

Ethernet WAN Security
How to Protect
Business-Critical Data over
High-Speed Ethernet
Networks



OVERVIEW

Universal connectivity is essential in today's complex business environments. Driven by the convergence of data, voice and video over sophisticated and expanding networks, growth in demand for bandwidth is outpacing Moore's Law to supply sufficient throughput. To meet this increasing demand, organizations are looking not only for larger network pipes but also for finer granularity and more efficient ways to use existing bandwidth. As a result, more and more companies have been considering native Ethernet to carry data over wide area networks (WANs). Ethernet delivers highly scalable granularity—from 1 Mbps to 10 Gbps—while providing lower per-port capital expenditures than traditional WAN technologies,

When investigating ways to increase the efficiency of securing high-speed WAN links, many companies have discovered the true cost of the overhead associated with encrypting at Layer 3 using IPsec in the router. At the small average packet sizes typical in today's converged networks, IPsec overhead reaches 40-50 percent of total bandwidth, with associated costs climbing to thousands of dollars per month. By contrast, Ethernet encryption at Layer 2 virtually eliminates overhead, and lowers total cost of ownership by streamlining security measures, simplifying security policy management, and eliminating the inefficiencies associated with conventional Layer 3 security. For example, in large organizations, administrators commonly are forced to reconfigure Layer 3 security policies and routing tables daily, increasing system vulnerabilities and raising the risk of misconfigurations that can cause network outages.

THE ETHERNET MARKETPLACE

Carriers deploying new infrastructures worldwide are choosing Ethernet as their preferred transport technology. Evidence of this trend includes a steady increase in sales for Ethernet Edge switches. Corporate customers are extending Ethernet at an increasing rate to WAN environments but are somewhat polarized in their selection of transport method. In a 2007 study by Current Analysis, 62 percent of respondents stated that they use Ethernet directly over optical fiber, while 40 percent use Ethernet riding on a SONET transport. Looking beyond Ethernet use for private connectivity, 38 percent of respondents indicated that they use Ethernet as a transport for dedicated Internet access. Industry trends indicate that Ethernet transport for private connectivity or for dedicated Internet access is growing in popularity and will begin to eclipse SONET in the near future.

The most common topology for Ethernet implementations is point-to-point, with 63 percent of participants in the Current Analysis study citing this type of configuration. Multipoint to multipoint (mesh) architectures account for 23 percent of implementations. However, many industry observers feel that figures for mesh Ethernet implementations will rise as availability increases.

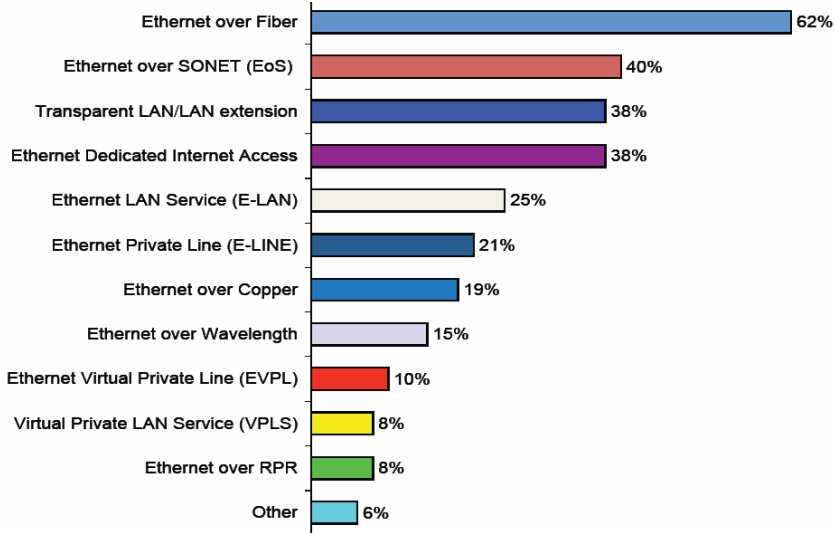


Figure 1: Type of Ethernet Services Used (Source: Current Analysis, 2007)

