WHITE PAPER

When 1% of the Light Equals 100% of the Information

Encryption Solutions for DWDM and OTN Networks

info@packetlight.com | www.packetlight.com

Introduction

Fiber optic communication infrastructure used to be considered more secure than copper infrastructure, since it does not radiate and is more resilient to tapping. Recent years have shown that it is, in fact, quite simple to tap fiber optic cables and extract the data transmitting over them. As a result, the need for data security over DWDM links has increased, especially in financial and government institutions, critical infrastructure, data centers and service providers. Moreover, security requirements such as confidentiality, integrity and authentication have become mandatory in most industries.

Optical Fiber Link Protection

Fiber optic infrastructure is widely used for remote data centers, disaster recovery connectivity, cloud, and virtual networks. WDM solutions enable multiplexing multiple data rates and transporting them across the network with ultra low latency. The fiber infrastructure also offers considerable capacity, with up to 96 wavelengths of 100G/200G (and above) capacity transported over a single dark fiber.

In order to provide secured fiber optic link, a combination of protection methods must be in place: physical on-site protection, secured management protocols, encryption, and monitoring. This combination provides network administrators with the tools they need to prevent, detect, isolate and counter any potential or occurring data hacking attempt.

Malicious fiber tapping is one of the main causes of degradation in the fiber attenuation. PacketLight's solutions provide advanced fiber monitoring capabilities between two sites in real-time, and provide system alerts in case of significant optical power degradation. Tapping can then be quickly identified and any damage, remedied.

The Challenge

Hackers and cyber attacks pose strategic threats to any enterprise. Fiber can be hacked using simple, available, tools and information is easily stolen. This has led to the realization that owning your own dark fiber infrastructure is no longer a guarantee for data security, and that security of the optical link itself is essential. Data encryption methods previously used only by military and intelligence services have become common practice in all data transfer networks across all platforms, in all industries.

Challenges of Encrypting Links

The first challenge is the need to encrypt all the data transmitted over the fiber, without any loss of information during the encryption process. Encryption must be transparent, and maintain full bandwidth of the traffic. This also includes the need to keep latency low, especially in the financial industry, where a millisecond delay can be crucial.

The second challenge is the need to comply with government laws and regulations aimed at protecting essential (e.g. financial and medical) infrastructures. Many local governments have their own set of rules and protocols, and they must be adhered to in order to be able to secure business opportunities.

The third challenge is the need to interface with existing DWDM infrastructure and Telco OTN networks, without the need to replace or upgrade Layer-2/3 switch/routers. The solution must be vendor-agnostic so that enterprises are not faced with the costly task of changing or replacing their existing infrastructure.

The Solution

The encryption solution ensures high security level of the fiber infrastructure by combining cryptographic protection of the service data flow, firewall, secured management protocols, password-protected role-based user authentication, and optical link power level monitoring. The solution resolves three major concerns in optical link security:

- **Confidentiality** - preventing disclosure of information to unauthorized parties
- **Data integrity** - ensuring that the message has not been altered
- **Authentication** – validating that the parties involved are who they claim to be

Optical link security provides network administrators with the tools to identify fiber tapping by detecting unexplained degradation of the link power. This has made Layer-1 (the physical layer) security a key part of a total cyber-security solution.

The solution performs GCM-AES-256 encryption on Layer-1 of the client signal, supporting full bandwidth of the 1/10/40/100G services. It is NIST FIPS 140-2 and Common Criteria ELA2 certified, and compliant with NSA Suite B requirements for GbE/10/40/100Gb Ethernet, as well as 4/8/10/16/32G FC, STM64/OC-192 SONET/SDH, and OTU2/3/4.

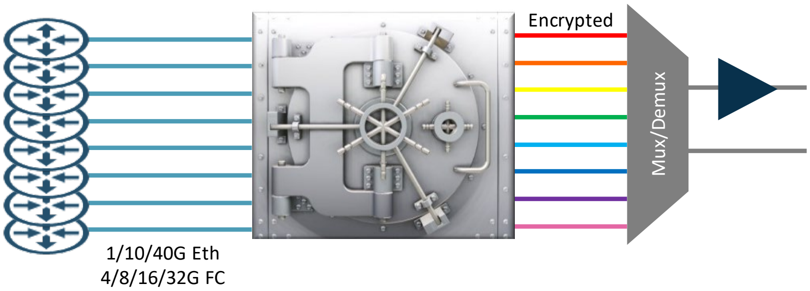

Figure 1: Encryption Mechanism

Three types of encryption solutions:

