inside-it.ch

PRESENTS:

LAYER 2 ENCRYPTORS
FOR
METRO AND CARRIER ETHERNET

ETHERNET ENCRYPTORS FOR METRO AND CARRIER ETHERNET

AN INTRODUCTION

Version 6.03, April 26 2016

© 2007-2016 Christoph Jaggi

All rights reserved

www.uebermeister.com
cjaggi@uebermeister.com

ISBN: 978-1-62018-001-3

Executive Summary

Networks 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. For Metro and Carrier Ethernet, the efficient encryption of all network data requires encrypting at layer 2 or below. The usage scenario and the business requirements should be the determining factor for the selection of the encryption layer.

Optical fiber links are unprotected
Optical fiber links are often considered to be "private" links, because the link's use down to the physical layer is exclusive to a single customer. But "private" just means exclusive use and should not be confused with "secure". Neither fiber nor wavelengths come with built-in security. It is actually pretty easy to tap optical fiber. Once tapped, the entire traffic running over the optical fiber is exposed.

Virtual Private Networks are only secure if 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.

Recommended Preventive Measures
The tapping of network data is unpreventable and the tapping of networks is a common practice. The difference in behavior between state actors, criminal organizations and individual hackers in that respect is minimal. The goals are used to justify the means. Next to the simple "passive" tapping of networks there is a multitude of commonly used possibilities to actively attack networks. Fortunately there are adequate means to minimize the impact or even completely inhibit such attacks:

(1) Secure enctyption devices,
(2) Secure keys,
(3) Authenticated encryption,
(4) Additional authenticated data, and
(5) Obfuscation of the Network Traffic (Traffic Flow Security).

Different Layer – Different Approach
Layer 1 encryptors are designed to encrypt direct connections at the physical layer, the

Optical Transport Network (OTN). They can encrypt different layer 2 protocols such as Ethernet, FibreChannel and InfiniBand.
Ethernet encryptors work at layer 2 and are designed to encrypt layer 2 and above. They are optimized for Ethernet and MPLS. Tunneling the original IP packet to encrypt IP running over Ethernet is unnecessary.The encryption of Metro and Carrier Ethernet connections Encryption is most efficient if it takes place at the native layer or below.
Layer 3 encryptors are designed for IPSec encryption and to encrypt IP payload. IP-Sec 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..

Security levels: High assurance, standard assurance and low assurance
Two main factors define the security level that is required: (1) The protection requirements for the data transmitted over the network, and (2) the protection requirement of the network in terms of security and continuity. Data that is considered to be somewhat sensitive causes less harm when stolen or compromised and therefore is subject to much less stringent protection requirements than data that is considered confidential or even secret. If an organization is dependent on a frictionless operation of the network, any impairment can have negative consequences for operations. If there is no such dependency, then less stringent protection requirements might be sufficient.

Only a dedicated appliance can deliver real high assurance and standard assurance
The lack of a secure encryption device and secure keys compromises the security from the outset.

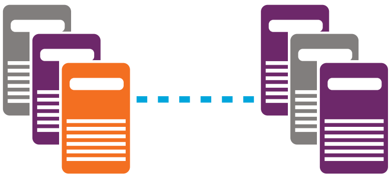
Key management is the core piece of network encryption
Unambiguous authentication of the participants, secure keys, frame format and encryption mode constitute the foundation. Key management takes care of the keys from key generation over to key assignment over to key exchange and finally over to key revocation. Key system and key assignment are an important part of key management and significant for an optimal network functionality.

Security certifications: What are they worth?
Not every product with a FIPS or a Common Criteria certification is secure. Many of them are not really secure and some of them are not secure at all. Despite this, many vendors often are using security certifications to pretend more “certified” security than actually present. For the protection of classified data, more stringent requirements apply. E.g. the German “Bundesamt für Sicherheit in der Informationstechnik (BSI)” evaluates the entire source code of software and hardware before admitting a product for government use for classified data. In the USA also multiple layers of less secure products are used for lower category classified data. This reduces the efforts needed and the security. Even a secure encryption device and secure keys can be optional.

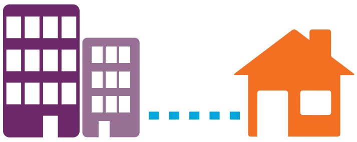
So your data is on the move...

From site to site, or multiple sites...

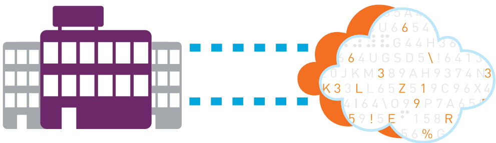
Data center to data center, back up and disaster recovery...



To the last mile, curb, cabinet...



On-premises, up to the cloud and back again...



But is it SAFENET SECURE?

SafeNet High Speed Encryptors

Proven High-Assurance Layer 2 network security for your sensitive data, real-time video and voice, as preferred by market leading commercial organizations and governments in over 30 countries.

- **Trusted security**
  - Protecting Fortune 500 customers across financial institutions, telcos and other commercial organizations
  - Certified FIPS 140-2 L3, Common Criteria, NATO, UC APL, CAPS
- **Maximum network performance**
  - Near-zero overhead
  - Microsecond latency
- **Scalable and simple**
  - "Set and forget" management
  - Low total cost of ownership
- **High-assurance vulnerability protection**
  - True end-to-end, authenticated encryption
  - State-of-the-art client side key management

For a consultation, click here or scan:

SENETAS
Security without compromise

gemalto
security to be free

SENETAS.COM

GEMALTO.COM

Gemalto distributes and supports Senetas encryptors globally under its SafeNet brand.

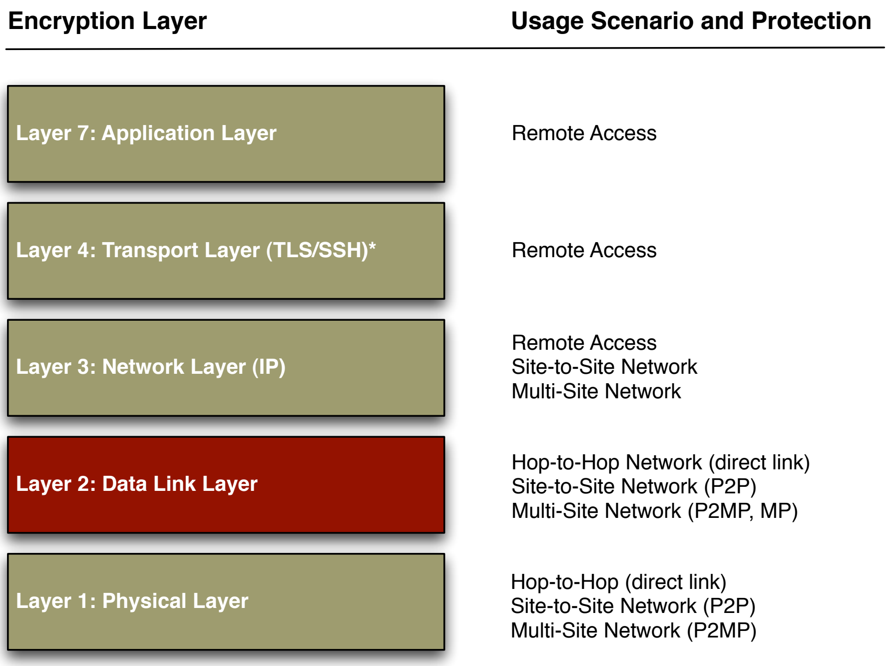
Table of Content

1. Securing Data Networks

1.1. Data networks are unsafe

Networks are unsafe. This 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 to attack a network. A simple search on the Internet will provide you with the necessary information. Without encryption networks passing public ground are unsafe. Therefore it is not a question if encryption is needed, it is only a question which encryption approach is the most efficient and the safest. Just encrypting the network traffic provides some security, but is not sufficient.