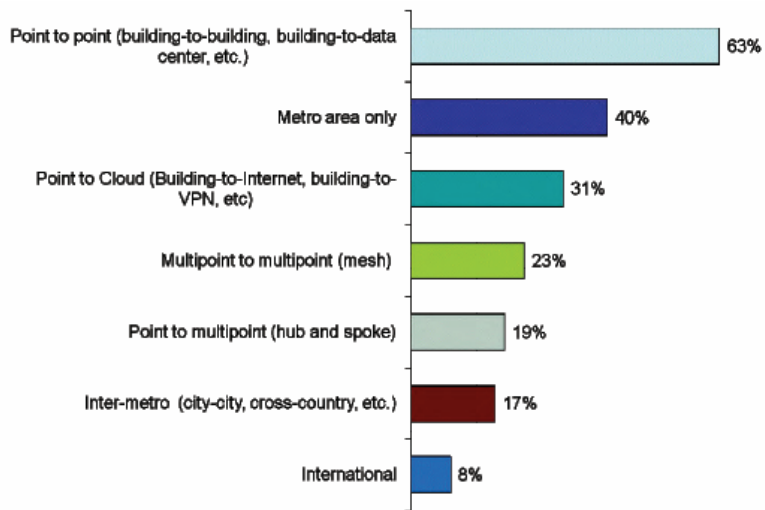


Figure 2: Most Common Ethernet Topologies (Source: Current Analysis, 2007)

Strong trend toward EPLs and EVPLs

A 2007 Heavy Reading study supports these findings by confirming that operators are becoming very ambitious in their Ethernet investments. It also indicates that as these providers increase expenditures related to Ethernet services—versus traditional TDM services such as SONET—they are investing substantially in point-to-point architectures. Specifically, they are delivering Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL) services. EPL provides point-to-point services dedicated to the customer. EVPL is also a private, point-to-point service, but offers a shared bandwidth, with associated efficiencies and cost advantages. Both within and between metro areas, EPLs and EVPLs are the dominant offerings worldwide partly because carriers can leverage their installed base of SONET/SDH MSPPs to deliver these capabilities. Services of this type are expected to be increasingly available to the market, and will likely expand in popularity as time goes by.

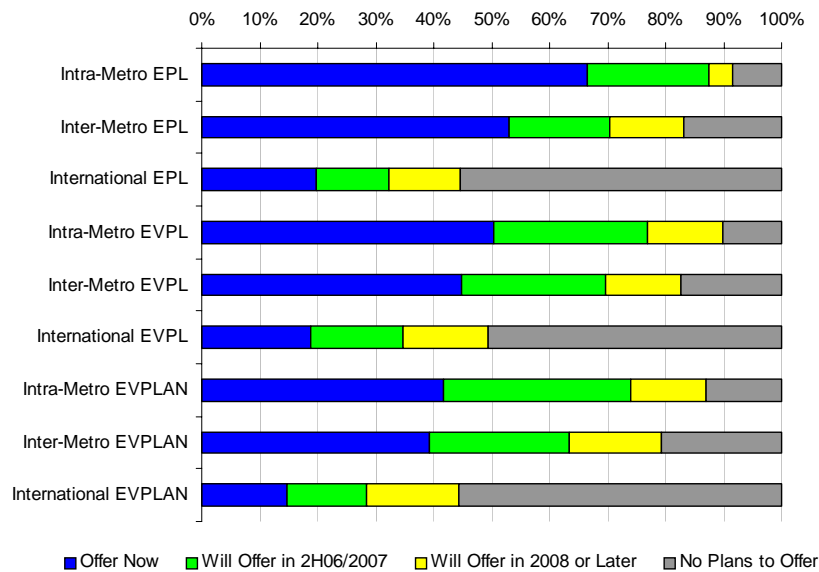


Figure 3: Operators Plan to Expand Ethernet Services
(Source: Heavy Reading, 2007)

