration for a small LAN enviroment. As a note, it must be understood that this is not a one size fits all, and depending on requirements and different types of architectures, the findings in this risk assessment may not be valid for all GPON FTTD or Cisco implementations.

4. Traditional Ethernet LAN VS GPON LAN

4.1. Internal LAN Communications

With the question of how and where layer two and layer three communications are done within the GPON FTTD LAN, we begin with the OLT. Like Cisco, the GPON OLT uses 802.1Q for VLAN provisioning, but all communications within or routing between VLANs is performed at the OLT. VLANs must be provisioned at the OLT device before the systems will send or receive traffic to devices on the ONTs (Zhone Technologies, 2012a). The primary difference between Cisco and GPON is switching.

Cisco's layer two switching protocols govern the primary path between switches and allow direct communications between clients. For example within a Cisco network, packets are forwarded to their destination over the root bridge determined by protocols such as STP (Spanning Tree Protocol) (Odom, 2012). GPON does not use any switching protocols between the OLT and ONT. The OLT broadcasts all traffic downstream to all ONT devices and the ONT devices in turn communicate directly with the OLT via TDMA. This means that every ONT system sees all traffic downstream, but only their specific traffic is sent upstream. This is drastically different from a distributed Cisco environment where devices can use the switched network within the access layer to communicate directly.

The obvious question with this method of communications is the ability to eavesdrop. The initial safeguard that GPON FTTD employs is the use of AES 128bit encryption to downstream traffic for confidentiality (ITU-T, 2008b). To break this encryption method in theory, an attacker must capture the upstream key exchange on the same splitter (above the ODN) or port (below the ODN) (Brenkosh, Roybal, Amberg, Heckart, & Vaughan, 2012). Though Cisco and GPON use wavelengths of 1310 nanometers upstream and 1490 nanometers downstream, Cisco uses protocols that support 802.3 Ethernet (Cisco Systems Inc., n.d.a), while GPON uses protocols that support ITU-T G.984 making them not compatible. This limits attackers to using vendor specific hardware such as a modified ONT device to capture the traffic. Simply using a media converter compatible with most switch vendors including Cisco in a traditional network will not work. Another strong advantage of this encryption is it is enabled by default, and does not require interaction by administrators for individual ONT systems. Cisco by contrast uses TrustSec MACsec 802.1AE with AES 128bit encryption on newer devices to protect from eavesdropping on communications. One drawback with Cisco is it is not available with LAN Base IOS versions, or most legacy equipment (Cisco Systems Inc., n.d.d). Unlike the GPON OLT, management of the MACsec could become a daunting task as enterprise networks would be comprised of a mix of systems that do and do not support it. Though the upstream communications for GPON are in the clear, the risk may not be as high as a Cisco trunked port sending data in the clear. For example,

a link between the ONT and Splitter would allow an attacker access to the data on that individual ONT. In theory, this is the same as an attacker gaining access to an individual port on a layer two switch. If the attacker was to gain access to the uplink from the splitter to the OLT, the risk would increase as access to all data from all ONT devices connected to the splitter would be visible. That would be the same as gaining access to trunked communications between a Cisco access layer switch and the distribution layer switch. GPON FTTD does however have physical medium and port security countermeasures that protect against this that will be covered in later sections. To validate proper communications at the ONT for VLAN data segmentation and to answer questions from the test environment section, the following three tests were conducted against Cisco and GPON in the test environment.

The first test consisted of connecting all three systems to VLAN 20. Once all systems were connected, Tcpdump was initiated on the data capture client3 system and a "clear arp" command was issued on the switches. This command was issued to force the clients systems to send an arp request. The last step was to start an Nmap scan using the following parameters (-T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389) to simulate traffic between client1 and client2. In the Cisco environment, client1 and client2 were separated by different C2960 switches, while in the GPON FTTD environment systems were connected to separate Zhone ONT devices. As would be expected in both the Cisco and GPON FTTD environment, the initial arp request was received by the data capture system.

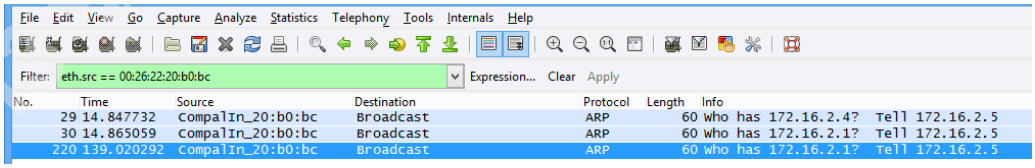

Figure 5. Wireshark Arp Packet Capture Test 1

In the second test, the data capture system was moved to VLAN 30. The rest of the test was performed exactly as the first. Within both the GPON FTTD and Cisco environment no data was captured between the two systems.

