SOLUTIONS **OVERVIEW**

tellabs™

Advanced security

Recent history has far too many high-profile worst-case scenario examples of network data breaches, which are driving CIOs and IT pros to invest in transforming IT infrastructure and ensure that corporate info is secure, protected and highly available. For example, in 2006 the Department of Veterans Affairs lost a large database with sensitive veterans' information due to human error. In 2009, you might remember that Google, Yahoo and other Silicon Valley companies struggled with the realization that highly valuable intellectual properties were being stolen from their networks on an ongoing basis. And then NASDAQ suffered the unfortunate event in 2011 where sensitive communications of senior executives were being accessed and leaked. This is why a Gartner study determined that security is a Top 10 technology priority for CIOs[1] and Infonetics security is a top concern for enterprise access networks.[2]

Introduction

Tellabs™ Optical LAN Solutions and Tellabs™ PON Manager play vital roles in providing more secure LAN where security policies and procedures are implemented consistently, with fewer human errors across a more reliable network [Figure 1]. To that end, this paper will cover the following security topics:

- Security impact on employees and businesses
- Passive Optical LAN compared to legacy copper-based LAN
- Element management security
- Across Optical LAN systemwide security
- Optical plant (cabling infrastructure) security
- Optical Network Terminal (ONT) security
- Exceeding Government, Military, HIPAA and PCI requirements

Highlights

- Optical LAN reduces the threat of both internal and external malicious attacks, while lowering LAN costs
- Modern LANs need a secure infrastructure, breach response plan and macro security program
- Optical LAN is deployed in HIPAA- and PCI-compliant LANs today
- Copper is good for antennas, grounding, power and heat transfer, but not good for LAN security
- Optical LAN is deployed in the most secure government and military networks in the USA
- All-Secure™ PON saves 66% in installation costs and 75% in faster moves, adds and changes
- Optical LAN provides powerful security measures at the physical layer, the data layer, the user level and port level

Security impact on employees and businesses

When tackling the topic of the security impact on employees and businesses, the first question that comes to mind is — what is the cost of losing data, files and records accessible through the LAN? In 2014, Ponemon Institute released a study covering the cost of data breach and concluded that the average cost to a company in the USA is $5.85 million per incident. The average cost paid for each lost or stolen record containing sensitive and confidential information for U.S. organizations is, on average, $201. The highest cost for verticals is Healthcare ($358 per file) and Education ($294 per file). Ponemon Institute stated that the root cause is 42% malicious/criminal, 30% human error and 29% system glitch.[3] *Healthcare News* penned an article that described how LAN downtime can result in lost data, files and records.[4] The Healthcare vertical provided an excellent example of this correlation between data loss and network reliability. This is because doctors, nurses and healthcare staff are constantly uploading critical data 24/7/356, and if the LAN is down, then data/files/records can be lost. The *Healthcare News* article went on to state that healthcare organizations for one are making significant IT investments to transform IT infrastructure and ensure that patient information is secure, protected and highly available.

[1] Gartner — http://www.gartnerinfo.com/sym23/evtm_219_CIOtop10%5B3%5D.pdf
[2] Infonetics — http://www.infonetics.com/pr/2014/Wireless-LAN-Enterprise-Survey-Highlights.asp
[3] Ponemon Institute — http://public.dhe.ibm.com/common/ssi/ecm/en/SEL03027USEN/SEL03027USEN.PDF
[4] *Healthcare News* — http://www.healthcareitnews.com/news/healthcares-slack-security-costs-16b

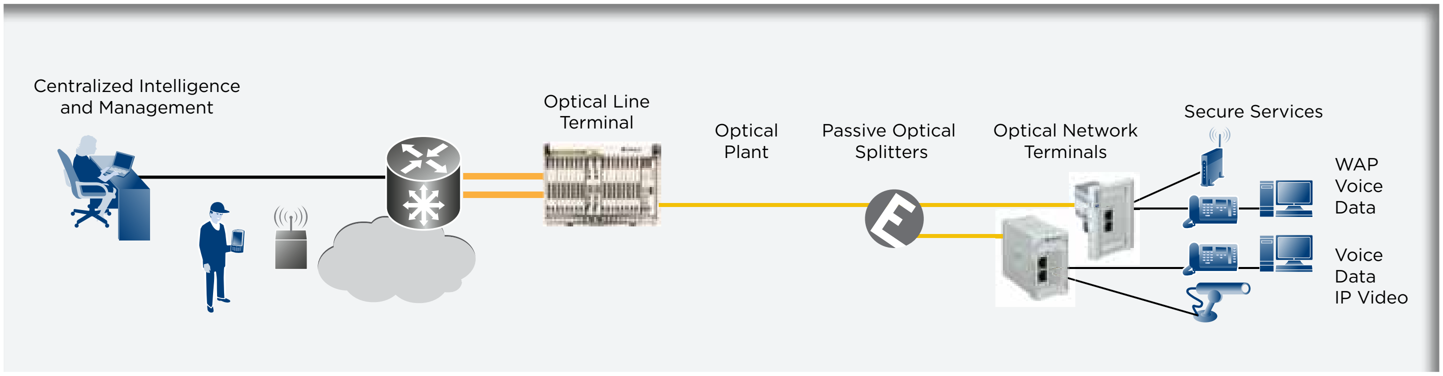
Centralized Intelligence and Management
Optical Line Terminal
Optical Plant
Passive Optical Splitters
Optical Network Terminals
Secure Services
WAP
Voice
Data
Voice
Data
IP Video