The lower the layer, the more comprehensive the protocols that can be encrypted and the more efficient the protection and the processing. Only encrypting at layer 2 provides the efficient encryption of all network data while maintaining a maximum of network compatibility. The encryption of the entire bitstream at layer 1 reduces the network compatibility to a minimum and thus is used only for direct optical fiber links (dark fiber or xWDM). A typical use case is the securing of data center interconnects (DCI). Complexity, overhead and cost of encryption on the different layers differ substantially. The usage scenario and the business requirements should therefore be the determining factor for the selection of the encryption layer and the security solution.

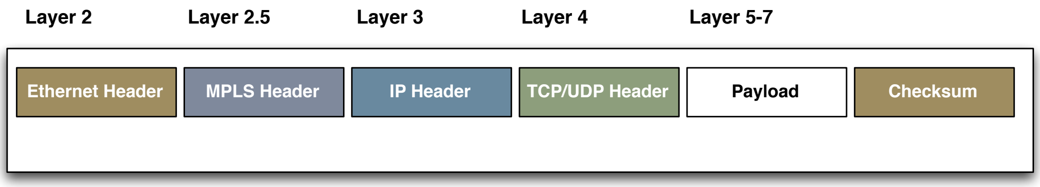


Encryption Layer	Usage Scenario and Protection
Layer 7: Application Layer	Remote Access
Layer 4: Transport Layer (TLS/SSH)*	Remote Access
Layer 3: Network Layer (IP)	Remote Access Site-to-Site Network Multi-Site Network
Layer 2: Data Link Layer	Hop-to-Hop Network (direct link) Site-to-Site Network (P2P) Multi-Site Network (P2MP, MP)
Layer 1: Physical Layer	Hop-to-Hop (direct link) Site-to-Site Network (P2P) Multi-Site Network (P2MP)

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

It is possible to create a tunnel to encrypt a lower layer at an upper layer, e.g. the data link layer (Ethernet, layer 2) at the network layer (IP, layer 3). At the same time it is quite obvious, that the required tunneling will result in increased overhead and additional latency. A native layer 2 encryptor can encrypt an Ethernet network directly, whereas layer 3 encryptor must lift each and every Ethernet frame up to layer 3 in order to encrypt the Ethernet network and accomplish the same task. As layer 3 encryptors operate at layer 3, they can only encrypt layer 3 and above in an efficient way. In order to encrypt Ethernet they first must transform Ethernet into layer 3 payload, which includes some heavy lifting. This is something that is better avoided whenever possible.

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 Ethernet and all layers above without having to resort to tunneling or encapsulation. Only encryption at the native layer can be optimized for that layer.

1.2. Optical fiber links are unprotected

Optical fiber links are often considered to be “private” links, because the link’s use down to the physical layer is exclusive to a single customer. But “private” just means exclusive use and should not be confused with “secure”. Neither fiber nor wavelengths come with built-in security. It is actually pretty easy to tap optical fiber. Once tapped, the entire traffic running over the optical fiber is exposed. Proper encryption can protect the network and the data. Optical links are best secured at the physical or the data link layer. Encrypting at layer 1 allows the encryption of multiple different layer 2 protocols, such as Ethernet, FibreChannel and InfiniBand, whereas encryption at layer 2 will secure a single layer 2 protocol. In both cases the widely used upper bandwidth limit is 10G, so that encryption of a 10G Ethernet point-to-point connection can be as efficient at layer 2 as it is at layer 1. For both layers there are already installations with higher bandwidths (40 Gb/Sec and 100 Gb/sec) and there are already encryption solutions for those bandwidths. The typical use case is a data center interconnect (DCI).

1.3. Virtual Private Networks (VPN) are unprotected

Virtual Private Networks are only secure if encrypted. The word “private” isn’t a synonym for “encrypted”; it only means that a given user’s virtual network is not shared with others. In reality a 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. Furthermore virtual private networks run on a transport network that provides the shared infrastructure and that can be attacked. Authenticated encryption can help secure a Virtual Private Network.

Only SSL- and SSH-VPNs come with required built-in and active encryption. The security provided is as only as good as its implementation. Recent events have highlighted that proper implementation is not a given. Due to buggy implementation on the encryption side and the violation of elementary security principles many of those networks are predisposed for successful attacks[1][2][3][4][5][6].

For IP-VPNs the use of IPSec is not mandatory, despite the omnipresence of IPSec functionality. While IPSec can be used for authentication only without encryption, it is rare to see an IP-VPN that is not encrypted. The standard key system for IPSec is limited to point-to-point connections. There is no standard for multipoint functionality. MPLS is situated on layer 2.5 and doesn’t come with any encryption. It can be either encrypted on layer 2 or on layer 3. There is also no official standard for encrypting Ethernet-VPNs at layer 2 and OTN at layer 1. Despite the lack of official standards, there are suitable solutions available on the market for both.

[1] http://www.securityfocus.com/archive/1/537999

[2] http://www.securityweek.com/default-ssh-keys-expose-ciscos-virtual-security-appliances

[3] http://arstechnica.com/security/2015/06/two-keys-to-rule-them-all-cisco-warns-of-default-ssh-keys-on-appliances

[4] http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/

[5] http://blog.fortinet.com/post/ssh-issue-update

[6] http://www.networkworld.com/article/3009139/millions-of-embedded-devices-use-the-same-hard-coded-ssh-and-tls-private-keys.html

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 data and network there is no way around properly securing the VPN. The added bonus is compliance with key regulations. An Ethernet encryptor that encrypts the network at layer 2 is the best option to secure an Ethernet-VPNs. An MPLS-VPN operates at an intermediate layer, right between layer 2 and layer 3. If it runs over Carrier Ethernet access it can be encrypted at layer 2 with an Ethernet encryptor that is MPLS-aware, or at layer 3 with all the performance penalties and additional overhead that layer 3 encryption is known for. If access is restricted to IP or a combination of Carrier Ethernet and IP is used, then there is the option of using a layer 2 encryptor with an extended feature set. This class of encryptors features native Ethernet encryption over Carrier Ethernet and IP by supporting Ethernet over IP (EoIP).

1.4. Recommended countermeasures

The tapping of network data is unpreventable. This is or should be common knowledge. All that is needed is the necessary determination and enough resources. Specialists have been aware of it for decades and a multitude of publications over the last few years finally made it official: The tapping of networks is common practice. The difference in behavior between state actors and criminal organizations and individuals is marginal. The goals are used to justify the means. Next to the simple “passive” tapping of networks there is a multitude of possibilities to actively attack networks. Adequate protection can minimize the impact or even completely inhibit the success of such attacks.

1.4.1. Secure encryption devices

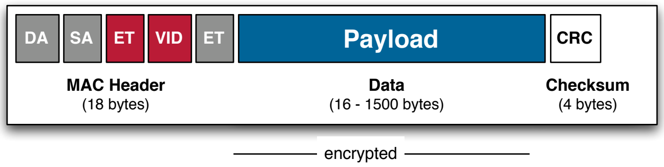
Security needs a dual protection, as there are attacks from the inside and attacks from the outside. If the encryption devices are not completely secured they can be an optimal gateway. Tapping is pretty easy if you have access to the encryption devices and the keys.

1.4.2. Secure keys

Insecure keys are a simple way to break encrypted network traffic. A secure key starts with the use of true random numbers and a sufficient key length and it continues with secure key storage and secure key distribution. Key lengths below 256 bit are critical. Keys weakened from the outset lead to a reduction of security in such a degree that it is barely existent. Often state organizations and institutions have a finger in the pie[7]. Such weakened processes find their way into program libraries, propagate through the use of these program libraries and end up in thousands of programs.