In both tests, standard network communications from the Cisco environment was captured. Within the GPON FTTD environment however, it was immediately noticed no network management traffic or switching protocols were seen. More specifically, no network communications between OLT and ONT systems were seen. This would be apparent when you think of the broadcast nature of the GPON system. Without these protocols being easily sniffed on the wire, it would make it much more difficult for an attacker to gather network information from a compromised system. Within the Cisco environment, common data such as ARP, CDP, HSRP, Loop, and STP was easily captured as seen in Figure 6.

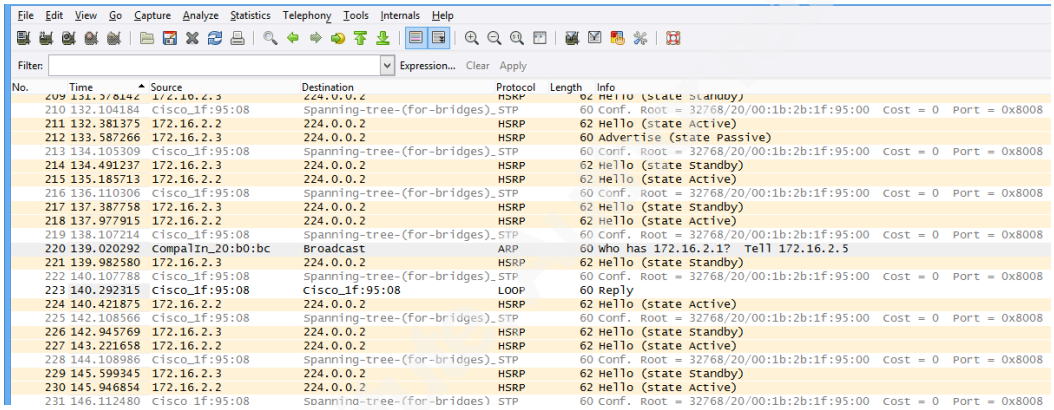

Figure 6. Wireshark Cisco Network Packet Capture Test 2

Though CDP can be disabled, and other data only provides basic knowledge of the network, there are risks involved. By comparison with GPON FTTD more security is available when no information can be gathered.

The last test conducted captured data on the trunked port between the access and distribution layer systems. During the test client2 generated traffic by pinging client1, the gateway 172.16.2.1, accessing http://yahoo.com, and conducting the same Nmap scan from the previous tests. All data from client2 was captured by client3 in the Cisco environment. Client3 was connected to the root bridge between the Cisco 2960 switch connected to client 2 and the primary Cisco 3560 switch. These data captures were easily done using an Ethernet or fiber connection. To eavesdrop on trunked port

communications, only a hub is needed to capture data on a wired port, while a hub and media converter are needed data captures as seen in Figure 7.

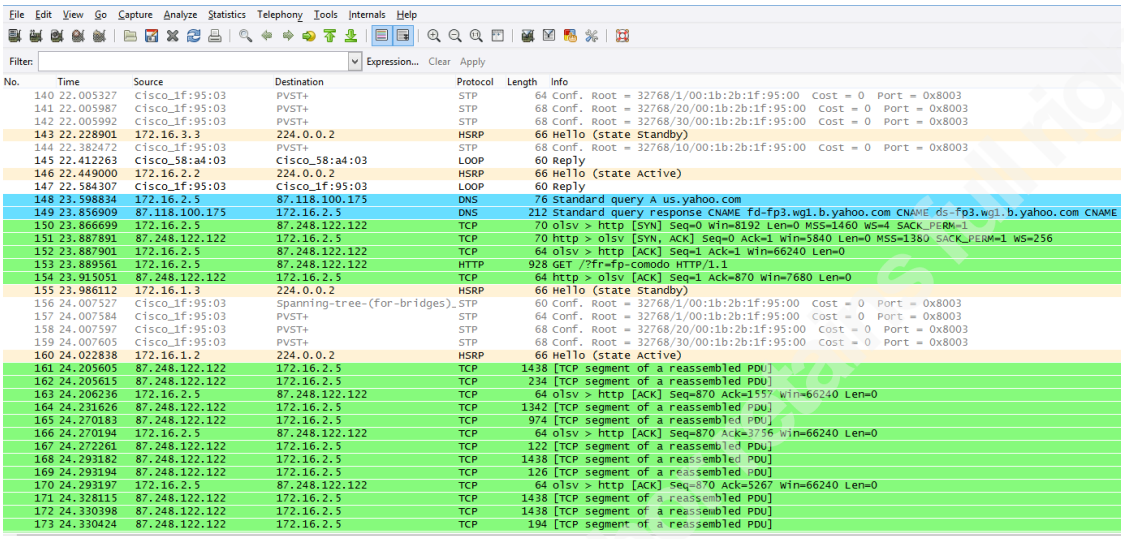

Figure 7. Wireshark Cisco Trunked Port Data Capture Test 3

If MACsec is implemented, then only encrypted traffic should be seen, but unfortunately the equipment used in this test did not support MACsec. One other advertised function of MACsec, is encryption can be extended to the client when supported. This would provide complete encryption of communications from the distribution layer to the access layer in the environment where all systems support MACsec.