Figure 1: Tellabs™ Optical LAN solution providing advanced security

We already mentioned that Ponemon Institute found that the root cause of breaches is 42% malicious/criminal, 30% human error and 29% system glitch — how often is LAN equipment and infrastructure responsible? An international Ethernet switch manufacturer polled the IT industry and found that 39% of IT professionals said that they have dealt with an employee accessing unauthorized parts of a company's network or facility. This is categorized as unauthorized physical and/or network access.[5] Regardless of how a security breach occurs, Gartner Research cautions that a data breach without a well-crafted response plan in place is likely to cost a chief information security officer his/her job.[6]

How can businesses protect themselves from data breaches as a result of insecure LAN equipment and infrastructure? The Federal Communications Commission published a security planning guide. In that guide, they noted that securing your company's network consists of[7]:

- Identifying all devices and connections on the network
- Setting boundaries between your company's systems and others
- Enforcing controls to ensure that unauthorized access, misuse or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur

And, the U.S. Department of Homeland Security says that cyber insurance should be considered to mitigate losses from security incidents, such as data breaches, business interruption and network damage. Insurance should promote the adoption of preventive measures in return for more coverage. And the insurance should encourage the use of best practices by basing premiums on the level of protection.[8] Therefore, proactively building a more secure LAN can lower the cost of cyber insurance.

One way that security can impact employees, especially CIOs and IT staff, is when security events are identified as key performance indicators for performance reviews and even compensation reviews. Here is a list of some CIO and IT staff key performance indicators:

- Number of security breaches/incidents in systems and infrastructure
- Percent of systems/applications compliant to security policies/standards
- Security patches applied within timelines/deadlines percentage
- Uptime percent for business critical systems
- Business time lost due to unscheduled downtime

In summation, there are real costs associated with data breaches. The LAN equipment and infrastructure are possible entry points for malicious activity. It is best for CIOs and IT pros to have a proactive data breach response plan. And with a proactive, highly secure LAN in place, CIOs and IT pros can benefit from lower loss costs, better KPI reviews and even lower insurance premiums. All of the above can also lead to a less stressful, more productive and healthier work environment with a highly secure LAN.

Passive Optical LAN compared to legacy copper-based active LANs

LAN security is gaining greater importance every year. Based on a Gartner survey, security is now one of the Top 10 technology priorities for a CIO.[9] What has not changed is the architecture, cabling and equipment used by legacy copper-based Active Ethernet LANs to improve security. Passive Optical LAN has many attributes that can tighten network security.

[5] Cisco — www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf
[6] http://www.fierceenterprisecommunications.com/story/poorly-handled-data-breach-could-cost-ciso-his-or-her-job-warns-gartner/2013-06-12
[7] FCC — http://transition.fcc.gov/cyber/cyberplanner.pdf
[8] DHS — http://www.dhs.gov/publication/cybersecurity-insurance
[9] Gartner — http://www.gartnerinfo.com/sym23/evtm_219_CIOtop10%5B3%5D.pdf

Legacy copper-based LAN — A legacy copper-based active Ethernet LAN is characterized as being a complex distributed network. All of its resources are distributed to the farthest reaches of the LAN, which make implementing and managing consistent security policy and process difficult. With network intelligence distributed to all disparate end-points, security policy, security procedures, equipment configurations and MAC require greater human touches, which increase the chance of errors and lower security. These copper-based active Ethernet LANs are inherently less reliable; therefore, their instability contributes to security risks due to loss of data, files and records. Copper cabling introduces security weakness because its radiant data is tasked to transport securely — that is, you do not need to tap into copper cable to gain access to the sensitive data, files and records within. Finally, all of the deep network devices with full functionality and full intelligence add complexity and vulnerability for malicious access.

Optical LAN — In comparison, a Passive Optical LAN architecture promotes centralized intelligence and management, which means that implementing consistent security policies and processes that can be done with confidence. The centralized intelligence of Tellabs™ Optical LAN and, in particular, the Tellabs Panorama™ PON Manager element management system reduce human touches and errors. It is a widely accepted fact that optical cabling is inherently more secure than copper cabling. Different from legacy copper-based LANs, Optical LAN's deep network devices (e.g., ONTs) store no configuration or user information, and these ONTs present no local physical management access.