In the past two years there has been an explosion in the number and types of Ethernet connectivity services available in the market. Survey feedback indicates that market competition may increase even further in the coming year. Operators will continue to expand their Ethernet portfolios and new players are expected to enter the market. Over 80 percent of respondents in the Heavy Reading study said that their companies planned to provide EPL, EVPL, and EVPLAN services within metro and national markets by the end of 2008. This is much higher than the currently available numbers associated with metro and national services, which range between 39 percent for inter-metro EVPLANs and 66 percent for intra-metro EPLs. This means that enterprises will shortly have a wider range of choices as they shop for Ethernet WAN services.



Granular scalability

Ethernet WAN connectivity is typically implemented to link two or more locations within multi-site organizations. These organizations are beginning to replace dedicated leased lines, Frame Relay and ATM implementations with Ethernet, which offers greater flexibility and ease of use. Physical Ethernet interfaces are available in 10-megabit, 100-megabit, 1 gigabit and 10-gigabit speeds. In addition, bandwidth can be scaled granularly from 1-megabit to 10-gigabits in 1-megabit increments. This means that organizations can pay for bandwidth according to how much they actually use rather than having to make large jumps in bandwidth when they exceed their existing link capacity.

ETHERNET SECURITY CHALLENGES

As with any transport technology, precautions must be made to protect data as it travels across the network. To ensure data security, organizations must maintain the availability, integrity and confidentiality of information in transit. Availability implies fighting against denial of services attacks. Integrity means that data recipients can trust the source and the data itself, i.e., can have confidence that the person who sent the data is actually the sender indicated and that the data is exactly what that person originally sent. Confidentiality refers to guarantees against eavesdropping.


Compliance driven security

A continually expanding number of regulations at the regional, national and international level place great pressure on organizations to increase and report on the effectiveness of data security measures. Familiar mandates include HIPAA in healthcare, Sarbanes-Oxley (SOX) for integrity and privacy in the financial world, and the Family Educational Rights and Privacy Act (FERPA), which controls private student records, grades and related information. California State Bill 1386 and similar laws in other states establish a model for controls related to data breaches. There are even greater requirements in Europe and Asia for ensuring data privacy. Other relevant national and international legislation includes SOX Japan, Basel II in Europe, Gramm Leach Bliley (GLBA) in the US, the EU Data Protection Directive, and the Payment Card Industry Data Security Standard (PCI-DSS).

Greater data value, higher risk

As more and more transactions are conducted over networks, more and more value is moving through the wires, which means that even a small breach can result in staggering data leakage with associated reputation and financial losses. The types of data that are commonly associated with the highest value include intellectual property, customers' personally identifiable information, and financial, legal, medical, and classified government data.

Demonstrated threats provide clear evidence that the risks are real. A well-known case in point, cited in The Wolf Report, involved an incident of fiber eavesdropping in New York City, outside a mutual fund company's headquarters shortly before the release of its quarterly numbers. The goal was evidently to gain an advantage in illegal insider trading. Breaches of this type reveal how easily certain malicious acts can be perpetrated. For example, for under \$1,000 an individual can buy a "microbend tap" device that can tap into fiber—without removing the cable sheathing—and pull data off without anybody being able to detect the intrusion. From a practical perspective, criminals will go straight to where the money is, and as



increasing volumes of financially-sensitive information travel over networks, threats of this type can be expected to increase as well.

The cost of a security breach has been placed at \$90 to \$305 per lost record. At 10-gigabit speeds, tens of thousand of records can be compromised within seconds of breach. This implies that a company whose sensitive proprietary and company data is unprotected over a shared Ethernet transport runs the risk of sustaining devastating losses. Encryption effectively removes this risk.