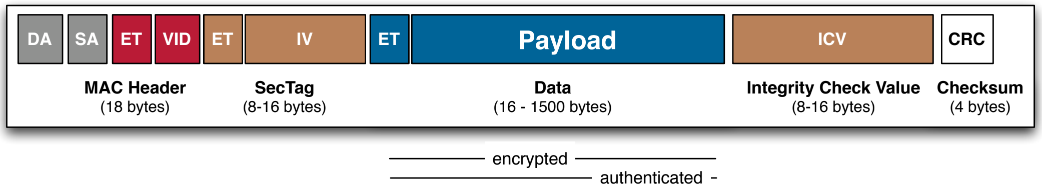
1.4.3. Authenticated encryption (AE)

Authenticated encryption combines the payload encryption with an initialization vector (IV) before, and a Message Authentication Code (MAC) behind the encrypted payload. The latter takes care of authentication and integrity protection. It is based on a shared secret key and the transmitted message. The sender uses the message to be transmitted to generate a MAC. He accomplishes this by using a MAC-algorithm that also makes use of the shared secret key. The MAC is then added as tag right after the payload to the frame that is to be transmitted. The receiver uses the same secret key and the same MAC-algorithm for calculating a MAC for the message that he received. The comparison of the self-calculated MAC with the MAC received shows if the message originates from an authenticated sender and has not been altered during transport. The security provided is dependant on the length of the MAC, who also is known as Integrity Check Value (ICV). A length of 16 bytes provides the necessary security.



Encryption without authentication

[7] https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html
http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html



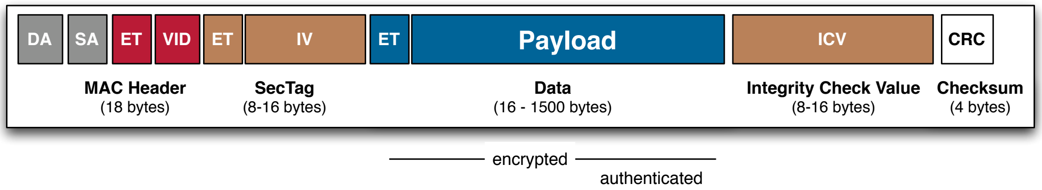
Encryption with authentication

The initialization vector (IV) in combination with a continuous counter makes sure that a message can only be sent once. The counter establishes the mandatory arrival order of the frames. For each key a counter state only exists once. This mechanism fends off replay attacks and other attacks that are based on the infusion of frames into a network. The initialization vector ensures the uniqueness of the combination of initialization vector and key used. On top of that, the IV also guarantees that only frames in the right order are accepted. As Carrier Ethernet mostly runs over transport networks, it is not that unusual, that the right order is not always completely maintained. This is the reason why the encryptor has to provide the option to define the maximum allowable range of the shift.
Authenticated encryption at layer 2 provides the functionality of a layer 2 firewall and a layer 2 Intrusion Prevention System (IPS). The receiving encryptor simply throws out the frames that do not meet all required criteria.

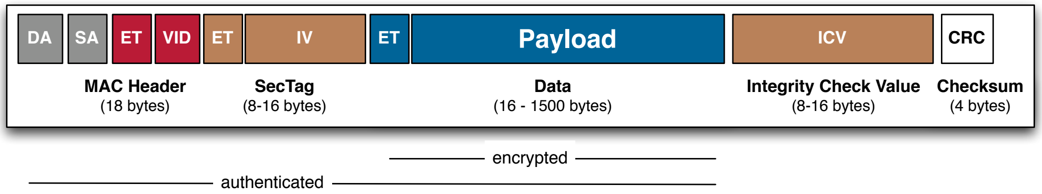
http://en.wikipedia.org/wiki/Authenticated_encryption
http://en.wikipedia.org/wiki/Message_authentication_codes

1.4.4. Additional authenticated data (AAD)

Messages consist of the payload and the header. Security requires that data is encrypted as much as possible and authenticated as much as possible. All parts of the header that are not supposed to change during transport should thus be authenticated. Depending on the frame format and the network this can be the entire header or just parts of it. This functionality is known as Additional Authenticated Data (AAD). In combination with authenticated encryption the use of the term AEAD (Authenticated Encryption with Associated Data) is predominant.



Frame with authenticated and encrypted payload



Frame with authenticated and encrypted payload and AAD

1.4.5. Obfuscation of the network traffic (Traffic Flow Security)

The tapping of a network provides information about the network usage including traffic patterns. It reveals who is communicating with whom, the sequence of the frames and frame sizes and the time of communication. The entire movement profile of frames and all meta-data is visible and gives an informative basis of what happens on the network[8]. Traffic analysis also permits the direct drawing of conclusions concerning the plain text that is being or has been transmitted.

Obfuscating the network traffic is an efficient and effective countermeasure. It is not enough to just generate and transmit dummy network traffic, as there would be still too much information visible to prevent valuable conclusions for traffic analysis. Real traffic flow security is a combination of grouped frames and dummy network traffic. This obfuscates the actual size of the transmitted frames as well as the actual real network traffic.

Traffic Flow Security belongs to the category of Transmission Security (TRANSEC). State-of-the-art solutions are flexible and support different network topologies, including the use of overlay transport networks.

1.4.6. Hardening against quantum computers

For years, the use of quantum computers to crack encryption has been threatening security. Main attack targets would be the asymmetrical key exchange and encryption using weak keys. To counter that threat you don’t need “quantum cryptography“. That term is mostly a marketing obfuscation for quantum-based key generation and/or quantum key distribution, which is used in combination with traditional encryption algorithms, such as AES. While one can employ such technologies, they are not a requirement. It is actually sufficient to use a sophisticated combination of asymmetrical and symmetrical key exchange and a key length of 256 bit for the symmetrical key. Widely used asymmetrical key exchange mechanisms such as RSA and Diffie-Hellman are the ones most likely to be vulnerable to attacks using quantum computers. Static network connections can be hardened against such potential future attacks by using es-

[8] http://en.wikipedia.org/wiki/Traffic_analysis

tablished methods such as AES-MAC to encrypt the asymmetrical key exchange with a symmetrical key[9] . A 256 bit AES key is used to sign the partial keys. Today it is widely believed, that a quantum computer could only manage to reduce the relative security of an Advanced Encryption Standard (AES) 256 bit key to that of a 128 bit key. This would keep even such a quantum computer busy for a very long time trying to crack that key by brute force. Attacks will thus primarily focus on the keys, not on a good encryption method, such as AES. Hardening against quantum computer attacks is to a large degree a hardening of the key generation, the key exchange, the key storage and the key usage environment. Quantum Key Distribution (QKD) covers part of the process but remains limited to optical networks and relatively short distances. Its main usage scenario is data center interconnect (DCI) where it is preferably used in combination with OTN encryption at layer 1. In theory, QKD can provide a longer protection horizon than the 10 years plus likely provided by a sophisticated "traditional" key exchange system.

Nobody can tell, how the situation will be in 5 to 10 years. It is safe to assume, though, that the available security measures will keep pace with the increasing attack potential. There is also plenty of research and development taking place in the area of post-quantum cryptography[10]. Attacks focusing on the end devices will remain easier and more successful than attacks focusing on the key exchanges, even in an era of quantum computers.

[9] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf? page 32 3.1.2

[10] https://en.wikipedia.org/wiki/Post-quantum_cryptography

thales-esecurity.com

Datacryptor®
High performance security for data in motion

Wherever safety and security matter, we deliver

MAN IN THE MIDDLE THREAT PROTECTION
Leverage Galois Counter Mode (GCM) to guard encrypted data against packet replay

SINGLE PURPOSE SECURITY
Unlike switches and firewalls, Datacryptor is purpose-built for securing data in motion

KEY LIFECYCLE MANAGEMENT
Enable complete management control including certified hardware-based random number generation and secure key storage

HIGH PERFORMANCE
Deliver consistent, optimum security from VoIP to jumbo frames, 10Mbps to 10Gbps

REGULATORY COMPLIANCE
Protect data to reduce risk of breach

Millions of critical decisions are made every day in data protection. Thales is at the heart of this, with more than 40 years' experience. Our customers rely on integrated smart technologies such as Datacryptor® to protect the confidentiality, integrity and availability of sensitive information. Our products, services and solutions help businesses and governments reduce risk, demonstrate compliance, enhance agility and make more effective responses in critical environments. Every moment of every day, wherever safety and security are critical, Thales delivers.