1. Encryption of services in OTN network with role-based and port-based separation (PacketLight PL-2000M, PL-2000AD, PL-2000ADS, PL-2000T)
2. Encryption feeder that connects to an existing OTN network (PacketLight PL-2000ADS)
3. Point-to-point encryption, and encryption feeder (PacketLight PL-1000TE)

Encryption of Services in OTN

The optical transport network (OTN) encryption solution provides enterprises and carriers with extended Layer-1 encryption capabilities across metro and long haul routes. The solution maintains a cost-effective approach to delivering bundled encryption solutions within the 200G multiprotocol multi-rate muxponder/transponder/ADM offering. The solution is simple to deploy in any environment with minimal cost and time, as it is agnostic to the equipment vendor and type, and does not require any changes to existing Layer-2 and Layer-3 switches and routers in the network.

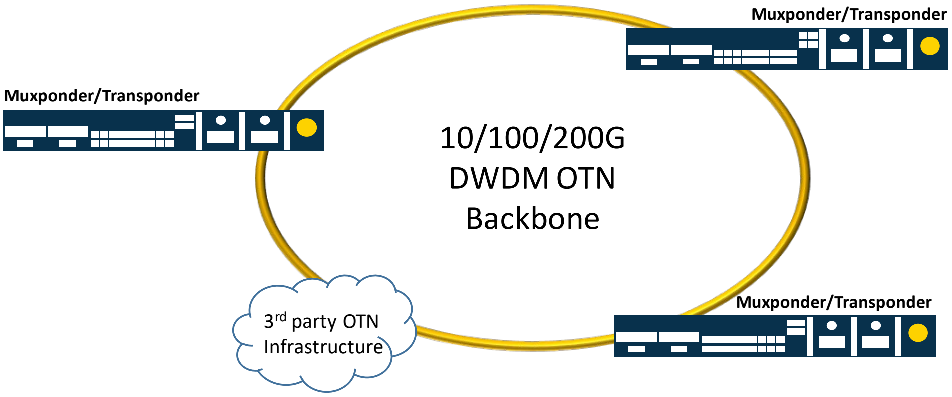

Figure 2: Encryption Solution on Ring Connectivity

Encryption Feeder

A 200G 1U multi-protocol multi-rate ADM/muxponder/transponder solution provides enterprises and data centers with modular, standalone 200G Layer-1 encryption solution. The solution acts as a vendor-agnostic encryption feeder, allowing enterprises with a DWDM network to benefit from encryption without altering their infrastructure.

The product is FIPS 140-2 Level 2 and Common Criteria EAL2 compliant, and provides GCM-AES-256 bit encryption and key exchange based on the Diffie-Hellman (DH) protocol, without compromising performance.

The solution is ideal for short haul 100G connectivity and Layer-1 encryption such as:

- Last mile access/aggregation CPE for 10G/40G/100G managed service
- High capacity, short haul enterprise, and campus networks
- Dynamic add/drop of services in ring and linear add/drop topologies
- Encryption feeder solution to any third party OTU4 transponder card
- Up to 200G Layer-1 encryption solution for 10G/40G/100G service
- High bandwidth connectivity for data center and cloud computing

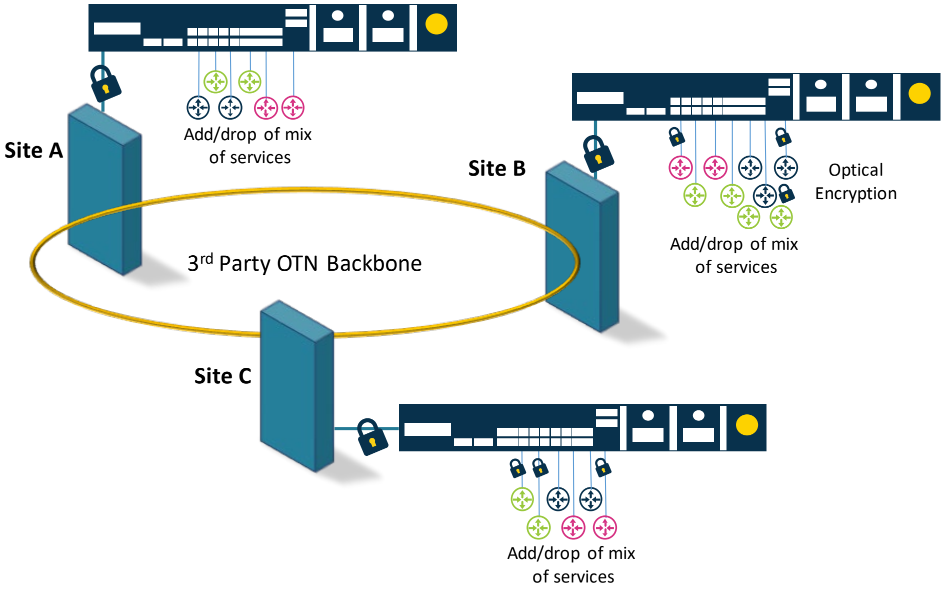
Site A
Add/drop of mix of services
Site B
Optical Encryption
Add/drop of mix of services
3rd Party OTN Backbone
Site C
Add/drop of mix of services