Enhanced Security Quantifiable Savings for less than 500 Users/End-point Devices from Tellabs Optical LAN	
Less than 500 users	Realistic deployment size for Enterprise LAN served by 1134 OLT
$99,944	2014 Symantec data breach calculator theoretical cost of a data breach for a "service only" company that has only employee/company info at risk
29%	Ponemon Institute states that the root cause of breaches is 29% system glitch, which is a good representation of IT and IT infrastructure responsibility; the other two causes are 42% malicious/criminal and 30% human error
$28,983	$99,944 x .29 = Percentage of responsibility for secure LAN infrastructure
$28,983	**Proportional savings from Tellabs Optical LAN, but one could also argue that $99,994 is the true value at risk**

Figure 2: Potential savings from Tellabs™ 1134 OLT blocking security breach for 500 users/end-point devices.

Enhanced Security Quantifiable Saving for 1,000 to 5,000 Users/End-point Devices from Tellabs Optical LAN	
1,001 to 5,000 users	Realistic deployment size for Enterprise LAN served by Tellabs 1150E OLT
$1,500,000	2014 Symantec data breach calculator theoretical cost of a data breach for a "service only" company that has only employee/company info at risk
29%	Ponemon Institute states that the root cause of breaches is 29% system glitch, which is a good representation of IT and IT infrastructure responsibility; the other two causes are 42% malicious/criminal and 30% human error
$435,000	$1,500,000 x .29 = Percentage of responsibility for secure LAN infrastructure
$435,000	**Proportional savings from Tellabs Optical LAN, but one could still argue that if and when an event happens, $1.5 million will be at risk**

Figure 3: Potential savings from Tellabs™ 1150E OLT system blocking security breach for 1,000–5,000 users/end-point devices.

Based on the information already presented in this overview, we can provide insight into the potential cost savings experience from Tellabs Optical LAN successfully blocking a data breach. A realistic deployment size for an Enterprise LAN being served by Tellabs™ 1134 Optical Line Terminal is 500 users and/or end-point devices. We can use a Symantec data breach calculator to get an estimation of $99,994 for the cost of the data breach for a "service only" company that has only employee/company info at risk. Since we already learned from Ponemon Institute study about the 29% system glitch, we could extrapolate that $28,983 (29% of $99,994) can be attributed to 500 user/device Optical LAN savings against data breach, but one could also argue that $99,994 is the true value of the total risk at hand [Figure 2].

An Enterprise LAN being served by Tellabs™ 1150 Optical Line Terminal is most likely around the 1,000 to 5,000 users and/or end-point devices size. Symantec data breach calculator estimated $1.5 million for the cost of a data breach for a "service only" company where only employee/company info is at risk.[10] If we apply the Ponemon Institute 29% system glitch percentage, we could extrapolate that $435,000 (29% of $1,500,000) can be attributed to 1,000 to 5,000 user/device Optical LAN savings against data breach. But again, just like the insurance cost for any calamity, one could also argue that $1.5 million is the true cost [Figure 3].

The goal of Tellabs Optical LAN is to improve physical LAN security, enabling consistent security policies that are centrally managed while reducing human error and increasing network stability.

[10] Symantec — http://databreachcalculator.com/

Element management security

A secure LAN starts with the Tellabs Panorama™ PON Manager, which is the element management interface for the Optical LAN. Within the Tellabs PON Manager, role-based access for users is established through strict authentication and authorization [Figure 4]. This is where secure passwords are assigned and managed. Based on IT staff credentials, privileges are defined for what a user can view and modify. Then the activity of the IT staff can be tracked, which helps root cause analyses during trouble-shooting and can help with junior IT staff training. User management is VERY important for achieving the highest levels of security, stability and operational efficiencies. The Tellabs PON Manager supports IPv6 and IPSec, which add additional security functions. Finally, Tellabs PON Manager is where secure profiles/templates are created for ONTs, ports, connections and other network elements. Within these secure profiles/templates, consistent policies and procedures can be ensured. Information managed within these profiles/templates include the ONT identifier and name, Ethernet port configuration, PoE settings, IEEE 802.1x, LLDP, RSTP settings and NAC, which are configured as autonomous rules-based provisioning.

Across Optical LAN systemwide security

It is true that the Tellabs Panorama PON Manager provides much of the systemwide centralized intelligence, control, automation and management. However, there are other security features and functionality associated with the Optical Line Terminal (OLT) and the greater Optical LAN solution [Figure 5].