Search: Thalesgroup

THALES
Together • Safer • Everywhere

2. Network Layers and Encryption

2.1. Different layer – different approach

Layer 1 encryptors are designed to encrypt direct connections at the physical layer, the Optical Transport Network (OTN). OTN has to a large degree replaced Sonet/SDH and is able to carry Sonet/SDH frames. Layer 1 encryptors can encrypt different layer 2 protocols such as Ethernet, FibreChannel and InfiniBand.

Ethernet encryptors work at layer 2 and 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. It is however possible to encrypt Ethernet at layer 2 and tunnel the encrypted frame over an IP network. This approach is used in situations where the security of layer 2 encryption is preferred but the connection is terminating on layer 3. Without the help of sophisticated traffic flow optimization schemes the additional overhead of Ethernet over IP (EoIP) leads to an increase in network traffic and reduces the effective throughput performance. The measurement of the actual throughput uses the Internet mix (IMIX)[11] to represent typical real-world network traffic with its different packet sizes.

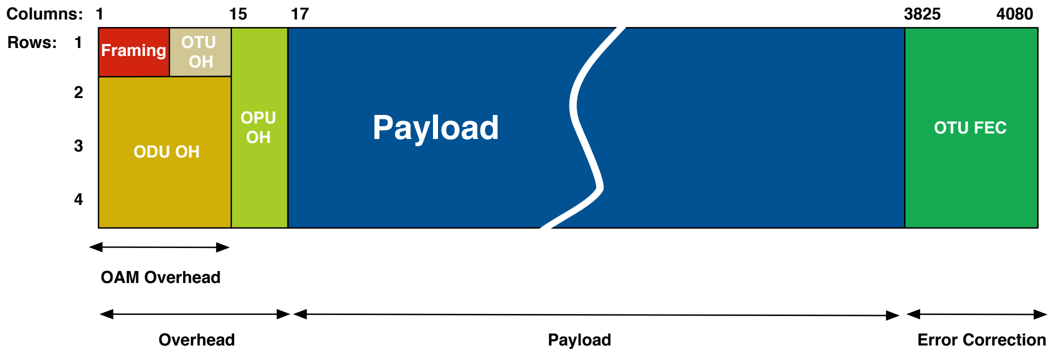
Layer 3 encryptors are designed for IPSec encryption and to encrypt IP payload. IPSec tunnels the original IP packet, so that it can encrypt the original IP header. If you want to encrypt an Ethernet frame with IPSec, the encryptor has to lift the Ethernet frame up to layer 3, so that the Ethernet frame becomes IP payload that then can be encrypted.
Encrypting 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. In such a case there is also the option of an Ethernet encryptor encrypting the entire Ethernet frame and adding an IP-header in front of it.

The comparison of encryption at layer 1, layer 2 and layer 3 below applies to the encryption of Ethernet networks. It compares the encryption at the corresponding layer and shows how an encrypted frame or packet looks like during transport.

[11] https://en.wikipedia.org/wiki/Internet_Mix

2.2. OTN encryption at layer 1

The Optical Transport Network (OTN) as described in general terms in International Telecommunications Union-Telecom (ITU-T) G.872.5 provides the physical layer of the network between two hops. ITU-T G.709 provides the network interface definitions. A G.709 frame consists of three elements: Overhead, payload and error correction.



The Ethernet frame is OTN payload and the encryption of the OTN payload will encrypt the entire Ethernet frame.

Most layer 1 encryption solutions do not provide replay and integrity protection through authenticated encryption. They are limited to providing confidentiality through payload encryption. This is due to the complexity of integrating the necessary elements into the limited overhead space. At upper layers authenticated encryption can be easily accommodated.

The International Telecommunication Union (ITU) is the governing body for the OTN standards. There is no official encryption standard.

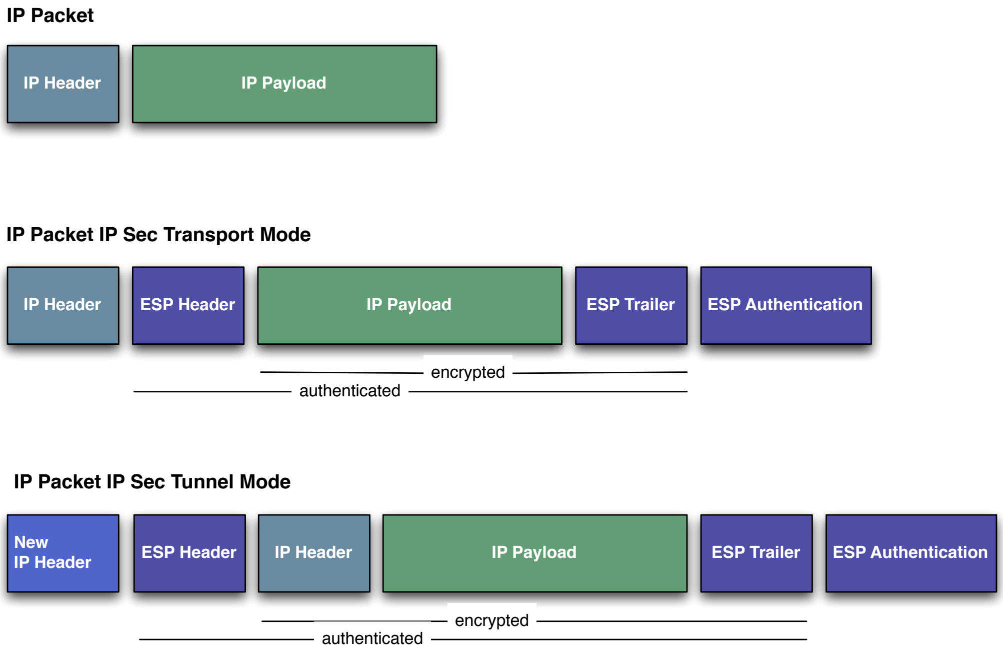
2.3. IPSec encryption at layer 3

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 at least 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 percentagewise 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 such an excessive overhead.

The layer 3 encryption overhead consists of three factors: the overhead generated by the encryption mode, the overhead generated by the encryption standard and the overhead generated by padding.
IPSec ESP mode provides encryption combined with authentication.

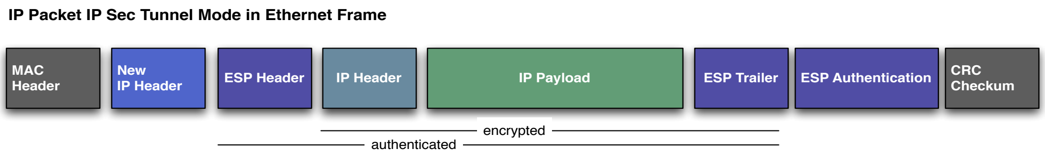
2.3.1. IPSec – the standard for layer 3 network encryption

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.

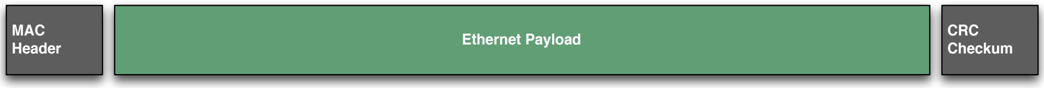


Let's start with a packet the way it is transported on layer 3: It consists of an IP header and the payload. IPSec ESP transport mode adds an ESP Header, an ESP trailer and ESP authentication. In transport mode only the payload is encrypted while the IP header remains unprotected. The established way 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.