Figure 3: Encryption Feeder Solution

Point-to-point Encryption

This solution enables secured fiber network infrastructure and data center connectivity for industries such as government, financial institutes (such as banks and credit card companies), cloud providers and ISP backbone, and utilities and essential infrastructure.

Point-to-point encryption is transparent to the traffic without any degradation to the DWDM link performance or to the QoS of transferred data, and low latency of less than 12 usec for 10G Ethernet. The solution includes fiber tapping alarm and can work as either a feeder of encrypted services to existing OTN, or as a managed encrypted wavelength service offered by service providers.

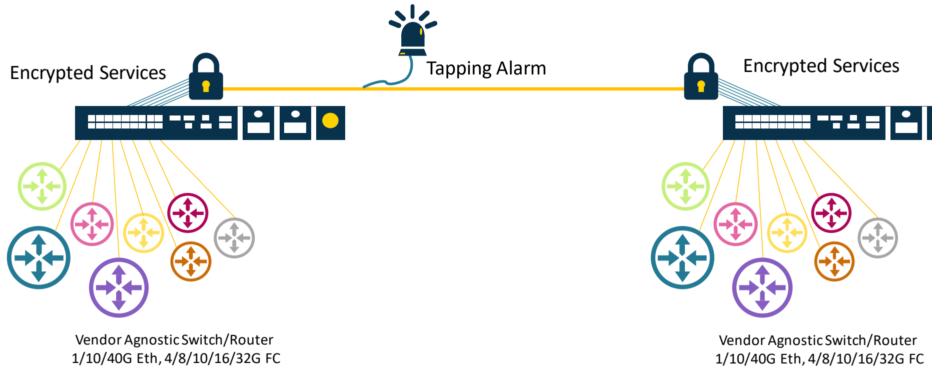
Encrypted Services
Tapping Alarm
Encrypted Services
Vendor Agnostic Switch/Router
1/10/40G Eth, 4/8/10/16/32G FC
Vendor Agnostic Switch/Router
1/10/40G Eth, 4/8/10/16/32G FC

Figure 4: Encryption Solution for Point-to-point Connectivity

The solution supports independent vendor-agnostic bi-directional encryption/decryption machines, where each port can be configured to a different service rate/type, and has its own key exchange and pre-shared secret. In this solution each service is isolated and encrypted independently of the others. The user can flexibly activate the encryption/decryption functionality for specific transponders and wavelengths.

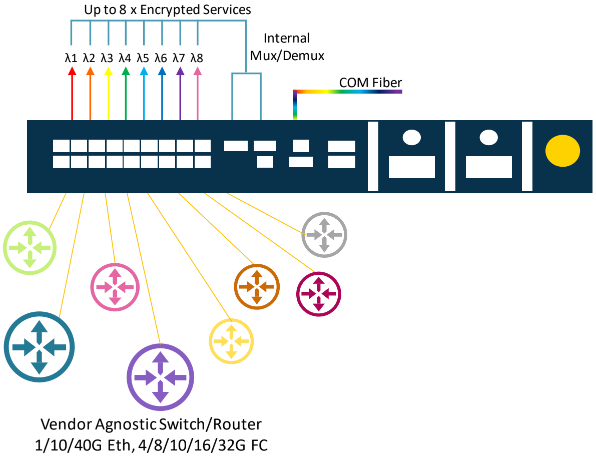
Up to 8 x Encrypted Services
Internal Mux/Demux
λ1 λ2 λ3 λ4 λ5 λ6 λ7 λ8
COM Fiber
Vendor Agnostic Switch/Router
1/10/40G Eth, 4/8/10/16/32G FC

Figure 5: Connecting to Multiple Services

Applications

The Layer-1 encryption solution is agnostic to the application layer and the SAN and LAN equipment used, which makes it cost effective and simple to deploy. The solution integrates with existing WDM infrastructure and encrypted wavelengths and can be added at any time with no impact on the existing applications.