Top worries of security executives

Interviews with chief security officers and information security officers reveal that regulatory compliance is their number one concern, in particular in connection with rules related to PCI, Sarbanes-Oxley and Gramm-Leach-Bliley. The unpredictability of audits is a major issue. Since auditing can take place without warning, these executives can be held accountable at any time, and must be ready at a moment's notice to effectively demonstrate compliance with mandates. Pressures are so great that many executives stated they are more worried about regulatory compliance than they are about actually securing the data.

An additional worry among security executives is the high turnover among IT professionals. Security-savvy people are the top echelon of IT. Once they are trained in security, especially if they have certification, they become highly desirable commodities and are often recruited from the outside for more attractive opportunities.

Another point that affects security decision makers involves perceptions about the source of threats. FBI studies show that 75 percent of all attacks come from within a company, which means that conventional efforts extended toward locking down data outside the enterprise focus on only 25 percent of the risk. Security methodologies must provide sufficient protections against internal as well as external threats.

HIGH-SPEED ETHERNET SECURITY SOLUTIONS


All of the concerns expressed by security officers can be addressed with a full-featured Ethernet security solution that delivers:

- advanced audit reporting for regulatory compliance;
- transparent Layer 2 security for maximum efficiency and ease of use;
- streamlined, roles-based administrative capabilities to eliminate the need for highly technical personnel; and
- built-in, easy-to-manage controls over the internal encryption network for protection against internal risk.

Encryption over high-speed Ethernet

With an Ethernet solution, everything in a network pipe is either encrypted or not encrypted based on source and destination MAC addresses, removing complexity, providing clear evidence of encryption at appropriate places, and ensuring transparency for Layer 3 data. This makes it possible for IP, AppleTalk, Token Ring, or any other kind of traffic to be transmitted transparently over Ethernet.

Ethernet encryption solutions can be used in a variety of enterprise configurations. For example, a company could use it for high-speed intra-



office connectivity, linking corporate LANs, core offices, data centers and network operations centers. Ethernet encryption is also effective for high-speed MANs (metropolitan area networks), protecting data and networks for captive networks and corporate campuses in the metro area. In addition, it is suitable for high-speed edge applications such as service aggregation, triple play (voice, video, data), VoIP aggregation, streaming video, and wireless LANs. It also makes sense for any situation where servers are being centralized, including server farms and SANs (storage area networks). Finally, high-speed WANs are well served by Layer 2 Ethernet encryption solutions, where protection can be applied to network backbones, LAN extensions in multinational organizations, and wireless backhaul.

Benefits of dedicated encryption devices

One of the first decisions to make when implementing an Ethernet encryption solution is whether or not to use a dedicated device. In general, dedicated devices provide a range of operational and financial benefits:

Increased security: Dedicated devices are designed specifically for a particular function, separating human managers (and associated risks) from the IT information.

Cost savings: Layer 2 devices eliminate bandwidth overhead—and associated telecom costs—for expensive transport pipes, and provide the full throughput available with Layer 2 Ethernet. They also reduce administrative costs. With Layer 3, administrators must continually cope with VPN rules, policies, and the tunneling of data or connections from point to point. Every time a new device is added to a mesh architecture, for example, all the connections have to be configured in complex routing tables. By contrast, the same change with Layer 2 security would only require adding a security authentication certificate, allowing other devices to talk to the new device securely without excess management time and costs. Overall advantages include simple deployment, ease of management and lower total cost of ownership.

Quality of service (QoS): Dedicated devices provide efficient support for VoIP, international video conferencing, and other real-time applications without the need for complex QoS schemes.

Increased performance: Layer 2 devices eliminate the excessive overhead in latency and throughput experienced with Layer 3. This is especially true at smaller packet sizes, where overhead is often 50 percent or higher. One obvious indicator of the difference lies in the fact that Layer 3 latency is measured in milliseconds, whereas Layer 2 latency is measured in only microseconds, providing clear evidence of reduced latency over Layer 2.