Advanced Encryption Standard (AES) — Advanced Encryption Standard (AES) is supported. AES is comprised of encryption algorithm and constantly churning keys. GPON uses 128-bit AES encryption for downstream transmissions. To illustrate the relative size of an 128-bit key, it would be a constantly changing (i.e., churning) 3,400,000,000,000,000,000,000,000,000,0 00,000,000,000 size number. AES has been adopted by the U.S. government and is now used worldwide. Why does GPON have no encryption in the upstream direction? All upstream transmission, from all ONTs, is granted and orchestrated by the OLT. The OLT has the intelligence to recognize rogue or unexpected ONTs that have NOT been properly authenticated or authorized. The GPON protocol is a stateful protocol; therefore, any interruption of communications will be deemed suspicious,

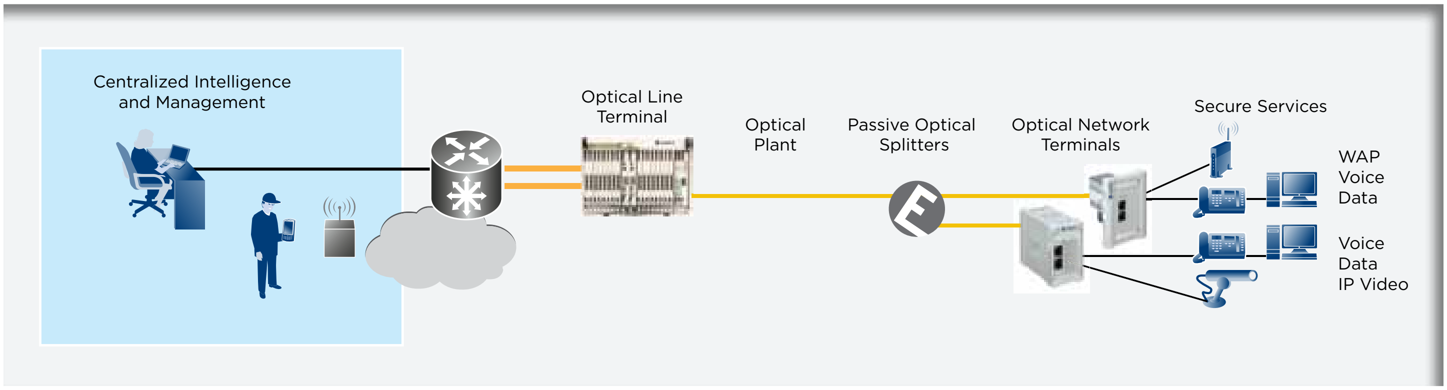
Centralized Intelligence and Management
Optical Line Terminal
Optical Plant
Passive Optical Splitters
Optical Network Terminals
Secure Services
WAP
Voice
Data
Voice
Data
IP Video

Figure 4: Tellabs Panorama™ PON Manager providing centralized intelligence, control, automation and management

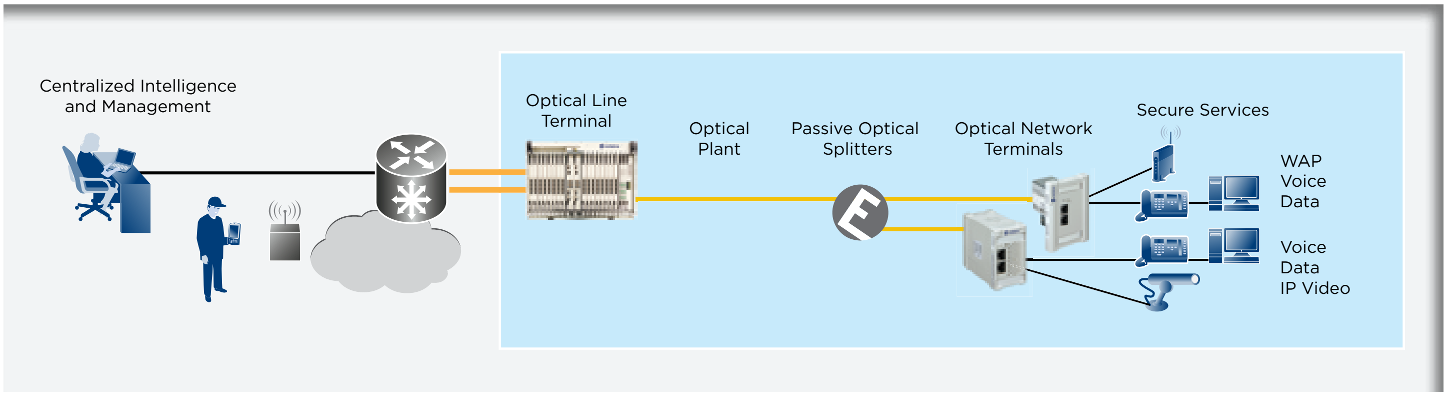
Centralized Intelligence and Management
Optical Line Terminal
Optical Plant
Passive Optical Splitters
Optical Network Terminals
Secure Services
WAP
Voice
Data
Voice
Data
IP Video