Capturing data between the ONT and OLT was not possible during our test. Using media converters compatible with Cisco equipment do not work as the protocols are not 802.3 compliant, and use TDMA/TDM communications per the ITU-T G.984 standards for GPON as discussed earlier. It is to be assumed that one could possibly manipulate an authorized ONT, or spoof the Registration ID an existing ONT with a device capable of converting ITU-T G.984 communications to Ethernet for a data capture with Wireshark or Tcpdump. This was beyond the beyond the scope of this assessment and must be explored further as it is not yet proven.

4.2. Port Security

In discussing port security, it is better to break the systems down into two categories. Category one is distribution layer to access layer communications and category two is access layer to client systems communications. Port security for communications between the distribution layer and access layer are completely different between Cisco and GPON FTTD. In the Cisco environment, there is no difference between a trunked port and an access layer port with the use of 802.1x and MACsec. For GPON, the ONT is registered to the OLT via the registration ID (Reg ID). No network services are sent until the ONTs Reg ID is entered by an administrator at the OLT (Zhone Technologies, 2012a). In the event a rogue ONT connects and the device Reg ID is not recognized, an alarm is sent to the administrator by software like Tellabs Panorama Manager (LaVallee & Stilp, 2012). Though spoofing a serial number is theoretically possible, a separate test manipulating an ONT system needs to validate this. This however would be a difficult task to perform even with modified equipment due to the physical securities afforded to GPON FTTD that will be covered later with physical security.

Port security for GPON wired clients include radius based authentication for 802.1x, sticky MAC addresses and Network Access Control (NAC). With the exception of Cisco's MACsec when it is supported by both client and switch, port security for wired clients is relatively the same. Without the use of encryption to the client, eavesdropping is a risk for communications between the ONT to the client. Given that the ONT systems are installed in the same locations as the RJ45 jack would be installed for connection to a Cisco switch, there is no real increase in risk. Wireless examples like the zNID-GPON-2426-NA provide WPA2 Network Authentication and PSK (Zhone Technologies, 2012b), as do Cisco access points. Security of the access points however is more dependent on the authentication methods used and supported between the radius authentication server, wireless controller and access point, rather than the security provided by the LAN architecture model we are currently evaluating.

4.3. Systems Management, Security and Access Control Lists

Systems management for OLT systems, whether Zone or Tellabs function the same, and similar to Cisco in most respects. For example Zhone Technologies uses an out-of-band management port and can also be accessed via in-band IP address on bridged VLAN. Other Access methods for Zhone OLT systems are serial CLI, SSH, SFTP, or WebGUI (Zhone Technologies, 2012a). Network Management software includes Panorama Integrated Network Manager (INM) discussed earlier for Tellabs systems. Authentication can be controlled via radius or through the creation of local accounts. One unique advantage that Zhone Technologies uses is an automated profile for secure management activities restricting the management to SSH, SFTP, and HTTPS. These systems also support Digital Signature Algorithms (DSA) and RSA keys for authentication, while port-access for management activities is controlled when the secure profile is selected. This restricts access via access control lists to certain IP address, networks or MAC addresses (Zhone Technologies, 2012a).

Management of the ONT systems by an OLT is defined by ONT Management Control Interface (OMCI) per ITU-T G.988. Management specifications of the ONT from the OLT include how the ONT establishes and terminates connections, exchanges the Reg ID 10 digit number, and where supported use a system password that is matched between the OLT and ONT (Zhone Technologies, 2012a). During our validation, no communications between the OLT and ONT were visible by client systems. That being said, more research must be done on this area ensuring no exploitations may take place against the exchange of the Reg ID for the ONT. As it stands, access to the Reg ID information will be determined upon the ability to exploit the ONT system.

