



PRESENTS:

**LAYER 2 ENCRYPTORS
FOR
METRO AND CARRIER ETHERNET
METROS AND WIDE AREA NETWORKS**

ETHERNET ENCRYPTION

INTRODUCTION:
PROTECTING VIRTUAL PRIVATE NETWORKS AND LAN EXTENSIONS:
LAYER 2 VS. LAYER 3

Version 3.01, April 26, 2011

© 2007-2011 Christoph Jaggi

All rights reserved. No copying, no commercial use and no republications (in part or in whole) without prior written permission of the author.

www.uebermeister.com
cjaggi@uebermeister.com

Executive Summary

Networks are unsafe. That is true for optical networks as well as for all other wired and wireless networks. It is actually quite easy to find all the tools and instructions needed. A simple search on the Internet will provide you with the necessary information. Without encryption networks passing public ground are unsafe. It is thus not a question if encryption is needed, it is only a question which encryption approach is the most efficient and the safest.

The lower the layer, the more comprehensive the protocols that can be encrypted and the more efficient the protection and the processing. The efficient encryption of all network data is only provided by encrypting at layer 2 or below. The usage scenario and the business requirements should therefore be the determining factor for the selection of the encryption layer.

Virtual Private Networks are not secure if not encrypted. The word “private” isn’t a synonym for “encrypted”, it only means that your virtual network is not shared with others. In fact your Virtual Private Network still runs on a shared infrastructure and is not secured. Carriers claim that a virtual private network is as safe as a leased line, but forget to mention the fact that leased lines are unsecured. It is also a known fact that virtual private networks run on a transport network that provides the shared infrastructure and that can be attacked.

Layer 2 and layer 3 encryptors work differently. Layer 3 encryptors are designed for IPsec encryption and to encrypt IP payload. IPsec tunnels the original IP packet, so that it can encrypt the original IP header. If you want to encrypt an Ethernet frame with IPsec, the encryptor has to lift the Ethernet frame up to layer 3, so that the Ethernet frame becomes IP payload that then can be encrypted. If you use IPsec to encrypt MPLS networks, IPsec will tunnel the original IP packet that forms the MPLS payload.

Layer 2 encryptors are designed to encrypt layer 2 and above. They are optimized for Ethernet and MPLS and don’t need to tunnel the original IP packet to encrypt IP or MPLS running over Ethernet. Encryption is most efficient if it takes place at the native layer or below.

To protect a layer 2 site-to-site or multi-site networks, layer 2 encryption just makes more sense as it can secure everything layer 2 and above and comes without built-in performance degradation. The same is true for layer 2.5 VPNs (MPLS), which can be encrypted at layer 2 without tunneling, contrary to the encryption at layer 3, which requires tunneling. From layer 2 you have direct access to all relevant network layers (2-7). The right product will let you encrypt all networks running over Ethernet MANs and WANs, Ethernet, MPLS or IP without tunneling and fork lifting. Encrypting Ethernet networks at layer 2 is faster, is simpler, more secure and more powerful.

The best solution for securing layer 2 networks is specialized, autonomous layer 2 encryptors. They come without dependencies and keep their focus sharply on their one and only job, thus operating as efficiently as possible. Processes and management are simple, straightforward and completely optimized for the job at hand. This does not only benefit performance and security, but also has a positive mid- and long-term impact on flexibility and cost. While there are different ways to integrate layer 2 encryption into other appliances and perform it as a side-job, none of those approaches provide the security and efficiency of a dedicated encryption appliance.

Contrary to encryption solutions on layer 3 (IPsec) and layer 4 (TLS) which are standardized to a certain degree, there is no standard for layer 2 (Ethernet). The information available for the existing solutions is very limited and the market completely lacks transparency.

The market overviews published on www.inside-it.ch - point-to-point and multipoint solutions - explain and show the key features of the different products. The links to the current versions of the short versions of the market overviews can be found on www.inside-it.ch. Currently version 3 (2011 edition) is up-to-date.

Table of Content

Executive Summary.....	2
------------------------	---

Ethernet Encryption: Layer 2 vs. Layer 3

1. Why encrypt at layer 2?.....	4
1.1. Networks are unsafe	
1.2. Virtual Private Networks (VPN) are unprotected	
1.3. Comprehensive encryption solutions	
2. Network layers and encryption: L2 vs L3.....	6
2.1. Different layer – different approach.....	6
2.2. IPSec encryption at layer 3.....	6
2.2.1. IPSec – The Standard for layer 3 network security	
2.2.2. Using IPSec for Ethernet encryption	
2.3. Native Ethernet encryption at layer 2.....	8
2.3.1. Native Ethernet encryption modes	
a) Bulk Mode	
b) Transport Mode	
c) Tunnel Mode	
d) MacSec/LinkSec	
e) Cisco TrustSec	
2.3.2. Site internal vs. MAN and WAN	
2.4. Security, efficiency and operational considerations.....	11
2.4.1. Security considerations	
2.4.2. Efficiency considerations	
a) Security Overhead	
b) Key System	
c) Processing Speed	
d) Scalability	
2.4.3. Operational considerations	
a) Ease of deployment	
b) Operational cost	
3. Implementation: Dedicated appliances vs. integrated appliances.....	13
3.1. Security	
3.2. Performance	
3.3. Upgradeability	
3.4. Costs	
4. Metro Ethernet Topologies for MANs and WANs.....	16
5. Ethernet encryptors: Market overview.....	16

