

# Mitigating Carrier Ethernet Security Risks

## Mitigating Carrier Ethernet Security Risks

Ethernet services offer tremendous benefits for enterprises, including highly flexible bandwidth options, the ability to quickly and easily increase bandwidth to meet ever-growing application bandwidth demands, and simplified network operations through a common technology for both LANs and WANs. Ethernet technology was originally developed as an in-building, LAN technology for a single organization, and its plug-and-play capability is one of its key benefits. Ethernet technology has been augmented over the years to improve security, but at the expense of additional complexity in network deployments. Such technologies included the introduction of Virtual LANs (VLANs) in IEEE 802.1Q, authentication via IEEE 802.1x (EAP) and IEEE 802.1ae (MACsec) and network access control solutions.

Despite these security improvements, prospective enterprise Ethernet service subscribers know Ethernet predominantly as a LAN technology where all user data is multiplexed over the network with limited separation or isolation. Furthermore, Ethernet service deployments using IEEE 802.1ad (also known as QinQ or VLAN stacking) expose the enterprise subscriber's host MAC addresses even though the Ethernet frame's IP payload may be encrypted. Therefore, the network is vulnerable to external threats such as MAC address spoofing, passive monitoring, man-in-the-middle attacks and MAC Denial of Service (DoS) attacks.

## Security Business Drivers

Information privacy and protection are significant concerns for enterprises, especially for any traffic that traverses the metro or wide area network. In addition to information security, enterprises in vertical markets such as finance, government, healthcare, retail and manufacturing have additional concerns such as disaster recovery and business continuity planning (DR/BCP). DR/BCP implementations are more critical than ever with businesses and governments due to significant natural and unnatural disasters over the past several years. Additionally, many forms of government legislation have information privacy and protection requirements with steep financial penalties for non-compliance. Such legislation includes the

Sarbanes-Oxley Act for all corporations whose securities are publicly traded on a U.S. stock exchange, the Health Insurance Portability and Accountability Act (HIPAA) for any organization that manages personal healthcare information transactions, the Payment Card Industry (PCI) data security standard for any organization processing financial transactions via credit/debit cards, and the Federal Information Processing Standard (FIPS) security requirements for transactions between U.S. Federal government civilian agencies and contractors.

## Networks Evolving to Meet New Security Requirements

For years, organizations have relied on and trusted their TDM-based private lines transported over dedicated SONET/SDH channels, and many enterprise IT managers are reluctant to trust their private data over a packet switched public Ethernet network. Organizations encrypt their IP VPN data when traversing the Internet. However, it is often impractical or cost-prohibitive for enterprises to encrypt their sensitive data on their private metro or wide area networks. As part of their network operations, service providers must correlate their network events and alarms to provide real-time situational awareness of potential threats, enabling them to identify and terminate an attack before it can seriously disrupt services to their customers.

## Easing Security Concerns of Ethernet Services

Service providers are also concerned about network security because they want to mitigate subscriber service disruptions and network downtime. By delivering Ethernet services with carrier Ethernet equipment supporting next-generation SONET/SDH using the Generic Framing Procedure (GFP), Virtual Concatenation (VCAT) and Generalized MPLS (GMPLS) technologies, service providers can significantly ease security concerns. There are several specific options.

Ethernet private line (EPL) services utilize Ethernet as the user network interface (UNI) to connect the enterprise's equipment to the public network and deliver site-to-site (point-to-point) services over one or more dedicated

SONET/SDH channel. EPL services provide the high availability, reliability, QoS and security that enterprise IT managers have become accustomed to with their TDM private line services, but with Ethernet's flexibility to meet growing bandwidth demands within their OpEx budgets. It's no wonder that EPL services have been, by far, the most popular Ethernet service offering worldwide for many years.

Now, a relatively new type of Ethernet service, referred to as an Ethernet Private LAN (EP-LAN) service, is emerging. EP-LAN provides the same benefits of EPL services (including secure delivery over dedicated SONET/SDH channels), and also enables multi-site connectivity. EP-LAN services provide an Ethernet UNI to connect the enterprise locations to three or more sites, extending the enterprise LAN over a metro or wide area network with the same availability, reliability, QoS and security of SONET/SDH transport networks. Many assume that multi-point E-LAN services can only be offered via IP/MPLS (VPLS) or switched Ethernet transport networks, but EP-LAN services can be very efficiently and cost-effectively delivered via carrier Ethernet equipment supporting next-generation SONET/SDH transport.

By using Ethernet-over-SONET/SDH technologies, service providers can utilize dedicated and diversely routed channels for transporting point-to-point EPL services or multi-point EP-LAN services across the public MAN and

WAN infrastructure with the highest possible level of security. Next-generation SONET/SDH networking equipment encapsulates the enterprise's Ethernet frames using GFP and diversely routes them across non-contiguous SONET/SDH channels using VCAT. GMPLS enables the dynamic assignment of SONET/SDH channels as new services are activated. These technologies effectively "scramble" the enterprise's Ethernet frames across the SONET/SDH network, making it impossible to eavesdrop, reassemble or redirect them—even if monitoring test equipment is placed in the SONET/SDH optical path, only Ethernet service frame fragments can be recovered.

Ethernet service bandwidth can easily and efficiently be added using the SONET/SDH Link Capacity Adjustment Scheme (LCAS). LCAS enables the service provider to dynamically increase or decrease bandwidth to an existing Ethernet service without any service disruptions. This capability enables Ethernet service providers to achieve maximum network bandwidth efficiencies on par with any packet switched networking technology.

### Ethernet Services without Angst

Ethernet services delivered over next-generation SONET/SDH transport networks using GMPLS, GFP, LCAS and VCAT enable enterprises to receive the highest service availability and QoS, along with the bandwidth scalability and ubiquity of Ethernet. Ethernet Private Line and Ethernet Private LAN services also provide the inherent security of SONET/SDH networks via GFP Ethernet data encapsulation and Ethernet data scrambling via VCAT's diverse routing of Ethernet frames and GMPLS's dynamic selection of SONET/SDH channels.

Despite the security concerns that have been associated with Ethernet, service providers can leverage and extend their existing SONET/SDH network infrastructure to provide secure, end-to-end Ethernet services that extend enterprise LANs around the world.

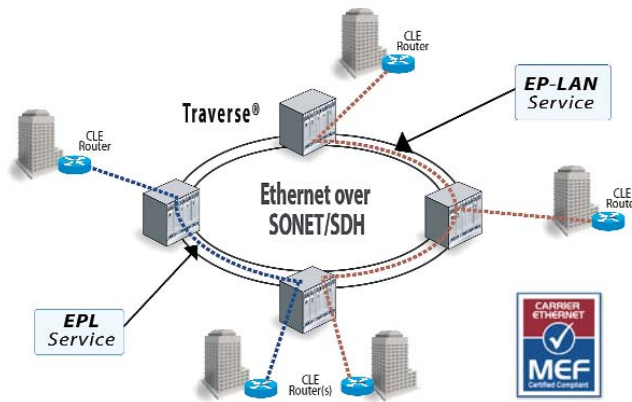


Figure 1. Ethernet Private Line (EPL) and Ethernet Private LAN (EP-LAN) Services