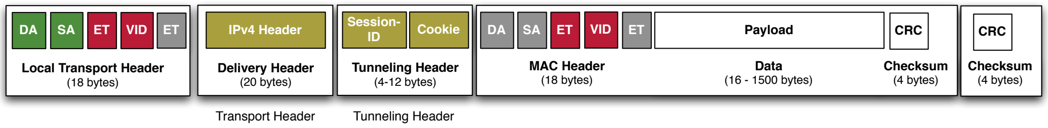
For Ethernet the entire IP packet encrypted with IPSec ESP Tunnel Mode is pure payload. An authenticated transport mode encryption at layer 2 can provide the same protection as IPSec ESP Tunnel Mode generating substantially less packet overhead. IPSec ESP Mode features Encapsulating Security Payload, 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 – between 24 and 32 bytes - and be much more flexible in terms of Ethernet 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.

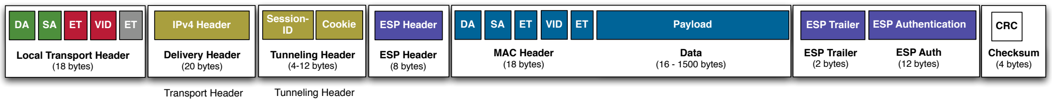
2.3.2. Using IPSec for Ethernet encryption

It is possible to encrypt Ethernet using IPSec, but 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. If you use IPv6 it will take another 20 bytes on top.



L2TPv3 with Ethernet frame

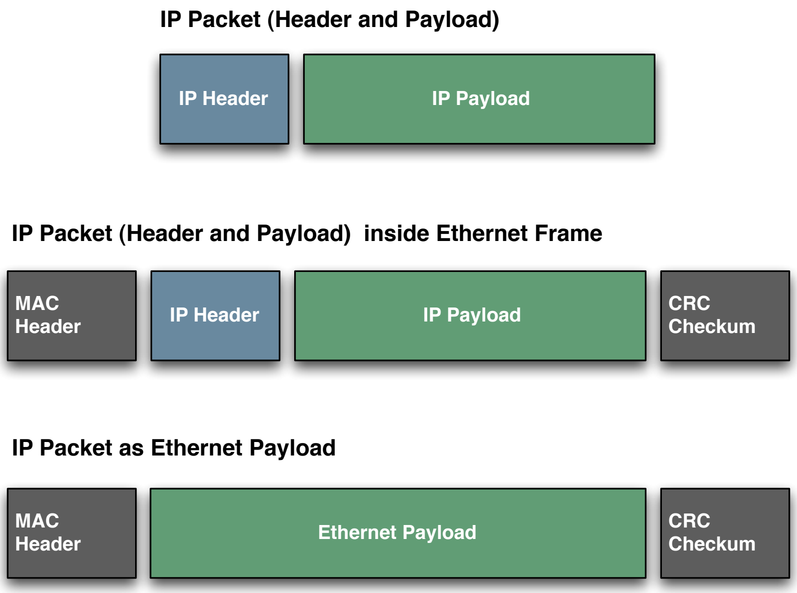
IPSec encryption will add at least another 38-53 bytes. As L2TPv3 already creates a tunnel, there is no need to use IPSec ESP Tunnel Mode and IPSec ESP Transport Mode can be used[12]. Without tunnel there is less additional overhead.



L2TPv3 with Ethernet frame encrypted using IPSec ESP Transport Mode

2.4. Native Ethernet encryption at layer 2

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 Header
IP Payload
IP Packet (Header and Payload) inside Ethernet Frame
MAC Header
IP Header
IP Payload
CRC Checkum
IP Packet as Ethernet Payload
MAC Header
Ethernet Payload
CRC Checkum

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 can add noticeable latency.

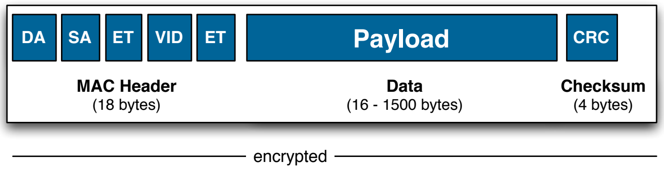
For Ethernet encryption there are a range of different encryption modes available that allow the optimizing of the encryption for different usage scenarios and security requirements. Use of unauthenticated encryption modes and lack of support for additional authenticated data (AAD) limits the extent of the se-

[12] https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

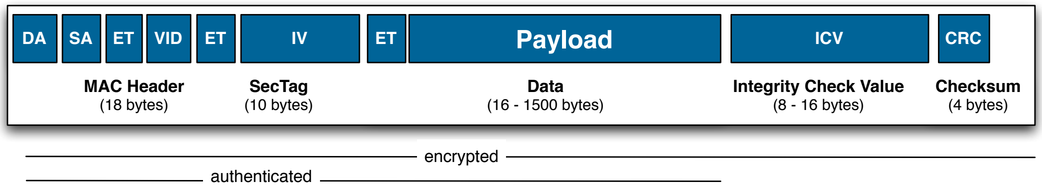
curity provided. Without security overhead there is no real security. The goal is to have maximum security and scalability without introducing too much overhead.

2.4.1. Frame mode (bulk)

Frame Mode (also known under the terms “bulk encryption” and “link encryption” encrypts the entire Ethernet frame between the preamble and the interframe gap. The usage scenario is limited to pure point-to-point connections between two encryptors over a dedicated line.



Frame Mode encryption without authentication

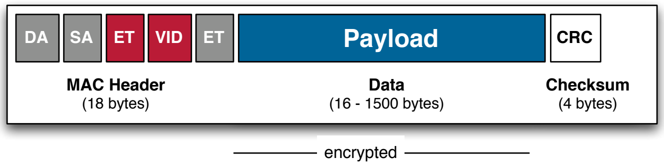


Frame Mode with authenticated encryption

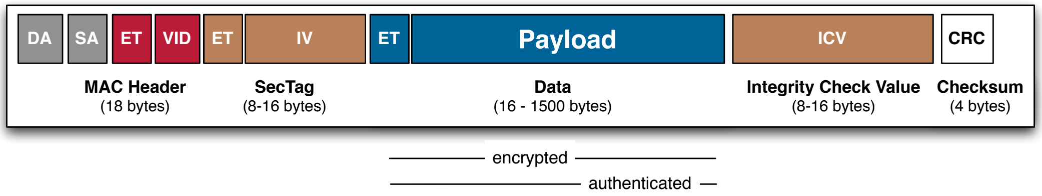
Encrypting the entire frame does not provide replay and integrity protection. Some encryptors do however offer frame mode in combination with traffic flow security, which conceals the presence and characteristics of the network traffic and disables any data traffic analysis. In high-security environments, frame mode is used in combination with both, traffic-flow security and authenticated encryption.
As all relevant addressing info is encrypted, frame mode on layer 2 limits the available usage scenario to hop-to-hop. Only the authenticated frame mode is considered to be secure.