1. Why encrypt at layer 2?

1.1. Networks are unsafe

Networks are unsafe. That is true for optical networks as well as for all other wired and wireless networks. It is actually quite easy to find all the tools and instructions needed. A simple search on the Internet will provide you with the necessary information. Without encryption networks passing public ground are unsafe. It is thus not a question if encryption is needed, it is only a question which encryption approach is the most efficient and the safest.

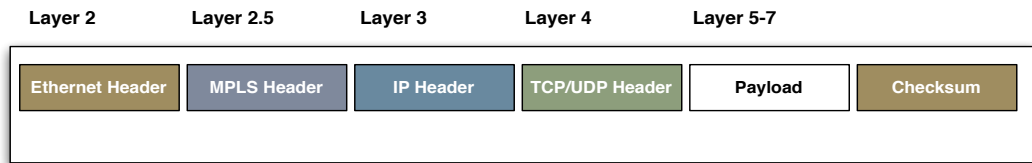
The lower the layer, the more comprehensive the protocols that can be encrypted and the more efficient the protection and the processing. The efficient encryption of all network data is only provided by encrypting at layer 2 or below. The usage scenario and the business requirements should therefore be the determining factor for the selection of the encryption layer.

Encryption Layer	Usage Scenario and Protection
Layer 7: Application Layer	Remote Access
Layer 4: Transport Layer (TLS/SSH)*	Remote Access
Layer 3: Network Layer (IP)	Remote Access Site-to-Site Network Multi-Site Network
Layer 2: Data Link Layer	Hop-to-Hop Network (Direct Link) Site-to-Site Network Multi-Site Network
Layer 1: Physical Layer	Hop-to-Hop (Wire)

*Layer 4 establishes the foundation, but the actual encryption takes place on layer 7

The diagram above shows that in order to encrypt link layer data, a layer 3 encryptor has to lift each and every layer 2 frame to layer 3 in order to encrypt the layer 2 network. Layer 3 encryptors are limited to layer 3, as they can only encrypt IP payload. Therefore for a layer 3 encryptor the layer 2 data must first be transformed into layer 3 payload, which includes some heavy lifting.

Looking at the network layers from an Ethernet perspective, the layers 2.5 to 7 follow the layer 2 header and the frame closes with the layer 2 checksum.



At layer 2 you can encrypt layer 2 and all layers above without having to resort to tunneling or encapsulation.

1.2. Virtual Private Networks (VPN) are unprotected

Virtual Private Networks are not secure if not encrypted. The word “private” isn’t a synonym for “encrypted”, it only means that your virtual network is not shared with others. In fact your Virtual Private Network still runs on a shared infrastructure and is not secured. Carriers claim that a virtual private network is as safe as a leased line, but forget to mention the fact that leased lines are unsecured. It is also a known fact that virtual private networks run on a transport network that provides the shared infrastructure and that can be attacked.

Only SSL- and SSH-VPNs come with required built-in encryption. For IP-VPNs the use of IPSec is not mandatory. MPLS- and Ethernet-VPNs do not have any useable official encryption standard.

VPN	VPN Layer	Security Standard
SSL VPN (Layer 4 VPN)	Layer 4: Transport Layer	SSL/TLS/DTLS
IP VPN (Layer 3 VPN)	Layer 3: Network Layer	IPSec
MPLS VPN (Layer 2.5 VPN)	Layer 2.5: MPLS	_____
Ethernet VPN (Layer 2 VPN)	Layer 2: Data Link Layer	_____

To protect your data and your network there is no way around encrypting your VPN. As an added bonus you also will be compliant with key regulations. If you have an Ethernet-VPN you will need an Ethernet encryptor which encrypts the network at layer 2. An MPLS-VPN operates at an intermediate layer, right between layer 2 and layer 3. You can encrypt an MPLS-VPN at layer 2 with an Ethernet encryptor that is MPLS-aware, or you can encrypt at layer 3 with all the performance penalties and additional overhead that layer 3 encryption is known for.

1.3. Comprehensive encryption solutions

Encryption at layer 2 is a necessity for Ethernet networks. The IEEE has therefore developed and published a standard for the encryption of Ethernet at layer 2 for site-internal networks: IEEE 802.1ae (MacSec). Authentication and key management are now standardized by IEEE 802.1X-2010, however, after the first try at standardization (IEEE 802.1af) has failed. As MacSec has been designed for use within local area networks it is limited to hop-to-hop scenarios. There is currently no IEEE standard for multi-hop networks. In other words: There is no encryption standard for Ethernet MANs and WANs that are based on Metro or Carrier Ethernet. Multi-hop, meshed multipoint networks are dependent on a comprehensive encryption standard that includes group key management. While there are no such comprehensive encryption standards for either layer 2 nor for layer 3, solutions do exist.