Figure 5: Tellabs Optical LAN solution systemwide security

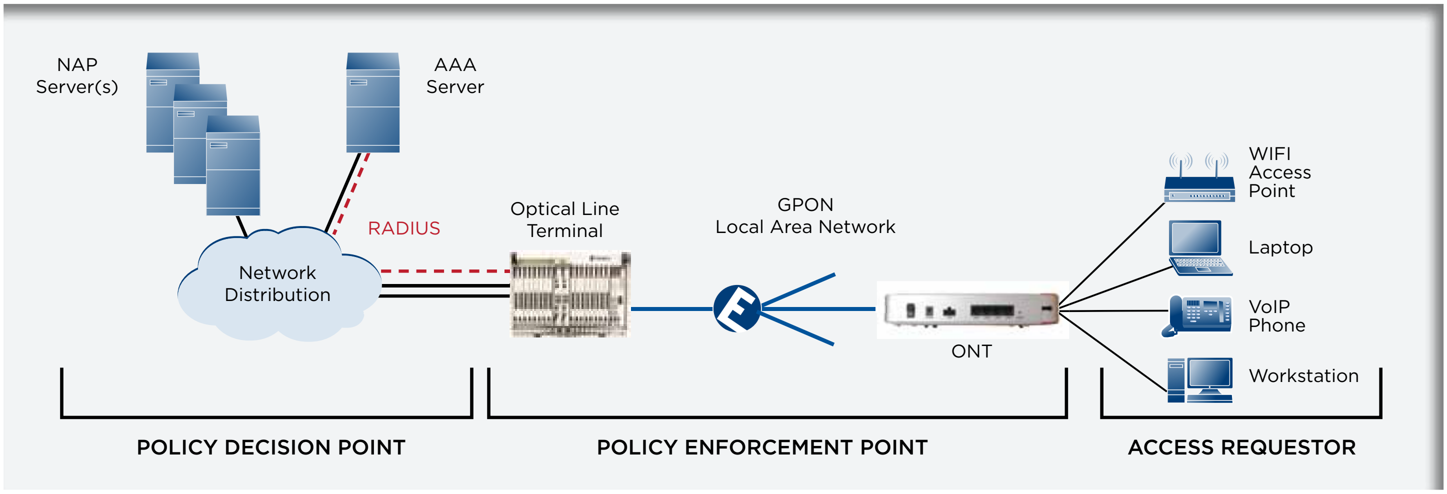

Figure 6: Tellabs Optical LAN systemwide secure authentication and authorization mechanisms.

and that ONT will be quarantined immediately. Simply stated, the OLT and its centralized intelligence are managing 10s if not 1,000s of ONTs simultaneously, and only it can decipher the order of the upstream transmission from multiple ONTs.

Service Segmentation — In the past, LAN services (e.g., voice, video, wireless access, etc.) were often physically separated onto different Layer-1 cabling for security purposes. These overlay networks were costly to purchase and operate — negatively impacting building space, introducing wasteful material, consuming power and emitting thermals. Today, it is accepted practice to provide secure transmission over a single physical network utilizing Layer-2 VLAN trunking because service-level VLANs can extend to all end-points. This is how Optical LAN segregates and secures data flows to each client device. Even different ports and ONTs on the same VLAN can be offered with different service level agreements with VLAN trunking. What used to be relegated to disparate physical networks can now be converged over a single fiber with Optical LAN.

Authentication and Authorization — Another important aspect of security over an Optical LAN is the support of consistent authentication and authorization policies. This is accomplished through the Tellabs PON Manager within profiles and templates, relying on IEEE 802.1x, NAC, PAC, DHCP and RADIUS. IEEE 802.1x provides controlled access through a strong authentication mechanism for end-user devices utilizing encryption keys. This helps with intrusion detection and protects from unauthorized activity down at per user and per device levels. These functions work in concert with Network Access Control (NAC) and Port Access Control (PAC) functions, which also include Dynamic Host Control Protocol, RADIUS and Change of Authorization (Cisco ISE) support [Figure 6].

Access Control Lists — Access Control Lists (ACLs) assist with end-to-end security across the Optical LAN. These ACLs can be created at Layer 2 (Ethernet), Layer 3 (IP) and Layer 4 (TCP/UDP). They can be either static or dynamic. Their purpose is to facilitate network protection for trusted and nontrusted devices, and to operate in conjunction with authentication mechanisms, for example:

- L2 Ethernet Filtering: source and destination MAC address, Ethertype and organizationally unique identifier (OUI)
- L3 IP Filtering: source and destination IP address and Protocol Level
- L4 TCP/UPD Filtering: Type and Port

The Tellabs Optical LAN system can support 2,048 basic ACL filters and 512 deep ACL filters with granularity down to the PON service module card.