When looking at the differences between Cisco and GPON FTTD with respects to access controls lists, the largest aspect noticed was the centralization of GPON FTTD security controls. Within GPON FTTD, depending on the type of ONT used, access control lists are applied at the OLT (Zhone Technologies, 2012a). ONT systems that provide a robust set of network services can apply their own access control lists, like those used for SOHOs (Small Office Home Office). As stated in the beginning, devices like these are not necessarily used in the enterprise LAN configurations we are trying to

assess. GPON OLT systems use management software such as Zhone's Smart-OMCI to centralize all management for multiple OLTs simplifying this process (Zhone Technologies, 2012a). This however is matched by the many software packages for Cisco such as Cisco ACL Manager or even Solar Winds Network Configuration Manager (Cisco Systems Inc., n.d.e; Cisco Systems Inc., n.d.f). The real difference is that the OLT natively provides this support to the ONTs simplifying and centralizing the creation of access control from the beginning.

For the access control lists themselves, there are not vary many differences between the two competitors. In comparison with Cisco standard and extended ACLs, GPON OLT uses the IP based control lists by identifying the source and destination IP address (srip, dstip) with the source and destination port (srcport, dstport) (Zhone Technologies, 2012a). As with Cisco MAC ACLs, GPON also has MAC address control lists. GPON uses the srcmac command within their access control lists to apply restrictions to individual MAC addresses or groups of MAC addresses. For example "rule add deny 1/2 dstmac 12:34:56:78:91:23/24" defines the group of MAC addresses filtered by 24 bits (Zhone Technologies, 2012a).

4.4. Support

When it comes to supporting you environment, Cisco is the most well-known network architecture currently. Most network administrators start out learning Cisco, and almost all I.T. support firms provide Cisco support. When searching for answers to problems with Cisco on the internet, there is little you cannot find when you need to.

GPON by contrast does not match up to this. Even though GPON has been used for a significant amount of time for service providers like FIOS, there is still little in the way of support for FTTD LAN architectures. Finding support from a firm or by using search engines for information can be non-existent. In the research for this assessment simply finding configuration manuals for the systems used as OLT or ONT devices for GPON were difficult for some vendors to find. Zhone Technologies was the exception with extremely detailed manuals for installing, configuring and maintaining their systems (Zhone Technologies, 2012a). The risk in lack of documentation for these systems is apparent with support, for example in the event of a catastrophic failure of an OLT, less

experienced administrators may not be to restore communications. In situations where an administrator is not available in-house to the organization, it could be an extended amount of time before external support can be acquired if not contracted ahead of time. Though this is a risk, it is a risk that can be mitigated, and one that will surely decline over time as GPON FTTD gains more influence in enterprise networks.

4.5. Redundancy

As redundancy relates to GPON FTTD from Cisco, we compare it to Figures 1 and 2 previously shown. For example, when one Cisco 2960 switch connects to two layer three switches at the distribution layer using HRSP for failover, there is redundancy to the distribution layer with two layer three switches. In this configuration, if one Cisco switch or the link to the switch at the distribution layer fails, communications will continue to function. If the Cisco 2960 switch fails, all clients connected to that switch will lose connectivity. GPON FTTD functions in approximately the same fashion. You have two OLT systems connected with a 2:32 ODN splitter providing failover communications between the OLT devices. If one OLT systems fails, the second OLT systems will pick up communications without loss of service (LaVallee & Stilp, 2012). In the event that an ODN splitter fails, all clients connected to that ODN splitter will also fail. Note that this is the same in principle from a Cisco environment, but they differ here. In the GPON FTTD environment the ONT may have more clients than any one port on a Cisco switch increasing the risk with the number of devices dropped during an outage. If this is the case, one other option for GPON FTTD exists. This is called the Dual GPON MAC configuration where one ONT is connected to two separate 1:32 ODN splitters. The 1:32 ODN splitters then connect to two separate OLT devices (Hoover, 2012).

In a Cisco network, systems links are more distributed with the use of switching protocols. GPON is limited to two OLT devices using a 2:32 splitter, or two 1:32 splitters (Hoover, 2012). No more than two systems can be used for redundancy in GPON. Where the risk is lower in GPON FTTD is the advantage it has with managing devices at the OLT. In the event of systems failure, a Cisco switch that must be replaced must have a working baseline that is consistently updated with the current IOS, access control lists, and be installed by a qualified technician. The ONT and ODN devices do not require any

intervention by the technician that is installing them, and no preinstalled configurations. Replacing an ODN only requires the serial number for activation (Zhone Technologies, 2012a). In an environment where 802.1x is used proficiently with managed security profiles, this is a large advantage as OLT administrators can pre-program the serial number to reestablish communications quickly during an outage.