2. Network layers and encryption: L2 vs L3

2.1. Different layer – different approach

Layer 2 and layer 3 encryptors work differently. Layer 3 encryptors are designed for IPsec encryption and to encrypt IP payload. IPsec tunnels the original IP packet, so that it can encrypt the original IP header. If you want to encrypt an Ethernet frame with IPsec, the encryptor has to lift the Ethernet frame up to layer 3, so that the Ethernet frame becomes IP payload that then can be encrypted. If you use IPsec to encrypt MPLS networks, IPsec will tunnel the original IP packet that forms the MPLS payload.

Layer 2 encryptors are designed to encrypt layer 2 and above. They are optimized for Ethernet and MPLS and don't need to tunnel the original IP packet to encrypt IP or MPLS running over Ethernet. Encryption is most efficient if it takes place at the native layer or below.

The comparison of encryption at layer 2 and encryption at layer 3 below applies to the encryption of Ethernet networks. It compares the encryption at the corresponding layer. To encrypt layer 2 frames at layer 3 requires a tunneling of the layer 2 frames at layer 3 to allow the encryption at layer 3 with IPsec. Tunnels are known to generate overhead, complexity and computing time. Tunneling a layer 2 frame over IP in combination with encryption using IPsec ESP tunnel mode is a less-than-ideal solution. It should only be used if the necessary layer 2 infrastructure is missing.

2.2. IPsec encryption at layer 3

For connecting sites at layer 3 the standard encryption mode used is IPsec ESP tunnel mode. Depending on the selected encryption standard this encryption mode generates an encryption overhead of 58-73 bytes. These numbers refer to IPv4, as the overhead increases by at least 20 bytes if IPv6 is used. Small packets of 64 bytes, which constitute an ever-increasing share of the overall network traffic, can therefore double in size due to the encryption. The percentage-wise increase is lower with larger packets. If the encryption is moved from layer 3 to layer 2, the IP packets are pure layer 2 payloads and can be encrypted at packet level without generating overhead.

The layer 3 encryption overhead consists of two factors: the overhead generated by the encryption mode and the overhead generated by padding.

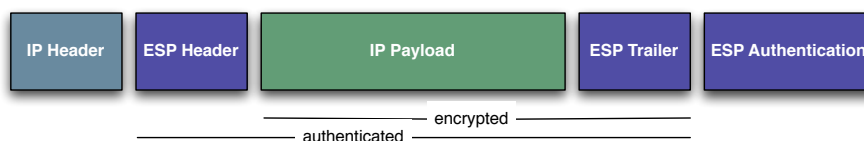
2.2.1. IPSec – The Standard for layer 3 network security

A look at an IP packet with its payload in both, IPSec ESP transport mode and tunnel mode, reveals the inefficiencies caused by the encryption mode on packet level.

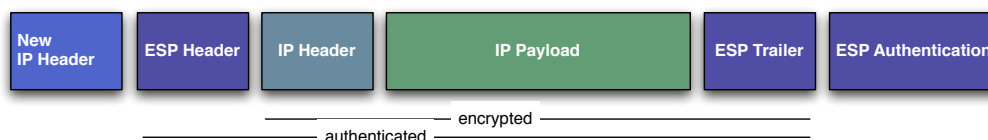
IP Packet



IP Packet IP Sec Transport Mode



IP Packet IP Sec Tunnel Mode



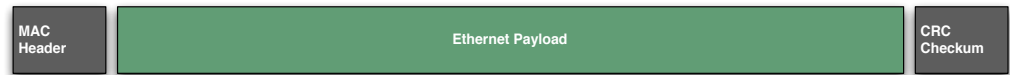
Let's start with a packet the way it is transported on layer 3: It consists of an IP header and the payload. IPSec ESP transport mode adds an ESP Header, an ESP trailer and ESP authentication. In transport mode only the payload is encrypted while the IP header remains unprotected. The established way to encrypt site-to-site traffic with IPSec is the tunnel mode. A new IP Header is added, so that the entire IP packet (header and payload) can be encrypted without sacrificing network compatibility.

For the transport over an Ethernet network the encrypted IP packet gets a MAC header and a CRC checksum.

IP Packet IP Sec Tunnel Mode in Ethernet Frame



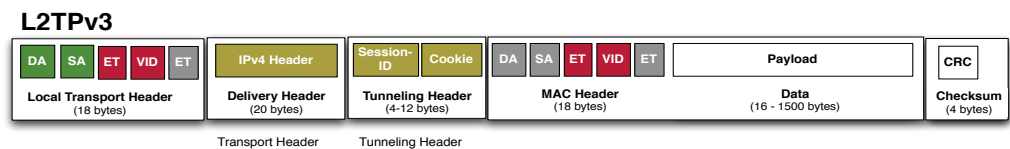
For Ethernet the entire IP packet encrypted with IPSec ESP Tunnel Mode is pure payload. Accordingly a transport mode encryption at layer 2 can provide the same protection as IPSec ESP Tunnel Mode without generating packet overhead. The encryption can encrypt the entire IP packet without introducing packet overhead. IPSec ESP Mode features Encapsulating Security Payload, which provides confidentiality, data origin authentication, connectionless integrity and an anti-replay mechanism. To maintain comparable layer-specific security, equivalent features need to be implemented at layer 2. Some of the overhead that would have been generated at layer 3 thus moves down to layer 2. Properly implemented it will cause less overhead and be much more flexible in terms of network functionality than IPSec at layer 3.