Rate Limiting — Ingress rate limiting is an element of security necessary when enabling Ethernet bridging across the Optical LAN. Its purpose is to limit all broadcast ingress datagrams down to a controlled and safe level. Rate limiting can be enabled on any ACL (not just broadcast). It protects against network flooding and blocking, and can be set in 64 Kbps increments. Rate limiting greatly reduces the potential for Denial of Service (DoS), redirects or other malicious attacks.

IP/Ethernet Protocols Supported — Finally, it should be noted that Tellabs Optical LAN systems exceed the expectations and needs of Enterprise LAN standards-based Ethernet and IP protocols. That is, Tellabs Optical LAN system supports a long list of IEEE and RFC protocols too numerous to list for the purposes of this overview.

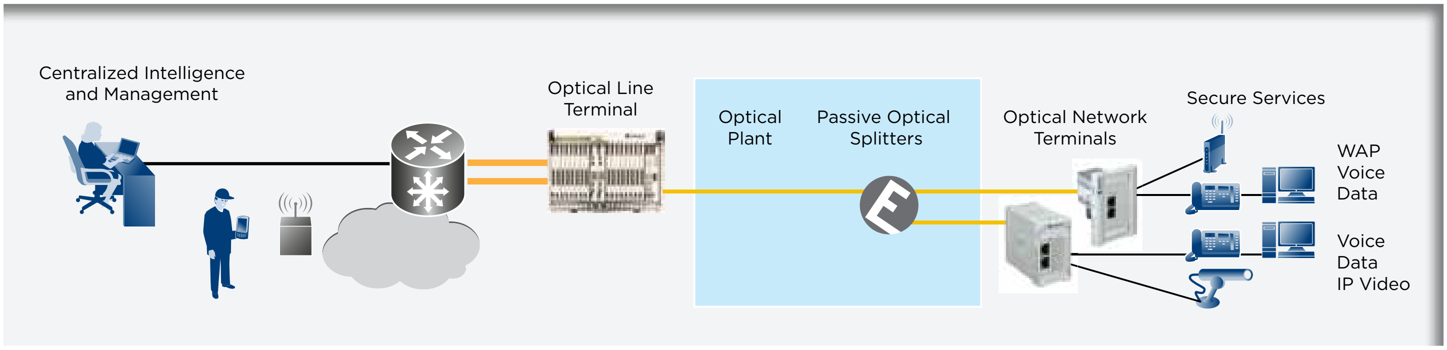
Centralized Intelligence and Management
Optical Line Terminal
Optical Plant
Passive Optical Splitters
Optical Network Terminals
Secure Services
WAP
Voice
Data
Voice
Data
IP Video

Figure 7: Optical Plant (cabling infrastructure) security

In summary, Tellabs Optical LAN systemwide security and intelligence is managed centrally by OLT and, ultimately, Tellabs PON Manager. From an end-to-end systemwide standpoint, Tellabs Optical LAN provides powerful security measures at the physical layer, the data layer, users and subtended devices levels.

Optical plant (cabling infrastructure) security

The optical plant, also known as the fiber cabling infrastructure, can make significant contributions to overall security [Figure 7]. Fiber optic cabling is more secure than copper cabling. Fiber is not susceptible to interference nor does it introduce interference. With fiber you have no cross-talk, no EMI, no RFI and no EMP. The opposite is true of copper cabling, which allows radiate emissions that can be eavesdropped without physical access. You CANNOT "listen to" fiber from any distance, and one would need to physically access fiber to gain entry to fiber-based communications. Physically tapping fiber is tremendously difficult, taking into consideration the expertise and equipment that would be needed. In the end, GPON is a stateful protocol that will detect all abnormal, rogue and intrusion events, so the physical tapping event will be thwarted.

All-Secure™ PON — All-Secure PON is a means of building highly secure LANs by combining the inherent security benefits of Optical LANs with armored, alarmed and 24/7/365 monitored fiber cabling.[11] All-Secure PON delivers unparalleled performance, security and information assurance [Figure 8]. It is JITC Certified, NSTISSI 7003 compliant and deployed throughout the U.S. Department of Defense. All-Secure PON can now be utilized by other vertical markets, such as Healthcare, Financial and Education, which experience the high cost associated with data breaches and thus require highly secure LAN. Legacy hardened carrier protective distribution system (PDS) with electrical metallic tubing and concrete encasement even requires periodic visual inspections (PVIs). The carrier (or cabling) was deployed below ceiling, above floor for the purposes of visual inspection. The electrical metallic tubing required welding and epoxying of all connections. The security for outdoor cabling required concrete encasement.