2.4.2. 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 without authentication

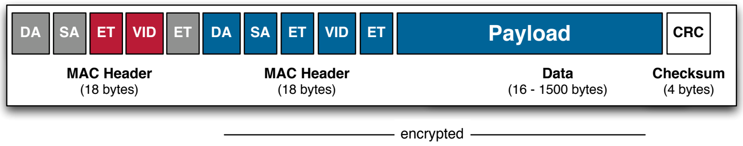


Transport Mode with authentication

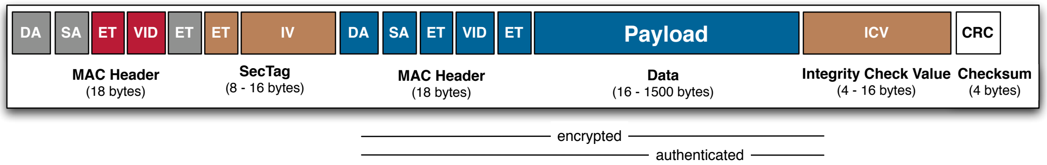
There are two different transport modes. The first one encrypts the layer 2 payload using AES and thus limits the security to confidentiality. The second mode uses AES-GCM to provide confidentiality, integrity protection, authentication and replay-protection. IPSec only has an authenticated transport mode, so a comparison with IPSec should always be done with authenticated transport mode. Any comparison between IPSec and native Ethernet encryption thus should be based on authenticated encryption.
Unauthenticated transport mode without any frame overhead is only possible if the EtherType of another service is used. Following the rules would require the encryption of the original EtherType together with the payload and adding either an own EtherType or an EtherType reserved for such services. That would add two bytes of overhead. To avoid this, EtherTypes belonging to other services are borrowed. If a vendor highlights in his marketing materials that the encryption does not generate any overhead, then he borrows an EtheryType belonging to another service. In marketing speak the use of a different service's EtherType is called "EtherType mutation" or "EtherType transformation". In some cases this might have a negative impact on network compatibility.
Encryption entirely without overhead is actually impossible, as the encryptors must communicate with each other and each key exchange inevitably generates network traffic.

2.4.3. 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 18 Bytes of overhead and a bit of processing time, but reduces the visible network addresses to the network addresses of the encryptors, limiting the metadata usable for traffic flow analysis. 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. Authenticated encryption should be preferred.



Tunnel Mode without authentication

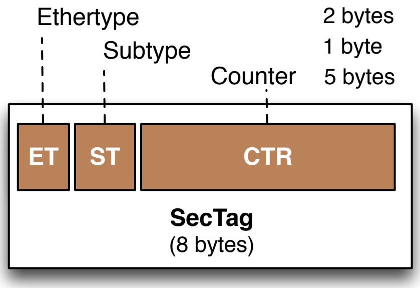


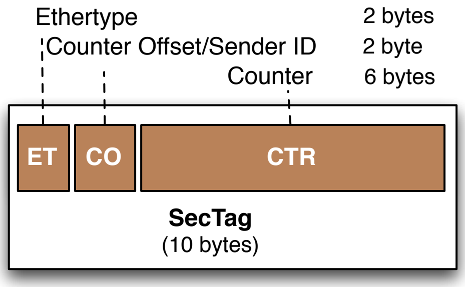
Tunnel Mode with authentication

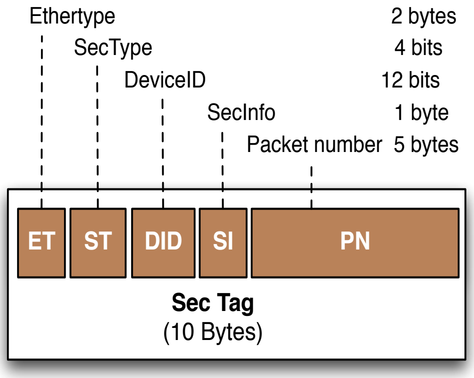
2.4.4. SecTag

The SecTag contains the EtherType used for the encrypted payload and the initialization vector needed for the encryption. The content of the initialization vector depends on the information needed by the key management. Most often it consists of a counter and the assignment of a counter to a sender. Different implementations use different counter sizes and have different limits for the maximum number of counter assignments. The longer the counter, the less frequent a forced key change is necessary. The larger the address space for counter assignments, the more members a group can have. A minimum of 1 byte for counter assignments to support up to 256 group members and a 5 bytes counter length should be supported. Using 2 bytes for the counter assignments and 6 bytes for the counter improves scalability and provides extended reserves for higher bandwidths and larger groups.

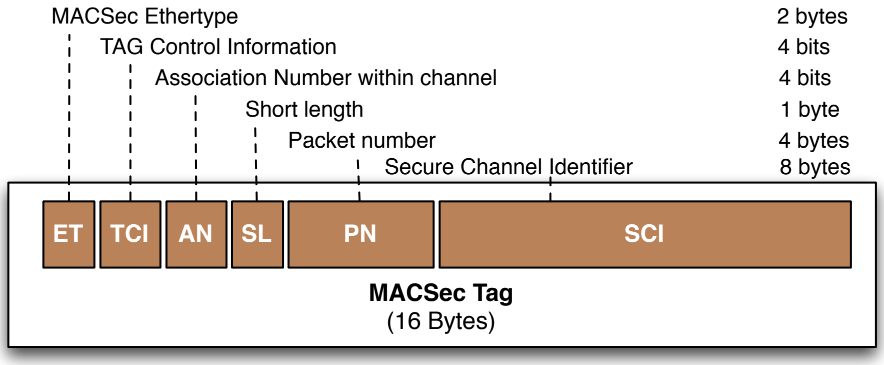
The corresponding SecTags look as follows:







The MACSec SecTag uses 16 bytes without having functional advantages. The MACsec frame overhead is 6-8 bytes higher than the one of other encryption solutions that also use AES-GCM.



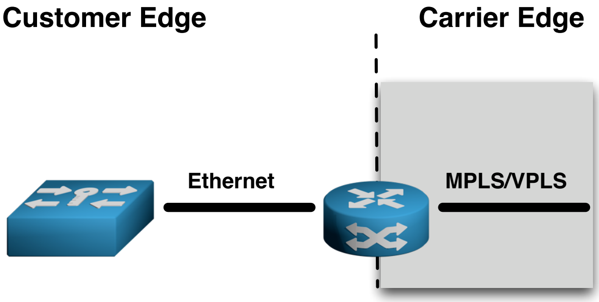
2.5. Encrypting MPLS networks

Ethernet is not only used to carry payload and data from layer 2 upward, but also to transport MPLS. MPLS stands for Multiprotocol Label Switching and is situated between layer 2 and layer 3. It is a layer 2.5 protocol that allows the connection-oriented transmission of data packets in a connection-less network. MPLS does not come with any native security mechanism or standard.

Processing Layer	Processing Mechanism
Layer 3: IP (Internet Protocol)	routed based on IP address
Layer 2.5: MPLS (Multiprotocol Label Switching)	switched based on MPLS tag
Layer 2: Ethernet	switched based on MAC adress

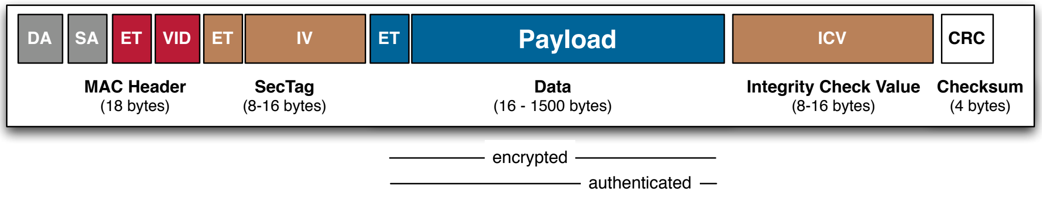
MPLS can be used to transport a large variety of payloads, including IP packets and Ethernet frames. Ethernet encryptors should support MPLS. Ethernet encryptors should support MPLS as much as possible. Depending on the position of the encryptor within the network a different kind of support is required.

If MPLS is used as a pure transport network for Ethernet frames on the carrier side, it is completely transparent for the customer. He passes over Ethernet frames and receives Ethernet frames on the other side.