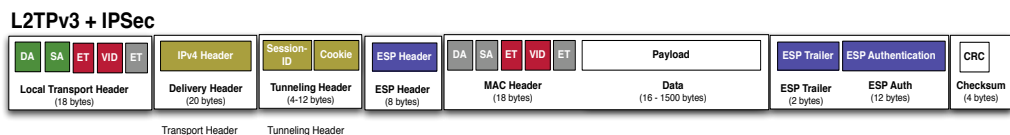
At layer 3 it also matters if you encrypt IPv4 or IPv6. Both are using IPSec as encryption standard, but the differences between IPv4 and IPv6 make it a completely different story. At layer 2 though, it does not make any difference if the payload to be encrypted consists of IPv4 or IPv6.

2.2.2. Using IPSec for Ethernet encryption

It is possible to encrypt Ethernet using IPSec. In order to do so the Ethernet frame has to be fork lifted up to layer 3 to become IP payload. As soon as the Ethernet frame is IP payload it can be encrypted at layer 3 with IPSec. As IP is transported over Ethernet the result is Ethernet transported over IP over Ethernet. It is as inefficient as it sounds. If e.g. L2TPv3 is used to transport Ethernet over IP the overhead generated by encapsulation is 50 bytes.



IPSec encryption will add another 38-53 bytes. The security overhead and the security are limited as only transport mode can be used in this scenario.



2.3. Native Ethernet encryption at layer 2

Let's start again with an IP packet the way it is transported on layer 3: It consists of an IP-header and the payload. For the transport on layer 2 on Ethernet the packet is framed with a MAC header and a CRC checksum. For Ethernet it doesn't make a difference if the IP packet is encrypted or not, it is just payload.

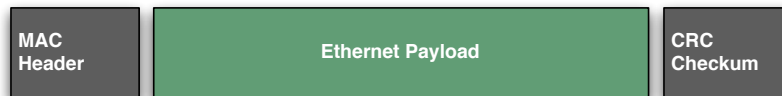
IP Packet (Header and Payload)



IP Packet (Header and Payload) inside Ethernet Frame



IP Packet as Ethernet Payload



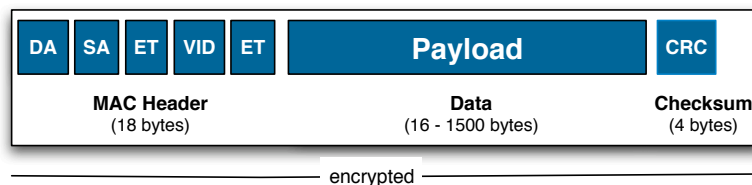
A transport mode encryption at layer 2 will encrypt the entire IP packet including the IP header without requiring any tunneling. Tunneling alone generates 20-40 bytes of avoidable overhead and adds noticeable latency.

To get a better understanding how layer 2 encryptors encrypt at layer 2 it is best to look at the different encryption modes:

2.3.1. Native Ethernet Encryption Modes

The available encryption modes for Ethernet consist of bulk, transport and tunnel.

a) Bulk Mode

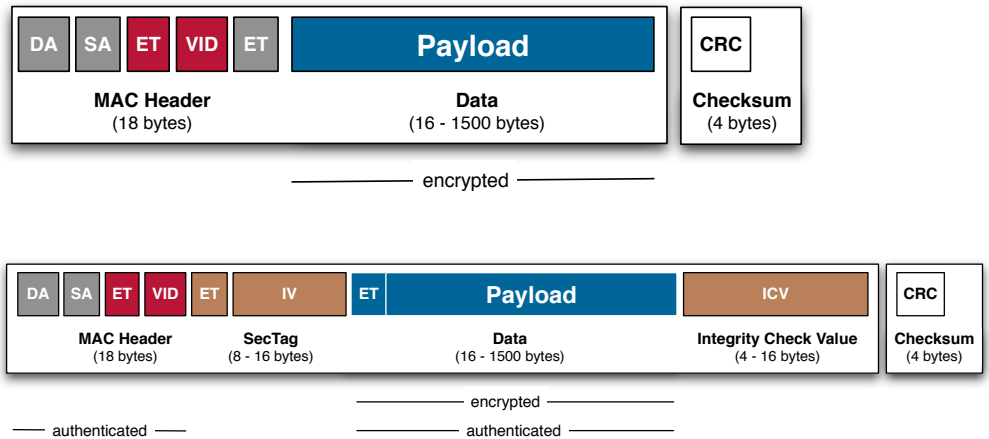


Bulk Mode (also known under the terms Frame Encryption and Link Encryption) encrypts the entire Ethernet frame between the Preamble and the Inter-frame Gap. To reach the same coverage when encrypting the frame with a layer 3 encryptor, the entire Ethernet frame would have to be lifted up to layer 3, encapsulated and then encrypted with IPsec ESP Tunnel Mode. This would cause massive and unnecessary overhead. The Bulk Mode on layer 2 limits the available usage scenario to Hop-to-hop, as all relevant addressing info is encrypted.