4.6. Climate Control and Environmental Risks

Depending on the environment in which systems are installed, climate control can be an extremely large risk. For example many manufacturing sector network installations are in environments extremely hostile to traditional networking equipment. Whether that is heat, cold, or humidity, the necessity of climate control increases risk to traditional networks systems from overheating, succumbing to moisture, or freezing. GPON eliminates the need for climate control on to the ODN and PDU in most situations due to their ability to withstand more environmental differences than a network switch. As the ODN is a passive device that requires no power and has no moving parts, temperature is not a real concern. For example the N-Lightened NRMS and NPDU are deployed together as a 2 RU solution to be installed in a ceiling zone box with an advertised temperature rating of -40 ºC to 80 ºC (N-Lightened Networks, n.d.), as compared to a Cisco 2960 which is rated for -5ºC to 45ºC (Cisco Systems Inc., n.d.b). For ONT systems, the Tellabs ONT 120W can operate within -5ºC to 50ºC, but this is the indoor version, and other ONT models are available when this requirement is exceeded.

Though much time has been devoted to environmental controls in this risk analysis, it must be understood that they play into the next section covered which is power. As power use and conversion generate heat, it affects the manner in which systems are housed and environmental controls needed. The main point here is that conversion from AC to DC power is done at the rectifier and not the PDU or ONT systems (Hoover, 2012). The PDU only transfers minimal amounts of power to the ONT systems reducing heat generated by the systems in tight enclosures.

4.7. Power

Power is always important when defining the risk to systems within an enterprise. With Cisco it is fairly straight forward, switches are installed in switch closets with two separate redundant power sources, a backup UPS or Cisco PDU. Other systems that use POE (power over Ethernet) connect to the switch via CAT5 or CAT6 cable. GPON FTTD however uses a much different and complex system. Starting with the ONT devices, they are connected via the PDU to a primary and secondary bulk AC/DC rectifier that provides power at 48Vdc. The large advantage with the centralization of DC power is the ability to provide redundancy and backup in the event of an outage to all systems that are part of the GPON network. A typical PDU provides 32 ports at 1.5A per port to the ONT systems for power (Hoover, 2012), and in the case of a dual GPON MAC configuration power is redundant at the ONT as well. The Tellabs 120 ONT observed uses 48Vdc power with backup batteries installed locally and provides 15W of POE to external systems (Tellabs, n.d.c). Power to the ONT is in a single fiber/copper cable that is daisy-chained from ONT to ONT as seen in Figure 8 below.

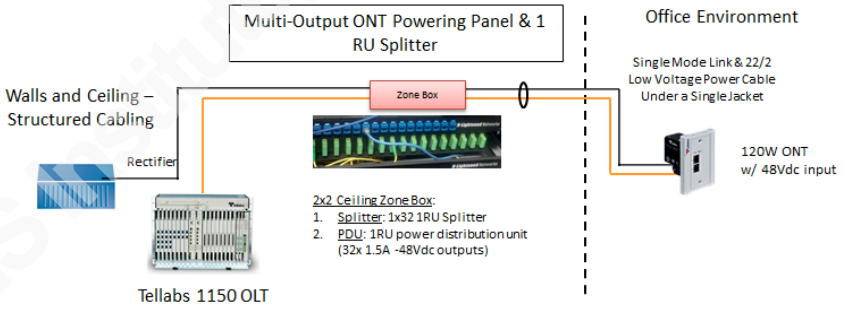

Figure 8: GPON FTTD Power Architecture Adapted from "Tellabs GPON Optical LAN," by Michael S. LaVallee & Jerry Stilp, (2012), p. 24. Copyright 2012 by Envistacom LLC. Adapted with permission.

One risk that comes from this configuration is the daisy-chaining of the ONT devices. If there is a break in the line, all ONT devices behind the break will lose power unless using the Dual GPON MAC architecture. The benefits to a distributed power system are clear when mitigating risks posed client systems and not just critical ones.

4.8. Physical Security

In evaluating the physical differences between Cisco and GPON, it was a general finding that elimination of Ethernet wired cabling and storage areas for access layer switches improved security from the distribution layer to the access layer within GPON FTTD architecture. To expand on why this is possible, the ability to gain access and eavesdrop on communications between the OLT and ONT is much more difficult. The main security advantage that GPON has over its Ethernet competitor is Secure Passive Optical Networks (SPON) (Hoover, 2012), that use alarmed fiber solutions like the Network Integrity Interceptor (NIS). NIS learns the environment such as the shutting of doors, or vibrations from production equipment, then sends alerts or can even shut down an ONT or a zone of ONTs in the event of a perceived attack. NIS uses 4 zones to break down an area on any alarm point for an OLT (LaVallee & Stilp, 2012). It is unknown however the number of false positive and potential for denial of service. Further research on this area is recommended as the potential for denial of service or abandonment of the system could be a problem. For example, administrators that continually deal with outages as a result of NIS disabling ONTs due to false positives may disable the system rather than correctly configure it. Vice versa in an environment that may not be suitable for the use of and intrusion detection system due to noise or vibrations, NIS may not detect an attack. This is however partially mitigated by the use of Flexible Interlocking Armored Fiber Optic Cable to help stabilize and enhance the use of NIS (LaVallee & Stilp, 2012).