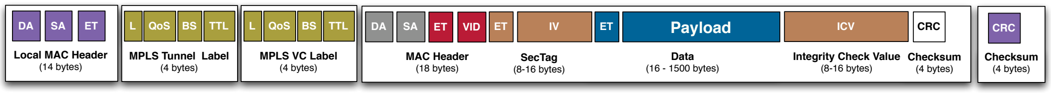
MPLS/VPLS used for transport of Ethernet frames

This scenario is a standard Ethernet scenario and the Ethernet encryptor will limit the encryption to the Ethernet payload.

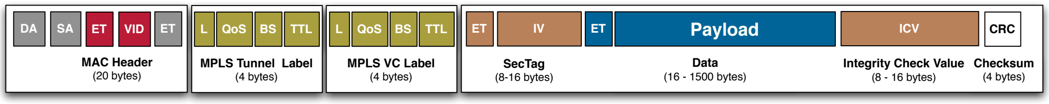


Standard authenticated transport mode encryption before handover for MPLS transport

There are basically two different ways to use MPLS: One is to insert an MPLS tag into the original frame and the other is to transport the original frame over MPLS. The encryption should support these different scenarios.

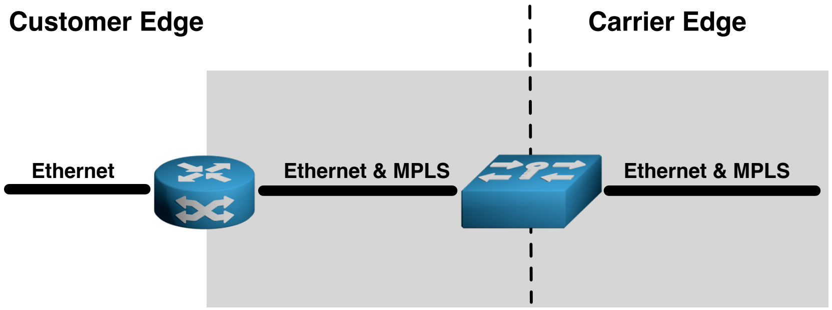


Ethernet over MPLS (EoMPLS)

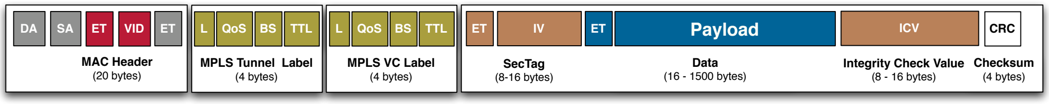


Standard authenticated transport mode with inserted MPLS tags

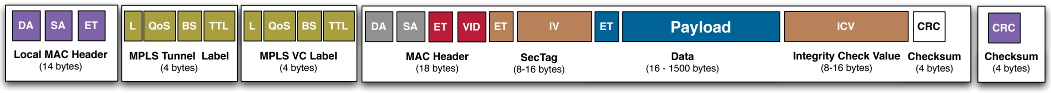
It is an entirely different scenario, if the encryptor is positioned between the MPLS switch/router and the Ethernet connection of the telecom service provider.



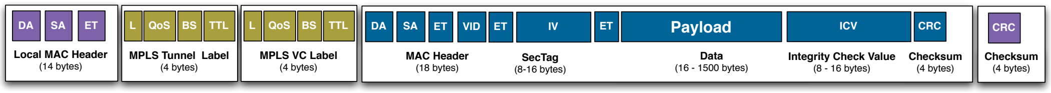
An encryptor positioned after a MPLS switch/router has more options to support than an encrpytor positioned before a MPLS/VPLS switch/router. The encryption must only start after the MPLS tag. At the same time the encryptor has to provide the ability to exempt frames with MPLS tags from the standard Ethernet encryption. This is a basic requirement for full MPLS support that covers the inclusion of sites that are only reachable through IP networks and has an impact on both, supported delivery formats and key exchange.
For full MPLS support an Ethernet encryptor needs an extended feature set that includes Ethernet over IP (EoIP) and sophisticated traffic flow optimization technologies on frame level to compensate for the overhead created by tunneling Ethernet over IP. The actually achievable IMIX throughput is higher than 96%. A big advantage of encrypting MPLS at layer 2 is the complete protection package that is provided: Confidentiality, intrusion detection, intrusion prevention, layer 2 firewall and resistance against DDoS attacks. The simplicity and cost savings, especially for broadband connections, are hard to match with security implemented at layer 3.



Ethernet frame with inserted MPLS tags



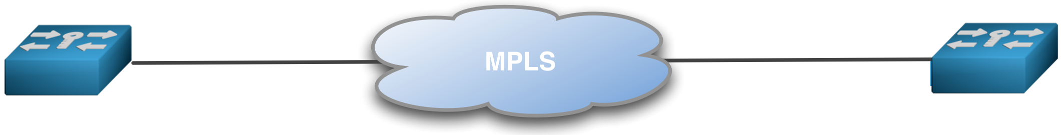
Original Ethernet frame with transport mode encryption transported over MPLS



Original Ethernet frame with frame mode encryption transported over MPLS

2.5.1. Ethernet over MPLS/VPLS

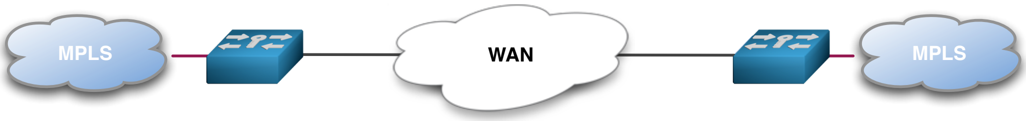
If Ethernet frames are transported over an MPLS network (EoMPLS) no direct MPLS support is needed as long as the Ethernet header remains unencrypted as MPLS needs the Ethernet header information.



Ethernet transport mode encryption will provide the necessary transparency. There are two different ways to transport Ethernet over MPLS: On a continuous Ethernet network MPLS puts its tags between the Ethernet header and the payload, If an Ethernet frame needs to be transported over different layer 2 networks MPLS encapsulates the original frame and turns it into MPLS payload. The MPLS tag is put in front of the payload.

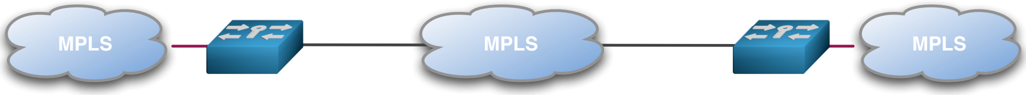
2.5.2. MPLS Interconnect

In a scenario in which local MPLS clouds are interconnected through a WAN that needs to be encrypted, the encryptor has to detect the frame format and adjust the encryption to it. The frame is either a standard frame with an inserted MPLS tag or an Ethernet frame with MPLS tag that carries the original Ethernet frame encapsulated as payload. In both cases only the payload should be encrypted, which consists in the first case of the original Ethernet payload and in the second case of the original Ethernet frame.