b) Transport Mode

The most widely used encryption mode is the transport mode. The reason behind this is the full network compatibility ensured by limiting the encryption to

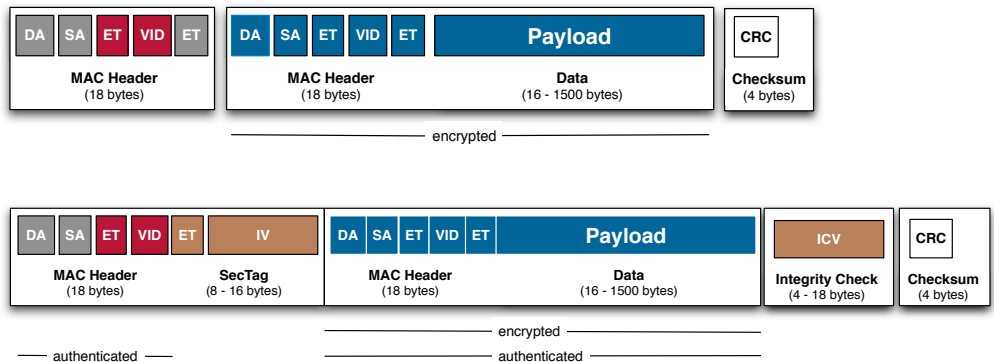
the payload.



Transport mode comes in two different main flavors: Simple and authenticated. In simple transport mode only the layer 2 payload is encrypted, whereas the authenticated transport mode also provides replay and integrity protection. IPsec only has an authenticated transport mode, so a comparison with IPsec should always be done with authenticated transport mode.

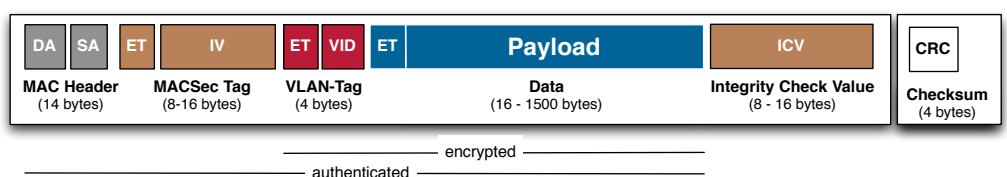
c) Tunnel Mode

Tunnel mode is also an option on layer 2, but only used if the entire original frame must be encrypted and the encryption needs to support a multi-hop-scenario. Tunneling adds overhead and processing time.



Tunnel mode comes in two flavors: One that encrypts only the payload – which consists of the entire original frame - and one that provides explicit replay and integrity protection on top of payload encryption.

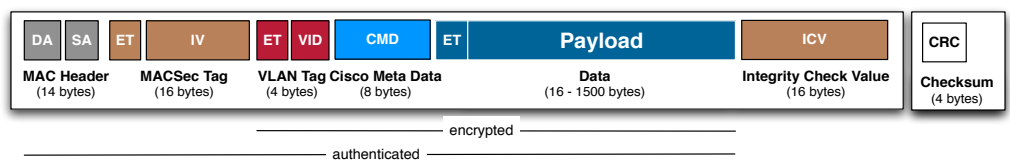
d) MacSec/LinkSec



MacSec (also known as LinkSec) is a pure link encryption. Contrary to transport mode, MacSec puts the SecTag right after the destination and sender address. Only devices with MacSec support are able to recognize the format. MacSec was designed to protect internal local area networks and is limited to hop-to-hop scenarios. The usage scenario consists of MacSec-capable devices that are next to each other on the network. Each MacSec device decrypts the incoming frame, so that the entire frame is completely unprotected and open within the device before it encrypts it again and sends it out. Contrary to specialized encryption appliances MacSec does not come with a built-in key management. Except for the frame format there is also no guaranteed compatibility between different MacSec implementations. Cisco's TrustSec is even incompatible with everything else despite being based on MacSec/LinkSec.

http://en.wikipedia.org/wiki/IEEE_802.1AE
<http://download.intel.com/corporate/education/emea/event/af12/files/kahn.pdf>
http://www.ixiacom.com/pdfs/library/white_papers/MACSec_white_paper.pdf