Physical security of the ONT device, and communications to client systems were also evaluated. When looking at the physical security of the ONT, many systems may be installed in areas that may not be suitable for network systems. This could be an uncontrolled location that may have access from unauthorized personnel. Though NIS may be able to detect an alert it does not help with the information stored within the ONT, or communications from the ONT to the client system. Generally speaking, a traditional Cisco solution would be more secure as the switch remains secured within the switch closet, or other secure location. With an ONT, depending on the model and version, some information will remain with the system. Security officers must ensure that enterprise environments use ONT devices such as a Tellabs 120W instead of the Zhone

zNID 2426 series ONT for installations in high risk locations. For example a Tellabs 120W is essentially nothing more than a wall jack with two ports. All configurations for this device are received from the OLT, and no information can be gleaned from the device if it is stolen. A Zhone nNID 2426 Series ONT provides services such as DHCP, VLAN assignment and access control lists. In the event a device that retains this information is stolen, data retained could be used for further exploitation of network services.

In looking at the ability to eavesdrop on communications between the client and the ONT, there are not many differences between GPON FTTD and Cisco. Other than the cases where both the client and switch support MACsec, communications will be in the clear for anyone that has access to the Ethernet medium. One exception to this is the current use of POE devices like an access points. Within a Cisco Environment, access points typically use POE CATV cable for communications and power. In many cases these access points are outdoors in hard to secure locations. With GPON, the CATV cable is eliminated and fiber to an ONT access point is used extending the range of NIS for protection.

Clearly the security provided from the distribution layer to the access layer is greater in the GPON FTTD environment. Though Cisco may have advantages with the use of MACsec, the incompatibility issues from legacy systems and overall complexity may make difficult to implement. In short, physical security of ONTs comes down to proper training, identifying the correct ONT devices, and deploying additional security measures for installations in unsecure areas.

4.9. Training

Though companies like Perpetual Solutions provide the Gigabit Passive Optical Networking (GPON) Course, there is no recognized industry certification for GPON FTTD administrators. Larger I.T. training companies like New Horizons have yet to start any training for GPON. Nothing yet has gained the standard that the CCNA and CCNP have for the networking world in Ethernet. Time will cause this to change as employers will gravitate towards one certification for professionals. With an inability to train

employees to a certain standard, there is risk involved in having administrators not trained correctly for deploying systems properly.

4.10. Certifications and Standards

Cisco generally is an example of a company that meets and defines standards for government organizations. Though there may sometimes be argument over whether that is good or bad in the case of Cisco, it makes the acquisition of products for enterprise networks a manageable task. For example, when the U.S. Department of Defense says that all I.A. (Information Assurance) enabled products must be validated according to NSTISSP No. 11 (United States Department of Defense, 2003), you can be assured that Cisco either has been, or is in the process of the certification. Common Criteria uses the Common Criteria Evaluation and Validation Schema (CCEVS) to evaluate whether software meets their target of evaluation (code executes only what it is supposed to)(United States National Information Assurance Partnership, 2002). Under the CCEVS none of the management software for GPON has been validated, as compared to Cisco where most of their products have been certified.

GPON systems are currently undergoing certifications to validate they meet security standards, but they are behind Cisco. They are not behind because they are new systems, they are just new to the LAN environment as GPON has been used in FTTx installations for years. An example of a current submission through a governmental body for certification would be the U.S. Department of Defense, Joint Interoperability Test Command (JITC) approval of Tellabs 1134 and 1150 Multiservice Access Platform OLT with Specified Tellabs 700 ONT (United States Defense Information Systems Agency, Joint Interoperability Test Command, 2012). As with Ethernet network vendors, competition for government contracts will force them to meet the requirements for these certifications ensuring a standard level of security is met.

4.11. Policy

In rating the potential to craft effective policy between Cisco and GPON in the LAN environment, Cisco has the advantage. Cisco is a well-established, well documented LAN technology used throughout the entire world, and in all types of environments. With

that in mind any security officer that is writing a policy from the beginning has no problem with Cisco, and can find exactly what they need to meet their requirements. One example would be the using the U.S. Military's Department of Defense Instruction 8500.2 Information Assurance (IA) Implementation and the corresponding Secure Technical Implementation Guide for Cisco Layer 3 Infrastructure Switch as an example of how the policy and procedures map together to meet requirements.

