Tellabs® Advanced Security Software Package

Improve physical LAN defensibility, enabling consistent protection policies that are centrally managed while reducing human error and increasing network stability

Overview

Modern local area networks (LANs) require secure infrastructure, a breach response plan and a macro security program. Tellabs® Optical LAN, single-mode fiber (SMF) infrastructure, Tellabs® Panorama™ PON Manager and Tellabs® Advanced Security Software Package all make positive contributions to hardening the LAN as part of a greater security program. All these Optical LAN elements work to improve physical LAN defensibility, enabling consistent protection policies that are centrally managed while reducing human error and increasing network stability. To that end, Tellabs Advanced Security Software Package adds the following LAN protection features and functions to the already secure Passive Optical LAN.

- Secure User Management
- Secure Access Control
- Secure Service and Application Delivery
- Security Against Malicious Attacks
- And the option to manage Tellabs® All-Secure™ PON

Benefits

CIOs and IT pros proactively looking to implement secure infrastructure, a breach response plan and a macro security program can benefit from Tellabs Advanced Security Software Package. It will allow them to define and manage consistent security policies and overarching procedures across their entire LAN. It also easily simplifies the replication of these LAN protection policies and procedures across local, regional and international locations. This centralized management of security directly results in reducing human error and increasing network uptime. Once leveraged, Tellabs Advanced Security Software Package can deliver many security benefits, such as:

- Central controlled user management
- Consistent and repeatable network authentication and authorization mechanisms
- Secure delivery of modern Enterprise services and applications
- Reduced threat of both internal and external malicious attacks
- HIPAA- and PCI-compliant LANs and deployment in the most-secure government and military networks
- Powerful security measures at the physical layer, the data layer, the user level and port level

Features and Functions

Passive Optical LAN, SMF cabling and Tellabs PON Manager provide many inherent benefits to CIOs and IT pros helping them build a highly secure LAN. Tellabs Advanced Security Software Package completes the security program by enabling these additional features and functions.

Secure User Management — 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. This is where secure passwords are assigned and managed. Based on IT staff credentials, privileges are defined on what a user can view and modify. Then IT staff activity can be tracked, which helps root cause analyses during troubleshooting and can also help with junior IT staff training. Finally, Tellabs PON Manager is where secure Profiles and Templates are created for ONTs, ports, connections and other network elements. Within these secure Profiles and Templates, consistent security policies and procedures can be ensured. User management is VERY important for achieving the highest levels of security, stability and operational efficiencies.

Secure Access Control — 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 by implementing secure protocols, such as 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 to the user and per device level. These functions work in concert with Network Access Control (NAC) and Port Access Control (PAC) functions, which also include Dynamic Host Control Protocol (including Option 82) and RADIUS support.

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.

Secure Service and Application Delivery — 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 security, 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, so 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 different service level agreements with VLAN trunking. What used to be relegated to disparate physical networks can now be converged and secured over a single fiber with Optical LAN.

Security Against Malicious Attacks — 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. Rate limiting can be established on broadcast, unknown unicast, multicast and IGMP messaging, including ICMP rate limiting for management plane protection. ACL can even be used for restricting IPv6 router advertisements. All of this 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. Also of interest is packet rate limiter to prevent control plane attacks and mechanisms to stop MAC spoofing.

Option to Manage Tellabs All-Secure PON — Tellabs 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. All-Secure PON delivers unparalleled performance, security and information assurance. It is JITC certified, NISTISSI 7003 compliant and deployed through-out the U.S Department of Defense. Tellabs All-Secure PON can now be utilized by other market verticals, such as hospitals, financial and education, which experience the high cost associated with data breaches and thus require a 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 the ceiling and above the 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 Tellabs All-Secure PON and its armored, alarmed and 24/7/365-monitored fiber cabling, both CapEx and OpEx are drastically reduced. With 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 the ceiling and below the floor.

Specifications

Tellabs® Advanced Security Software Package is a specialized license of specific features and functions provided in conjunction with Tellabs® Optical LAN Base Software Package and Tellab®s Panorama™ PON Manager Software. Therefore, the hardware and software specifications are the same.

Solaris Operating System

Solaris			
Number of OLTs	**Number of GUIs**	**Processor**	**Memory and hard disk**
1–10	5	√ Sun SPARC T5-1B server module (3.6 GHz SPARC T5 16-Core CPU) √ Sun SPARC T4-1 (2.85 GHz SPARC T4 8-Core CPU) √ Sun SPARC T3-1 (1.65 GHz SPARC T3 16-Core CPU) √ Sun SPARC Enterprise T5120 (1.4 GHz UltraSPARC T2 8-Core CPU)	√ 8 GB RAM √ 300 GB SAS Disk
Operating System		Solaris 10 (any update) for Oracle 10g and Postgres Solaris 10 (update 6 or later) for Oracle 11g	
Database Support	64-bit Standard Edition for Oracle	√ Postgres Release 9.2 √ Oracle Database 10g Release 2 (10.2.0.1) for standard deployment √ Patch #8202632 to update to Release 10.2.0.5 for hardened deployment √ Oracle Database 11g Release 1 (11.2.0.1) for standard deployment √ Oracle Database 11g Release 1 (11.2.0.4) for hardened deployment	

Windows Operating System

Windows			
Number of OLTs	Number of GUIs	Processor	Memory and hard disk
1–2	2	√ 1 Intel CPU with at least 2-core	√ 4 GB RAM √ 160 GB SATA Disk
1–10	5	√ 1 Intel CPU with at least 4-core	√ 8 GB RAM √ 160 GB SATA Disk
Operating System		√ Windows 7 64-bit Professional Edition or above, SP1 for Postgres only √ Windows Server 2008 64-bit Standard Edition R2 for Oracle or Postgres	
Database Server	32-bit Standard Edition for Oracle	√ Postgres Release 9.2 √ Oracle Database 10g Release 2 (10.2.0.3) for standard deployment √ Patch #8202632 to update to Release 10.2.0.5 for hardened deployment √ Oracle Database 11g Release 1 (11.2.0.1) for standard deployment √ Oracle Database 11g Release 1 (11.2.0.4) for hardened deployment	√ Minimum RAM requirement becomes 8 GB if Oracle 11g is used

Ordering Information

Each Software Package license provides the ability to operate and manage a single OLT of the type designated by the license. Selection must include the Base Software at a minimum and Advanced Security, Advanced Availability and Advanced Operational as optional selections. The Tellabs® Advanced Availability Software Package does not include the hardware described in this data sheet. If additional hardware is needed, then that hardware should be purchased separately. The Tellabs Advanced Availability Software Package provides the authorization and means to manage such hardware.

Tellabs Advanced Availability Software Package Part Number and Other Software Package Part Numbers

	1150 OLT	1150E OLT	1134 OLT	1134AC OLT	1131AC OLT
Base Software	81.SR290BASE1150	81.SR290BASE1150	81.SR290BASE1134	81.SR290BASE1134	81.SR290BASE1131
Advanced Security	81.SR290AS1150	81.SR290AS1150	81.SR290AS1134	81.SR290AS1134	81.SR290AS1131
Advanced Availability	81.SR290AA1150	81.SR290AA1150	81.SR290AA1134	81.SR290AA1134	N/A
Advanced Operational	81.SR290AO1150	81.SR290AO1150	81.SR290AO1134	81.SR290AO1134	81.SR290AO1131

For more information, please contact your local Tellabs sales representative or local Tellabs sales office at the phone numbers provided below, or visit www.tellabs.com.

Take the next step. Contact Tellabs today.

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

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

TEL9455 11/14