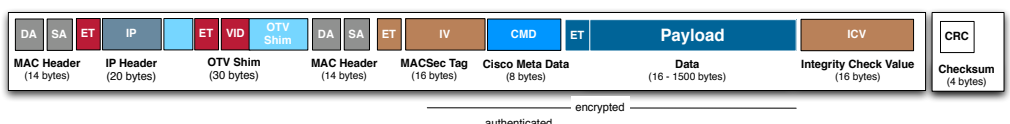
e) Cisco TrustSec



Cisco's TrustSec for layer 2 is based on MacSec/LinkSec, thus inheriting all MacSec-related security benefits, but also inheriting all the drawbacks, such as the limitation to hop-to-hop scenarios. TrustSec adds Cisco Meta Data to the frame, causing an increase of the encryption overhead from 32 bytes to 40 bytes.

http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/ps9512/brochure_cisco_nexus_7000_series_security_features.pdf

As MacSec is limited to hop-to-hop environments, it is practically useless for MAN and WAN scenarios, as those tend to be multi-hop environments. Instead of developing a proper native solution on layer 2, Cisco decided to encapsulate the entire Ethernet frame for transport over IP. The net effect is that Ethernet is transported over IP that itself is transported over Ethernet. Cisco calls it Overlay Transport Virtualization (OTV), but despite its fancy name it is nothing else but an inefficient way to compensate for using the wrong encryption approach for layer 2.



It is actually as inefficient as it looks. MacSec/TrustSec generates a security overhead of 40 bytes. OTV adds at least another 42 bytes per frame, moving the total up to 82 bytes per frame. If IPv6 is used instead of IPv4 there are another 20 bytes that go on top of the already excessive overhead. This is neither good news

for the network performance nor for the costs.

2.3.2. Site internal vs. MAN and WAN

Layer 2 encryption shows its strengths when securing mid- to high-bandwidth infrastructure, be that site internal or between sites. The approach taken for securing site internal networks differs substantially from the one used for securing links between sites. One differentiation is the supported network scenario: For site internal networks, hop-to-hop support might be sufficient, whereas multi-hop support is needed for site-to-site and multi-site MANs and WANs. Another differentiation is the key management: For site internal networks encryption tends to lean on the internal authentication and key management structure, whereas the encryption of broadband links between sites is preferably set-up in a strictly autonomous way. The encryptors then constitute a clear demarcation point between internal and external network infrastructure (red and black network).

2.4. Security, efficiency and operational considerations

2.4.1. Security considerations

To secure networks, you want to encrypt as much as possible as simple as possible. There are trade-offs between network security and network compatibility. IPsec was designed to encrypt the IP layer and what is above at layer 3. It can protect the IP protocol and everything that runs on top of it, but it can't protect the network with all the other protocols that run on layer 2 side-by-side with the IP protocol. ARP, STP, CDP etc. remain completely unprotected unless the entire Ethernet frame is lifted up to layer 3, where it can be encrypted using IP-Sec. To protect layer 3, IPsec needs to tunnel the original IP header and to protect layer 2, it needs to encapsulate the entire layer 2 frame. Both mechanisms lead to a noticeable performance degradation.

2.4.2. Efficiency considerations

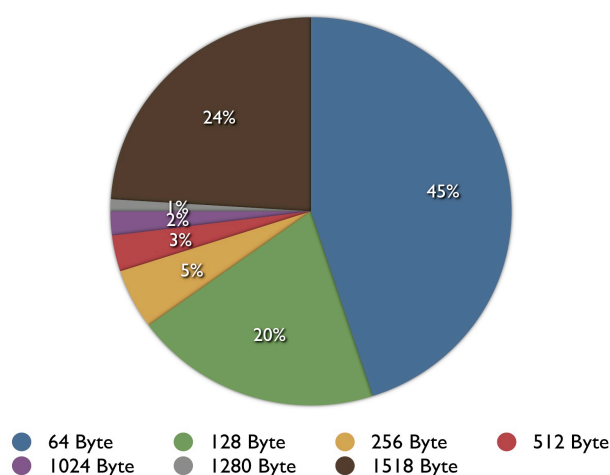
Efficiency is determined by the security overhead footprint, the key system, the processing speed and the scalability.

a) Security Overhead

The security overhead is generated by the encryption standards and encryption modes. Avoiding the need for padding will limit the security overhead. Contrary to layer 3 encryptors, most layer 2 encryptors use encryption standards that avoid padding: e.g. CBC (Cipher Block Chaining) is used in its most efficient variant that includes Ciphertext stealing (CBC-CTS) instead of simple CBC to avoid padding and the related overhead. The use of stream ciphers instead of block ciphers also prevents cryptographic overhead caused by padding. The savings in terms of avoidable overhead are between 2 and 17 bytes per frame.

A comparison of the entire security overhead when using the same encryption standard (AES) and equivalent confidentiality, data origin authentication, integrity and replay protection shows a security overhead of 58-73 bytes when using IPsec/IPv4 and a security overhead of 16-26 bytes when using a specialized layer

2 encryptor. The overhead caused on layer 2 is significantly lower, making the layer 2 solution the better option.



