

Understanding layer 2 encryption

At first glance encryption seems an easy choice; after all why expose confidential information to prying eyes when you can protect it by scrambling?

Some of the traditional objections to encryption include loss of performance and the complexity of managing encryption keys.

Today however modern hardware and software systems have whittled away these issues to the extent that it is now possible to deploy hardware encryption to secure information at full line rates up to 10Gbps and with simple fully automatic key management.

Where to encrypt ?

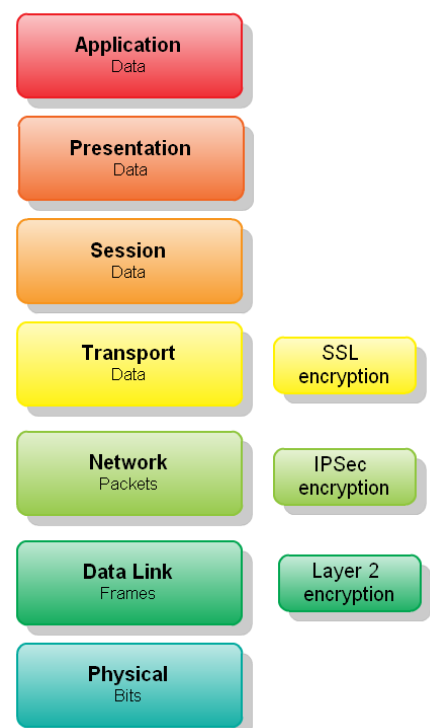
There are several ways to encrypt data in motion; common options include Secure Sockets Layer (SSL) for the Internet, the IPSec standard (or layer 3 encryption) for "tunneling" and layer 2 encryption.

The word "layer" refers to the way in which network communication systems are designed, for example layer 1 is the physical layer (wire, cables, connectors etc), layer 2 is the data link layer (eg ethernet frames) & layer 3 is the network layer (eg IP packets).

In reality, encryption can happen at different layers of a network stack, the following are just a few examples:

- End-to-end encryption happens within applications.
- SSL encryption takes place at the transport layer.
- IPSec encryption takes place at the network layer.
- Layer 2 encryption takes place at the data link layer.

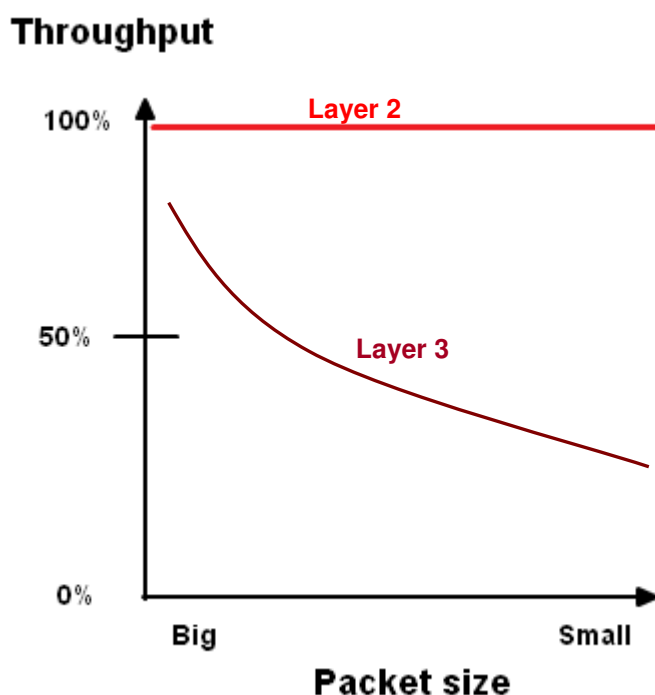
The challenge lies in maintaining the performance and simplicity of high speed networks while assuring the



security and privacy of user data, whether it be a voice, data or video transmission.

Benefits of layer 2 encryption

Layer 2 encryption is often referred to as a “bump in the wire” technology. The phrase conveys the simplicity, maintainability and performance benefits of layer 2 solutions that are designed to be transparent to end users with little or no performance impact on network throughput.



In a recent study by the Rochester Institute of Technology (RIT), it was determined that Layer 2 encryption technologies provide superior throughput and far lower latency than IPsec VPNs, which operate at Layer 3.

The RIT study concludes: Enterprises that need to secure a point-to-point link are likely to achieve better

encryption performance by shifting from traditional encryption with IPsec at Layer 3 to the overhead-free encryption of frame payloads at Layer 2.”

When contrasted with encryption at higher layers some of the additional advantages of encrypting at Layer 2 include:

- Lowest impact on network performance
- Reduced complexity (bump in the wire)
- Transparent to media (voice, data, video etc)
- Little or no configuration
- Operates at wire speed up to 10Gbps.
- Introduces no overhead. In contrast, Layer 3 IPsec typically adds significant overhead (over 40% of available bandwidth for smaller packets)
- Implementation of Layer 2 encryption devices is simple

Outsourcing of routing tables is also seen as a weakness of Layer 3 VPN services because many corporations don't want to relinquish control or even share their routing schemes with anyone, not even their service provider. They prefer Layer 2 network services, such as Ethernet, Frame Relay or ATM as these are simpler in architecture and allow customers to retain control of their own routing tables.

Senetas competitive advantage

Senetas is an Australian public company whose core business is the development of high performance encryption hardware.

Senetas has developed a comprehensive product range called CypherNet that is capable of encrypting nearly any LAN/WAN infrastructure.

Senetas leads the market in the development of true wire speed encryption technology for networks that run up to 10Gbps. By encrypting at layer 2 in the protocol stack the products run at full line speed, perform zero packet expansion and hence have the lowest overhead on the network.

CypherNet is accredited to the most rigorous independent standards for cryptographic product design including FIPS140 and EAL4. These standards are designed to provide an independent assessment of a products security and give an assurance of trust other than the vendors.

Governments and organizations worldwide use these assessments as a mark of trust for the security products they choose to encrypt their data.

Senetas's encryptors are used in some of the most demanding environments imaginable including high speed US Defence department networks in the US, AsiaPac and Europe. We also secure critical backbone infrastructure for banks and other large financial institutions globally.

Senetas is committed to assisting organizations in meeting their long-term vision of network-centric operations with highly secure reliable commercial-off-the-shelf (COTS) solutions.

Senetas' "bump in the wire" layer 2 technology has the lowest impact on network performance, is transparent to media and reduces complexity thus allowing business and Government to significantly reduce costs in meeting data protection and privacy regulations.

Senetas has a complete range of products that scale from low speed to high speed networks and a single management platform that manages the entire product range.

Key differentiators of the Senetas products include:

- Reliable field proven hardware solution
- Support for AES 256 bit keys
- Support for point-point, hub & spoke and fully meshed topologies
- Common Criteria EAL4 & FIPS 140 accreditation
- True full duplex wire speed encryption up to 10Gbps
- Single management encryption platform for link, E1, ATM, SONET & Ethernet networks
- SNMP network management
- Remote upgrade capability
- Inband and out-of-band management
- Flexible pluggable interface architecture
- Robust tamper detection
- Support for AC/DC supplies
- Redundant supply capability
- Use of pluggable transceivers for both optical and electrical connections