Advantages of Layer 2 encryption

An independent study by the Rochester Institute of Technology (RIT) demonstrated that the potential benefits of costly transport services can be seriously overshadowed by loss of throughput, often increasing rather than decreasing total cost of ownership due to excessive management and bandwidth overhead issues. As shown below, the findings determined that Layer 2 encryption technologies provide superior throughput and far lower latency than IPsec VPNs, which operate at Layer 3.

In Figure [x] (below), theoretical throughput losses fall in the 50 percent range, primarily reflecting overhead. However, actual IPsec blades perform even worse, with small frame sizes showing a loss of almost 80% of the 1-gigabit throughput. By contrast, with an Ethernet encryptor (in this case a SafeNet 1-gigabit device), the overhead is eliminated. The cost implications of this comparison are enormous, since companies may currently be paying huge prices for an expensive pipe while losing 80 percent of the throughput.

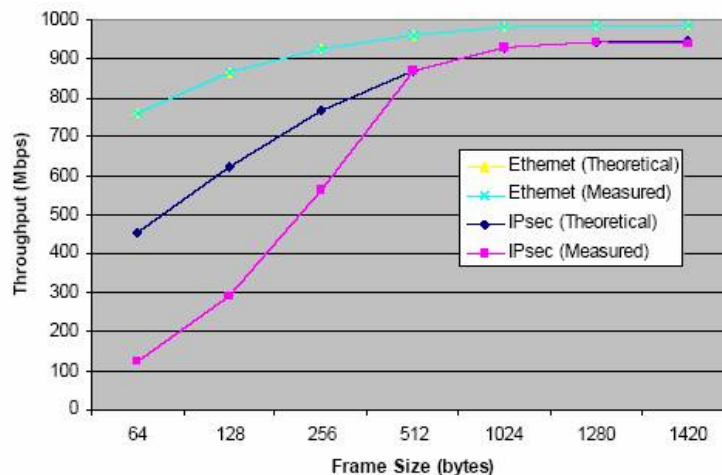



Figure 4: Comparison of Theoretical with Actual Measured Throughput (Source: RIT, 2006)

In part, the RIT study states: “Overwhelming logic suggests that, from a theoretical performance perspective, Layer 2 Ethernet encryption should be superior to Layer 3 IPsec encryption. The current battery of tests, and data generated in the study[s], confirm[s] the reality of the throughput and latency limitations induced by the IPsec wrapper overhead. Testing exposed the detrimental effect on network performance that is typically imposed by IPsec’s innate processing requirements, as well as the processing limitations of the tested IPsec hardware.”

It also states: “In contrast, the SafeNet Ethernet Encryptor operates at line speed. Testing also revealed no significant frame loss with the SafeNet Ethernet encryption solution, whereas significant frame loss was encountered at comparatively low data rates with the IPsec solution. This resulted in a significant reduction of the data rate, as seen in throughput testing, and indicates that achieving line rate encryption, even at the reduced maximum theoretical throughput of IPsec, is impossible at regardless of frame size with the IPsec solution.”



Studies such as this emphasize that in small frame sizes (e.g., 64 byte)—which are being driven more and more by real time applications, such as voice processing, imaging, and simulation programs—nearly 50 percent of potential throughput is wasted. Simple put, a 1-gig pipe becomes a 500-megabit pipe.

Another benefit of Ethernet is that, once it is installed for infrastructure connectivity, all Layer 3 transports are supported transparently, including IPv6. Options include Ethernet over Layer 2 MPLS, Metro Ethernet, Ethernet over SONET, Ethernet over BWDM or CWDM, and wireless applications. Even DSL is supported using MAC-level Ethernet over copper services.

Centralized management platform

To ensure best performance, lowest costs and maximum ease of use, a Layer 2 Ethernet encryption solution should provide a complete solution for centralized management of the security architecture. Key capabilities include strong configuration management for adding and managing devices, along with simplified fault and alarm management features that make it easier to identify, isolate and solve problems. In addition, there should be a consolidated view of network of encryption devices, a network-wide policy manager and secure audit reports. Devices themselves should deliver the capabilities described above, providing wire speed throughput and low latency. Ideally, management features should be easy to learn and use, removing the need for costly personnel and training, and offering efficient, flexible methods for managing high-speed Ethernet data protections across the enterprise.