The smaller the packet, the higher the relative size of the overhead generated by IPSec. IMIX, the standardized average packet size mix for IP traffic, shows that packets with a size of 64 bytes account for 45% of all IP packets. The total of IP packets with a size of 64 bytes and 128 bytes accounts for a little bit less than two thirds of all packets.

b) Key System

The capability and flexibility of the key system has an impact on network overhead as only group key systems can handle multicast and broadcast efficiently to avoid the flooding of multicast across all connections is avoided. IKE, IPSec's native key system has severe shortcomings in that area, which has caused many vendors to develop proprietary group key systems. Most layer 2 encryptors feature built-in sophisticated group key systems with built-in failover mechanisms.

c) Processing Speed

The latency for hardware-supported layer 2 encryptors is measured in microseconds, whereas encryption with IPSec is measured in milliseconds. Between microseconds and milliseconds there is a factor of 1000.

d) Scalability

Ethernet encryptors can encrypt line speeds from 10Mb/sec to 10Gb/sec full duplex with minimal delay. There is hardly any IPSec encryptor that can handle 10Gb/sec full duplex, especially if it also has to encapsulate layer 2 before encrypting.

2.4.3. Operational considerations

a) Ease of deployment

Ethernet encryptors are a bump in the wire. The set-up is quick and practically error-proof. Network downtime is reduced to a minimum.

b) Operating cost

Ethernet encryptors hardly need any maintenance. They are mostly considered to be deploy-and-forget as they do their job in the background and do not have a negative impact on network performance. Little maintenance translates into cost savings.

To protect a layer 2 site-to-site or multi-site networks, layer 2 encryption just makes more sense as it can secure everything layer 2 and above and comes without built-in performance degradation.

The same is true for layer 2.5 VPNs (MPLS), which can be encrypted at layer 2 without tunneling contrary to the encryption at layer 3, which requires tunneling.

From layer 2 you have direct access to all relevant network layers (2-7). The right product will let you encrypt all networks running over Ethernet MANs and WANs, Ethernet, MPLS or IP without tunneling and fork lifting. Encrypting Ethernet networks at layer 2 is faster, is simpler, more secure and more powerful.

3. Implementation: Dedicated appliances vs. integrated appliances

The best solution for securing layer 2 networks is specialized, autonomous layer 2 encryptors. They come without dependencies and keep their focus sharply on their one and only job, thus operating as efficiently as possible. Processes and management are simple, straightforward and completely optimized for the job at hand. This not only benefits performance and security, but it also has a positive mid- and long-term impact on flexibility and cost. While there are different ways to integrate layer 2 encryption into other appliances and perform it as a side-job, none of those approaches provide the security and efficiency of a dedicated encryption appliance.

The issue with integrated appliances is the fact that they would need to be optimized to do all the different tasks concurrently and all of that without performance degradation and functionality reduction. That is simply not possible. Integrated solutions can do many things, but not everything well. The reason for this lack of excellence is to a large part due to the compromises required to make the integrated appliance cheaper than the dedicated appliances it competes with.

3.1. Security

Dedicated appliances are optimized for security and meet the highest requirements. The systems form a closed and tested environment that has been proved to be secure. They only provide the interfaces that are absolutely necessary. Both, case and key storage are fully secured and the protection includes measures against emissions. Any attempt to tamper with the unit will result in the immediate emptying of the key storage and the notification that an attempt at tampering took place. The casings are tamper resistant. For integrated appliances it is between difficult and impossible to provide such a security level.

3.2. Performance

Dedicated appliances are optimized for performance. There is no competition for the available resources between different functionalities.

Integrated appliances are optimized for specific performance features that hardly ever can be fully exploited in parallel. Often cost considerations favor the use of ASICs (Application Specific Integrated Circuits) over FPGAs. Those ASICs support only a limited set of functions. If functions are used that are not implemented in hardware, they are executed in software, which leads to a performance loss. If the entire processing is executed on a standard CPU, the performance is limited to low and medium bandwidths and latency and jitter are increased. If the CPU is dedicated to a dedicated encryption appliance, the performance characteristics can be properly predicted and remain constant. A CPU which has to serve a range of different applications – as is typically the case with integrated appliances and virtualized environments – has a performance characteristic that is dependant on the particular load generated by other applications at a given time and thus is variable and unpredictable.

3.3. Upgradeability

Dedicated layer 2 encryptors tend to be specified and dimensioned in a way that allows the expansion of the functionality at a later point in time. This is an essential requirement to keep the device state-of-the-art for the years to come. Amply dimensioned FPGAs (Field Programmable Array) fit the bill, but they increase the cost. Underpowered FPGAs are quickly saturated and draw a high amount of power, which leads to extensive heat development.