The GPON FTTD equivalent does not exist, and policies must be designed from the beginning. Security officers that do not have a technical background in networking, or passive optical networks specifically, will have difficulties creating policy and procedures to effectively govern the security of an organizations GPON FTTD network. There are many examples within this risk assessment that must be defined within new policy for GPON FTTD. Physical security for ONT devices, logical port security differences with relation to access control lists, physical implementation of alarmed fiber solutions, management of the distributed power solutions, and centralized management of all ONT devices. These differences will define a different methodology to govern the security of GPON FTTD. These methodologies in turn will drive new policies and procedures as GPON makes its way into the enterprise LAN landscape, but as of now it is in its infancy.

4.12. Results

Rating on a scale of 1 to 10 for each of the items that were covered in this risk assessment, we rate GPON FTTD against its Cisco competitor. It is understood that this is not a one size fits all and depending on the environment one type of LAN technology is superior to the other in terms of risk.

Item	Cisco	GPON
3.1 VLAN Provisioning and Security	6	10
Comments: With encryption to all downstream traffic, no access to networking protocols for the client systems and centralized management, GPON clearly provides more security in the areas tested. Though Cisco has MACsec, it is not supported on legacy systems, and will be long before an enterprise network could manage all links with this protocol.		

3.2 Port Security	8	6
Comments: Reg ID architecture for GPON provides a one factor form of authentication as compared to Cisco with multiple. With connections to clients, the same services that Cisco provides are available to GPON with the exception to MACsec.		
3.3 Systems Management	5	7
Comments: Though both have management software, GPON has centralized management built into the system natively and intuitively for managing ONT systems.		
3.3 Systems Security	6	8
Comments: OLT and Cisco Switches have virtually the same security settings. The large difference between the two technologies is the management control of the ONT systems by the OLT with clients unable to see any of the management traffic.		
3.3 Access Control Lists	6	7
Comments: GPON has the advantage due to the centralized nature of access control lists at the OLT.		
3.4 Support	9	5
Comments: Ability to support GPON by firms with qualified personnel is limited when compared to Cisco.		
3.5 Redundancy	7	9
Comments: Though a switched network may have more redundancy, the ONT redundancy at the client in the Dual GPON MAC Configuration gives the GPON an edge in this category.		
3.6 Climate Controls and Environment Risks	5	9
Comments: GPONs ability to withstand harsh environments and no need for climate control in most circumstances greatly reduces risk.		
3.7 Power	5	9
Comments: Fully redundant power solutions to all systems provide a much lower risk for the GPON solution.		
3.8 Physical Security	5	9
Comments: With the use of NIS, Fiber Armored Optical Cable, and		

ONT devices that retain no information if stolen, risk is greatly lowered in this area if GPON is implemented properly.		
3.9 Training	9	7
Comments: Though much training for GPON is available, Cisco has the industry standard on this.		
3.10 Certifications and Standards	8	6
Comments: Cisco has put their systems through most of the industry certifications while GPON has yet to fully comply.		
3.11 Policy	9	6
Comments: Little or no examples for policy have been created yet for GPON, though much can be taken from other LAN technologies.		

5. Conclusion

In conclusion, the GPON FTTD architecture appears to provide more security from the distribution layer to the access layer than its Cisco counterpart. Within a more centralized architecture that provides encryption to all downstream traffic, intrusion detection systems that prevent physical tampering, and limitations to systems that can connect to the fiber, GPON FTTD natively provides the ability to secure your network with much less effort and complexity than its Cisco competitor. That being said, an architecture is only as secure as the systems providing the services. Assessments need to be done to validate the OLT and ONT advertised security protocols. Examples would be testing the security of the Web GUI and management network between the OLT and ONT. Further testing is also needed on the ability to manipulate ONT devices, and/or spoof the Reg ID to gain access to internal network communications.

In looking at the basic architecture, Cisco is a much more distributed LAN technology, while GPON FTTD centralizes LAN communications. Even with the exception of MACsec providing security to the client when supported, there are too many improvements on security that are built intuitively into the system from the access layer to the distribution layer for Cisco to really compete with. Systems like NIS provide a

service that is just not possible in a wired Ethernet environment. A simple checkbox on the OLT and all communications downstream to ONT systems is encrypted, which is a leap forward in secure communications. In the end, items that are weak points for GPON FTTD, such as policy, support, and validation of individual systems will become stronger with increased use, providing a more mature and manageable level of security.