Recommended applications:

- High capacity DCI for enterprise, campus and cloud computing networks
- Ring and linear networks
- Secured optical encrypted communication for all protocols
- Building efficient transport long haul networks with 2500 km spans
- Increasing capacity and spectral efficiency of existing 10G/40G/100G OTN/DWDM long haul and metro networks
- Mix of muxponder and transponder
- Last mile access/aggregation CPE for GbE/10/40/100Gb Ethernet, 8/16/32G Fiber Channel managed services
- Building backbone for utility, oil and gas, and mining industry
- High conformance 100G for alien wavelength applications

Government Institutions

Government institutions have already awakened to a reality in which hacking information is a daily occurrence, and the understanding that protecting private information is crucial. In some countries, legislation has already been put in place, which requires all enterprises to encrypt and protect information transmitted and stored. This especially applies to government-related information such as tax, health and social security.

Financial Institutes

The need for data security is growing among all financial institutes due to the high sensitivity of financial data and transaction flow between data centers. In some countries, legislation requires encryption of the data transmitted over fiber between data centers. The typical encrypted interfaces are the GbE/10/40/100Gb Ethernet and 4/8/10/16/32G Fiber Channel protocols used for data and storage transport.

Cloud and Data Centers

One of the major challenges for cloud and data center service providers is the link security, since the enterprise's most vital information is sent between locations typically over fiber. In most cases, there is a core router located at the main data center site and through it different streams of services and end users are carried. The need for full throughput encryption of the connections between the core routers of the data centers is obvious. PacketLight's product offers cost effective, transparent, high security solution for such service providers.

Encrypted Wavelengths over OTN Networks for Service Providers

Service providers are operating in an extremely competitive market. Offering value added services to distinguish themselves among the other service providers is one of the essential challenges for their business. Encrypted wavelength is one of the value added services that can be offered in a cost effective way with PacketLight's most compact high bandwidth DWDM CPE solutions with guaranteed short term ROI for the equipment. The encryption is enabled or disabled per each interface independently and is applied transparently to the client as a part of the DWDM service. The encryption supports the most common FC and Ethernet signals and is configured flexibly by the user to the type and service rate.

The same box is used for transparent DWDM managed service and encrypted solution, so the encrypted WL service is a "no brainer" addition to the service provider's offerings. The encryption can be configured either by the cryptographic officer of the end enterprise or by the service provider as different level of permissions are supported for the encryption functionality.

Solutions Discussed in this White Paper

PL-1000TE Layer-1 DWDM Encryption - multi-rate, multi-service DWDM transponder with cryptographic capabilities. Click here for more information.

PL-2000M 200G Single Wavelength Muxponder - 200G multi-protocol multi-rate muxponder/transponder for building high capacity 200G encrypted optical transport networks. Click here for more information.

PL-2000AD 200G ADM for Long Haul - 200G multi-protocol multi-rate muxponder/transponder/ADM solution for building encrypted 100G high capacity optical transport networks. Click here for more information.

PL-2000ADS 200G ADM for Short Haul - 200G multi-protocol multi-rate muxponder/transponder/ADM solution for encrypted 100G high capacity optical transport networks, and Layer-1 encryption. Click here for more information.

PL-2000T - 800G 8 x 100G Transponder - highly integrated solution with four 200G pluggable optical modules, delivering up to 8 x 100Gb Ethernet or OTU4 in a 1U chassis. Click here for more information.

Find out how PacketLight's encryption solutions and product portfolio. Contact info@packetlight.com

About PacketLight

Established in 2000, PacketLight Networks™ offers a suite of leading 1U metro and long haul CWDM/DWDM and OTN solutions, as well as Layer-1 optical encryption for transport of data, storage, voice and video applications over dark fibre and WDM networks. PacketLight provides the entire optical layer transport solution within a highly integrated compact platform, designed for maximum flexibility, easy maintenance and operation, with real pay-as-you-grow architecture, while maintaining a high level of reliability and low cost. PacketLight works with an international network of resellers and partners to provide you with a complete set of network services, with installations worldwide.