Upgradeability and expandability are cost drivers and thus not high on the priority list for developers of integrated appliances. They prefer to focus on initial cost containment rather than on mid- to long-term cost efficiency. Software-based real and virtual appliances running on standard CPUs can easily be upgraded, but are substantially less powerful. Extensions of the software functionality can accentuate this lack of performance

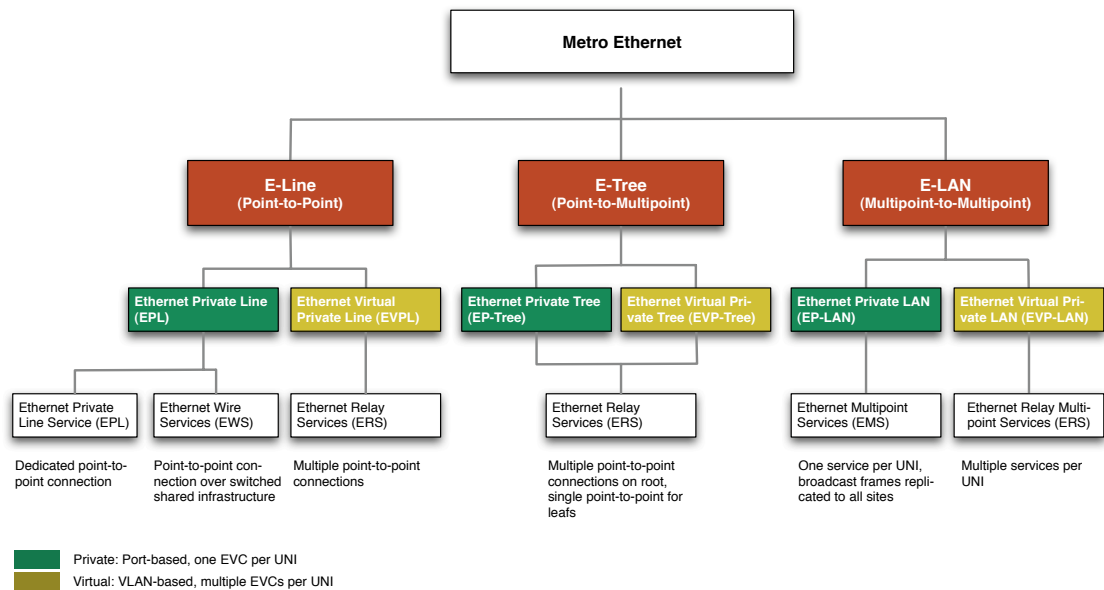
3.4. Costs

Encryption implemented as function in integrated appliances can use a lot of the basic network and management infrastructure provided by the main functionality of the device. There is no cost for an additional case, an additional redundant power-supply or a network processor. This reduces initial cost and price, but ties the encryption to the integrated appliance. The average product life of a dedicated encryption appliance exceeds that of an integrated appliance by 3-4 years, leading to lower cost of the dedicated encryption appliance over the entire product life. The initial cost savings of the integrated appliance turn into higher cost over time.

Another aspect that is often not taken sufficiently into consideration is the vendor lock-in: Due to incompatible key systems and different feature sets, you cannot mix and match layer 2 encryptors. Not a single platform is compatible with another platform, even if a standard such as MacSec is used. If the encryption is integrated with the switch/router, there is even a double vendor lock-in. Changing the vendor at a single site will exclude that site in terms of encryption from the MAN/WAN. It is mandatory to use the same vendor for encryption and for switching at all sites, resulting in a double vendor lock-in. No cost reductions are possible through a change of suppliers, such as from Cisco to Juniper, HP or Huawei, as all integrated appliances would need to be changed at the same time. Only dedicated encryption appliances are completely independent of switches and routers and thus reduce vendor lock-in.

4. Ethernet Topologies for MANs and WANs

The Metro Ethernet Forum (MEF) defined and structured all the different topologies available for Metro and Wide Area Networks based on the Ethernet networking standard. Only some of the available Ethernet encryptors support all topologies and usage scenarios.



5. Ethernet Encryptors

Contrary to encryption solutions on layer 3 (IPSec) and layer 4 (TLS) which are standardized to a certain degree, there is no standard for layer 2 (Ethernet). The information available for the existing solutions is very limited and the market completely lacks transparency. The information published by the vendors, be that on their website or on their datasheets and whitepapers tends to cause more questions than it answers. What has been sorely missing in the past is the possibility to compare the different products available on the market based on objective criteria.

The market overviews published on www.inside-it.ch - point-to-point and multipoint solutions - explain and show the key features of the different products, but do not rate them in order to remain completely objective. It is up to the reader to make his own judgment. The listed features are of rather quantitative nature. Whoever plans to deploy layer 2 encryptors must first establish the functional requirements based on his network topologies and his business requirements before starting to evaluate the different products.

The links to the current versions of the short versions of the market overviews can be found on www.inside-it.ch. Currently version 3 (2011 edition) is up-to-date. The previous editions are outdated.

The premium versions of the market overview, which cover much more detail, are available directly from the author. They cover nearly every aspect that is relevant for an evaluation and can be used for defining the functional requirements for an evaluation.

© 2007 - 2011 **Christoph Jaggi**

All rights reserved. No copying, no commercial use and no republications (in part or in whole) without prior written permission of the author.

www.uebermeister.com
cjaggi@uebermeister.com