With All-Secure PON and its armored, alarmed and 24/7/365 monitored fiber cabling, both CapEx and OpEx are drastically reduced. With the constant auto-learning threshold monitoring of the cabling 24/7/365, the requirement for periodic visual inspections is removed. The cables can then be installed out of sight above ceiling and below floor. Real-world business cases for All-Secure PON have showcased 66% savings in installed costs and 75% in faster moves, adds and changes.

Optical Network Terminal (ONT) security

The ONTs are inherently secure as well [Figure 9]. Optical LAN ONTs are designed with no local management access. This is done because there are few needs for human touches at the ONTs. The ONTs are basically simple optical-to-electrical terminals. ONTs are highly secure and reliable, which ultimately helps improve security. Furthermore, Optical LAN has centralized intelligence and management; no information is stored at the ONTs. That is, user and provisioning information does not reside on ONT. ONTs are a thin client — user/device policies are managed solely at the OLT. Thus, ONTs can move freely around the LAN and be sent back to the manufacturer for repair/return without the risk of network/user data being compromised.

What if someone with malicious intent tries to access ports on the ONTs? The open unused ONT ports are dead by default and CANNOT pass traffic. And even if that open port somehow got activated, the perpetrators would be blocked by network access control (NAC) protection mechanisms. The activation of an open unused ONT port can only be done centrally back at the secure PON Manager console, most likely positioned in a locked room. Pulling a working service connection (i.e., cable) from an active ONT port triggers an alarm through the PON Manager, and then, once again, there is NAC protection that would block hacker access.

[11] Tellabs and Network Integrity Systems — http://www.tellabs.com/solutions/opticallan/tlab-secure-pon.pdf

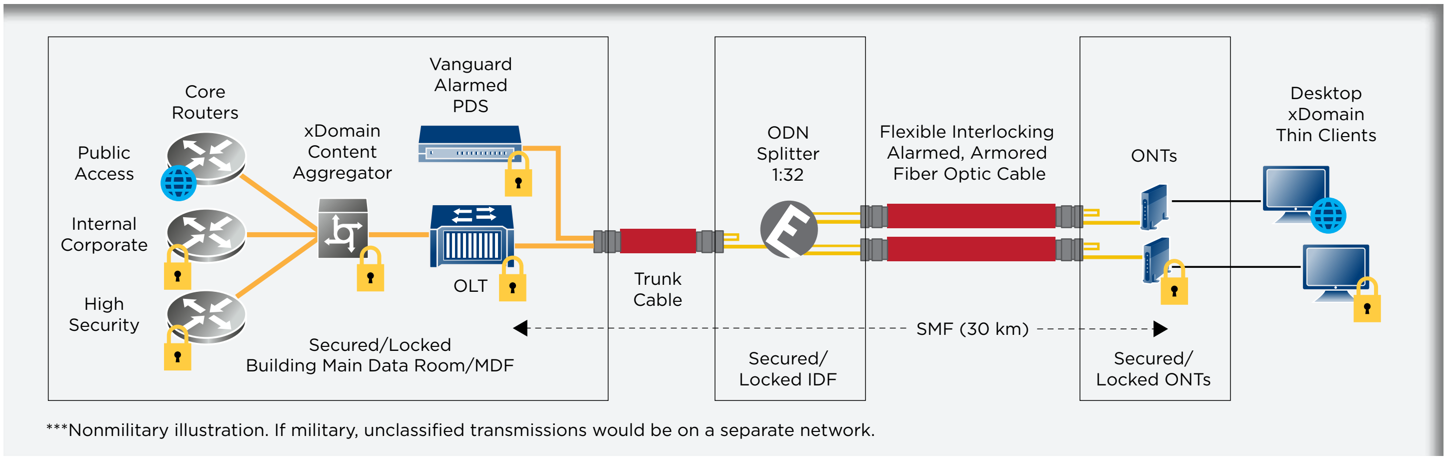

Figure 8: All-Secure™ PON

A common question is — if the fiber is tapped at the ONTs, could meaningful data, records and files be extracted? First, know that the reflection loss is too great to recover any ONT's upstream signal at another ONT. Second, only the OLT can synch upstream data from multiple ONTs because the upstream frame alignment is offset. This offset frame alignment means that an intermediate interception would not have the correct frame alignment synchronization; therefore, no useful data, records or files could be gathered. Last, even if inline monitoring of a single ONT were attempted, once the fiber accessed, the OLT (especially with All-Secure™ PON), it would be immediately detected and alert the system to the fiber tampering.

Additional physical security at the ONTs of note include the fact that the Tellabs™ 120W Mini Optical Network Terminal faceplate screws are alarmed through Tellabs PON Manager. Also, there are lockable cover options that can be deployed with Tellabs™ 100 Series ONTs and Tellabs™ 700 Series ONTs end-devices.