6. References

BroadbandSoHo. (n.d.).*Verizon MDU FTTP overview*. Retrieved from http://www.broadbandsoho.com/PDF/Broadbandsoho.com_VZ-FTTP_Overview_Rev1.1.pdf

Cale, I., Salihovic, A., & Ivekovic, M. (2007). *Gigabit passive optical network - GPON* . Retrieved from https://dspace.ist.utl.pt/bitstream/2295/711408/1/12_GPON_%2520Information%2520Technology%2520Interfaces,%25202007.%2520ITI%25202007.%252029th%2520International%2520Conference%2520on.pdf

Cisco Systems Inc. (n.d.a). *Cisco 10GBASE SFP+ modules data sheet*. Retrieved from http://www.cisco.com/en/US/prod/collateral/modules/ps5455/data_sheet_c78-455693.html

Cisco Systems Inc. (n.d.b). *Cisco Catalyst 2960-X Series data sheet.* Retrieved from http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12995/data_sheet_c78-728232.html

Cisco Systems Inc. (n.d.c). *Configuring MAC ACLs*. Retrieved from http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_macacls.pdf.

Cisco Systems Inc. (n.d.d). *Configuring MACsec encryption*. Retrieved from http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/15.0_1_se/configuration/guide/swmacsec.pdf.

Cisco Systems Inc. (n.d.e). *SolarWinds network management guide*. Retrieved from http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns824/sbaBN_solarwinds.pdf.

Cisco Systems Inc. (n.d.f). *Using the ACL Manager*. Retrieved from http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/configuration_guide/acl_manager.html.

Hayes, J. (2006). *FTTH/FTTP/FTTC/FTTX*. Retrieved from www.thefoa.org

Hoover, J. (2012). *Gigabit passive optical networks (GPON): Making waves in your local area.* Retrieved from https://www.bicsi.org/uploadedfiles/conference_websites/winter_conference/2012/presentations/gigabit%20passive%20optical%20networks.pdf

International Telecommunication Union, Telecommunication Standardization Sector of ITU. (2008a). *ITU-T G.984.3 series g: transmission systems and media, digital systems and networks digital sections and digital line system – optical line systems for local and access networks*. Retrieved from http://www.itu.int/rec/T-REC-G.984.3

International Telecommunication Union, Telecommunication Standardization Sector of ITU. (2008b). *ITU-T G.984.4 series g: transmission systems and media, digital systems and networks, digital sections and digital line system – optical line systems for local and access networks*. Retrieved from http://www.itu.int/rec/T-REC-G.984.4

Joseph P. B., Glen B. R., Brian L. A., David G. H., and Janice M. V. (2012). *Evaluation of the Tellabs 1150 GPON multiservice access platform.* SANDIA REPORT. Retrieved from http://prod.sandia.gov/techlib/access-control.cgi/2012/129525.pdf.

LaVallee, M. S., Stilp, J. (2012). *Tellabs GPON optical LAN.* Retrieved from from http://envistacom.com

Lippis III, N. J. (2012). *GPON vs. gigabit ethernet in campus networking*. Lippis Consulting. Retrieved from http://www.cisco.com/web/strategy/docs/gov/gpon_paper.pdf.

N-Lightened Networks. (n.d.). *NRMS-2-32 data sheet*. Retrieved from http://www.nlightenednetworks.com/data/files/Specs/N-Lightened_NRMS-2-32_Data_Sheet.pdf

Odom, W. (2012). *CCNA ICND2 640-816 official cert guide*. (3rd ed.). Indianapolis: Cisco Press.

Tellabs Inc. (n.d.a). *Debunking the myths about optical LAN*. Retrieved from http://www.tellabs.com/resources/papers/tlab_debunking-myths-about-olan.pdf

Tellabs Inc. (n.d.b). *Fiber-to-the-desktop technology for voice, video and data delivery to government agencies.* Retrieved from http://www.tellabs.com/markets/government/tlab_fttd-gov_an.pdf

Tellabs Inc. (n.d.c). *Tellabs 100 series mini optical network terminals (ONTs).* Retrieved from http://www.tellabs.com/products/1000/tlab1100ont_120_mini.pdf

United States Defense Information Systems Agency, Joint Interoperability Test Command. (2012). *Special interoperability test certification of the Tellabs 1134 and 1150 multiservice access platform (MSAP) optical line terminals (OLT) with ppecified Tellabs 700 series optical network terminals (ONT) passive optical network (PON) with software release F P 25.7.* Retrieved from http://jitc.fhu.disa.mil/tssi/cert_pdfs/tellabs_1134_1150_pon_aug12.pdf.

United States Department of Defense. (2003). *Department of Defense instruction, number 8500.2, Information assurance (IA) implementation*. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.

United States National Information Assurance Partnership. (2002) *Common criteria evaluation and validation scheme.* Committee on National Security Systems. Retrieved from http://www.niap-ccevs.org/cc-scheme/nstissp_11.pdf.

Zhone Technologies. (2012a). *MXK configuration guide for software version 2.4. 830-01812-19.* Retrieved from http://zhone.com.

Zhone Technologies. (2012b). *zNID 24xx series configuration guide for software version 2.5. 830-03782-02.* Retrieved from http://zhone.com.