SAFENET HIGH-SPEED ETHERNET SECURITY SOLUTIONS

SafeNet SafeEnterprise™ Ethernet Encryptors are a family of high-performance Layer 2 security appliances that protect 10Mbps, 100Mbps and GbE Ethernet networks. With seamless end-to-end integration on metro Ethernets, SafeEnterprise Ethernet Encryptors deliver instant protection across the network at Layer 2, with cut-through data streaming for low latency. SafeNet encryptors operate transparently, and unlike Layer 3 encryption solutions, have minimal impact on the network.

With SafeEnterprise™ Ethernet Encryptors, payload data is encrypted up to the MAC address, ensuring that data is completely secure. A cryptographic payload offset feature permits users to offset deeper into the frame (supporting VLAN tagging and MPLS shims), thus permitting the solution to accommodate multiple architectures. These devices are also designed to international Common Criteria and U.S. Government FIPS security standards (FIPS 140-2 Level 3 accredited).

Like all SafeNet high-speed security appliances, the SafeEnterprise Ethernet Encryptor is managed by the SafeEnterprise Security Management Center (SMC), a robust, Web-based policy management application with secure, flexible, and transparent SNMP-based control and monitoring capabilities. SMC provides the ability to define integrated security policies that can be centrally and remotely distributed across multiple devices, reducing management complexity and cost.

Layer 2 vs. Layer 3 – Security Overview

The following is a breakdown of the comparative characteristics of Layer 2 and Layer 3 encryption technologies, detailing the benefits of SafeEnterprise Ethernet Encryptors:

	Layer 2 (e.g., Ethernet)	Layer 3 (e.g., IPsec)
Performance	<ul style="list-style-type: none"> ▪ Throughput up to 10Gbps ▪ No performance degradation for small-packet traffic (real-time VoIP, video) ▪ Virtually no latency ▪ No bandwidth wasted for security overhead 	<ul style="list-style-type: none"> ▪ Throughput up to 1Gbps ▪ Poor performance especially for small-packet traffic (real-time VoIP, video) ▪ High latency, especially for small-packet traffic ▪ Up to 50% of bandwidth wasted by security protocol overhead
Ease of Integration and Maintenance (Simplicity)	<ul style="list-style-type: none"> ▪ Easy to integrate, plug-and-play ▪ Virtually no maintenance required ▪ Separates physical network from security 	<ul style="list-style-type: none"> ▪ Hard to integrate into IP networks due to IP address management issues ▪ Changes in network setup impact security ▪ Changes to network require frequent policy changes and cause inadvertent network outages
Depth of Security	<ul style="list-style-type: none"> ▪ Default mode of operation is fully secure ▪ FIPS 140-1/2 and CC-certified hardware ▪ Supports latest encryption standards such as AES-256 	<ul style="list-style-type: none"> ▪ Provides more granular security options which leaves room for errors in security implementation (e.g., unencrypted connections)
Reliability	<ul style="list-style-type: none"> ▪ Highly resilient ▪ Changes in IP layer do not affect Layer 2 security 	<ul style="list-style-type: none"> ▪ Changes in IP network (e.g., IP address changes) can interfere with security setup
Cost	<ul style="list-style-type: none"> ▪ Cost-effective security solution requires only minimum number of encryptors to secure entire circuits 	<ul style="list-style-type: none"> ▪ Fast IPsec encryptors are expensive ▪ 10Gbps solutions are scarce and are cost prohibitive



About SafeNet, Inc.

SafeNet is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Internal Revenue Service and scores of other customers entrust their security needs to SafeNet. In 2007, SafeNet was taken private by Vector Capital.

For more information about SafeNet's solutions for high-speed network encryption, please visit www.safenet-inc.com/HSE.