Exceeding Government, Military, HIPAA and PCI requirements

The U.S. Federal Government and the Military were the early adopters of Tellabs Optical LAN due to its ability to improve network security both at the electronics and across the cabling infrastructure. Today, other industry verticals such as Healthcare, Education, Retail and Financial, are looking toward Optical LAN for the same security benefits.

Government and military — All Tellabs Optical LAN hardware and software pass rigorous and constant testing through Joint Interoperability Test Command (JITC). All Tellabs Optical LAN products are listed on the DISA JITC UC-APL, which is publicly accessible to all Healthcare, Education, Retail and Financial entities considering the technology. In addition to JITC testing, Tellabs Optical LAN has successfully completed the U.S. Army I3MP/I3C2 Performance Evaluation Test and Certified TEMPEST Technical Authority (CTTA), and meets UCR 2013, STIGs and FIPS 140-2 criteria. Tellabs Optical LAN is deployed in the most secure government and military networks in the USA.

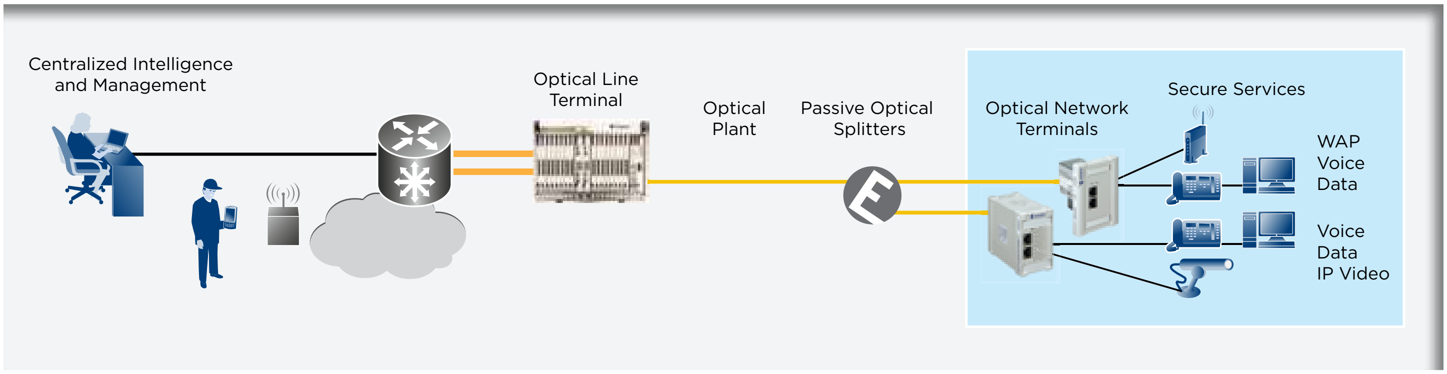

Figure 9: Equipment redundancy options include uplink, control, timing, service module, power plant and fans.

Health Insurance Portability & Accountability (HIPAA) — The intent of HIPAA is to protect patient data integrity from eavesdropping, manipulation and theft. Optical LAN is a robust and secure solution that meets applicable HIPAA requirements. Optical LAN presents no access to any ePHI data. As such, Optical LAN's primary role is to provide transport and systemwide security. Optical LAN's combination of very robust security and no ePHI data minimizes any risk to ePHI data. Optical LAN can also provide documented hardening of operational systems and procedures. These HIPAA policies and procedures are well-defined step-by-step procedures, otherwise known as a Security Technical Implementation Guide (STIG) for hardening the operating system, the Tellabs PON Manager and the Optical LAN hardware (OLTs and ONTs). Tellabs' Optical LAN is deployed in HIPAA-compliant LANs.

Payment Card Industry (PCI) — The purpose of the PCI is to provide protection for credit cardholders by ensuring that merchants meet minimum levels of security when they store, process and transmit transactional data. Optical LAN can help build and maintain a secure network for the protection of credit cardholder data. Optical LAN is ideal for implementation consistent with PCI policies, including strong access control measures and regular monitoring and testing of the network, all of which should be part of an overarching information security policy and procedure, of which Tellabs Optical LAN and Tellabs PON Manager play a vital role. Tellabs Optical LAN is deployed in PCI-compliant LANs across multiple vertical markets.

Optical LAN can help build and maintain a secure network for the protection of credit cardholder data.

Summary

No company wants to be the victim of a data breach, and no business wants their security weaknesses to be showcased across all media outlets in the event of such an unfortunate breach. No doubt there are real costs for businesses and a negative impact on employees as a result of a breach. Tellabs Optical LAN Solutions, fiber-based LAN infrastructure and Tellabs PON Manager are viable options for building more defensible LANs where security policies and procedures are implemented consistently.

Take the next step. Contact Tellabs today.

tellabs™

+1 800 690 2324
+1 630 798 9900
www.tellabs.com

1415 West Diehl Road
Naperville, IL 60563
U.S.A.