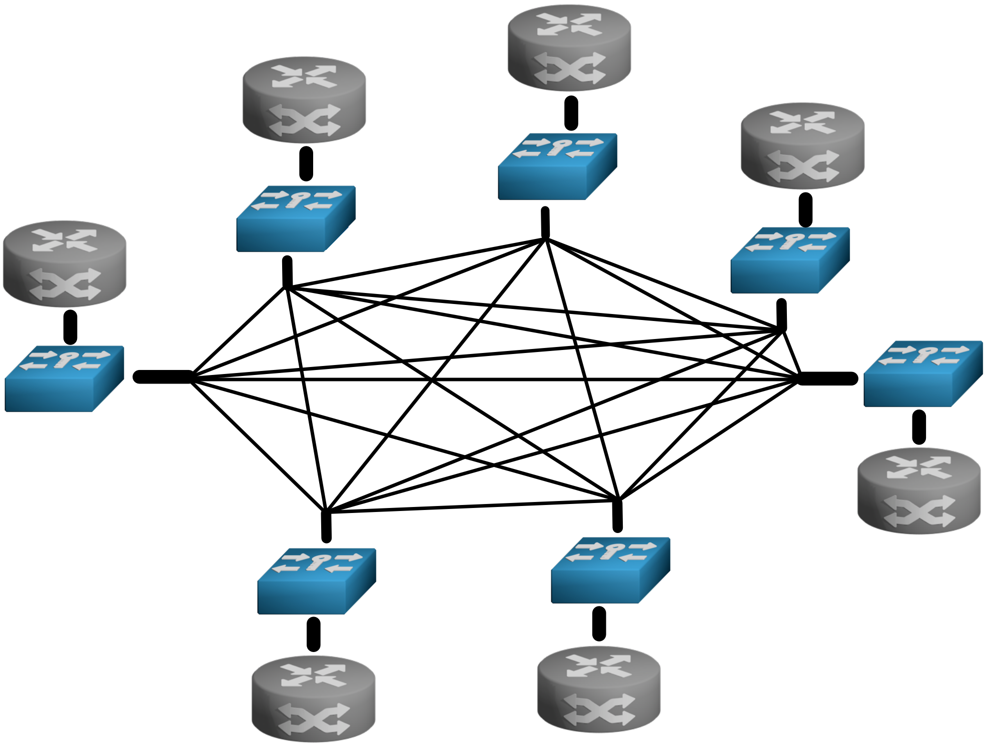


2.5.3. Between MPLS clouds

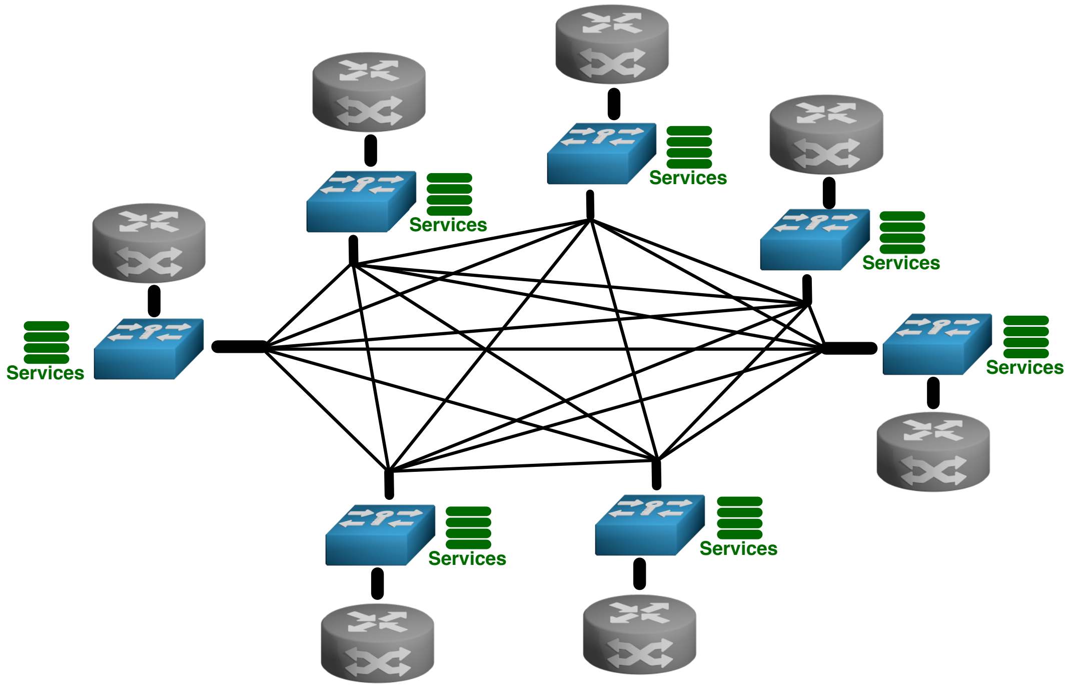
In a scenario where local MPLS clouds are interconnected through a Carrier-MPLS cloud, the encryptor must limit itself to the payload, which consists of the encapsulated original frame. The encryptor must detect that the frame contains MPLS and where the payload is located.



The following two diagrams show MPLS-based multipoint networks: One uses an Ethernet Private LAN topology and the other one an Ethernet Virtual Private LAN topology. An EP-LAN only makes sense for a closed Ethernet network without connection to external IP networks. For all other scenarios an EVP-LAN is required.



Interconnection of local MPLS clouds over Ethernet Private LAN



Interconnection of local MPLS clouds over Ethernet Virtual Private LAN

The Ethernet Virtual Private LAN allows supporting the MPLS network as one of many networks

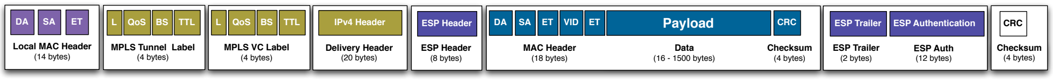
The product requirements for the encryptors differ depending on the usage scenario and the topology. Decisive are among others the encryption modes, the key system, the key assignment and the network support. Only a few of the encryptors can be parameterized to support all different scenarios in a sufficient way.

http://en.wikipedia.org/wiki/MPLS

2.5.4. Using IPSec to encrypt MPLS

MPLS networks come in different flavors. The security measures adapt to those different variants: MPLS over Ethernet, MPLS over IP, MPLS over GRE and MPLS over L2TPv3. For all variants of MPLS over IP IPSec is used in transport mode as MPLS itself is already a tunnel.

Securing MPLS with IPSec can make sense for a pure IP network, but less so in a Carrier Ethernet environment, as there it doesn't provide the combination of security and efficiency that offered by a layer 2 encryptor with full MPLS support. In terms of security it is missing the encryption and authentication of the data below layer 3 and in terms of efficiency overhead and processing speed are significantly below the possibilities of a good Ethernet encryptor.



MPLS over Ethernet, tunneled over IP and secured with IPSec

http://tools.ietf.org/html/draft-ietf-mpls-over-l2tpv3-03
http://tools.ietf.org/html/draft-ietf-mpls-in-ip-or-gre-08

Big decisions need strong security.

Wherever important decisions are made, data safety becomes just as important. Giesecke & Devrient and secunet is your team for this task. Together, we ensure governments can safely exchange critical data. And secrets stay secrets.

www.cybersecurity-madeingermany.com

secunet

Giesecke & Devrient

3. Encryption: Security, Efficiency and Operational Aspects

Different approaches have an effect on security, network compatibility, efficiency, supported usage scenarios, operations and cost. In most security concepts metropolitan and wide area networks are seen as security zones. They often carry important and sensitive data traffic, including classified data. It pays to protect these security zones properly, as it can be done at a relatively low cost when looking at cost per megabyte secured. This frees up resources for zones that are more complex and more difficult to secure.

3.1. Network security

Network security encompasses a multitude of different aspects and there are different solution approaches for most of them. Decisive for the security is the particular complete system with its implementation and not single features taken out of context[13].
In most cases, the best solution for securing layer 2 networks is the use of specialized, autonomous layer 2 encryptors. They are complete solutions that come without dependencies and keep their focus sharply on their one and only job. This is a precondition to operate as efficient and as secure 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, currently none of those approaches provides the security and efficiency offered by most of the available dedicated encryption appliances.

Two main factors define the security level that is required: (1) The protection requirements for the data transmitted over the network. Data that is considered to be somewhat sensitive causes less harm when stolen or compromised and therefore is subject to much less stringent protection requirements than data that is considered confidential or even secret. The importance and the confidentiality of the data define the security requirements. (2) The protection requirement of the network in terms of security and continuity. If an organization is dependent on a frictionless operation of the network, any impairment can have negative consequences for operations. In cases of such a dependency it is essential to have a protection of the network against attacks that is as good as possible. If there is no such dependency, then less stringent protection requirements might be sufficient.

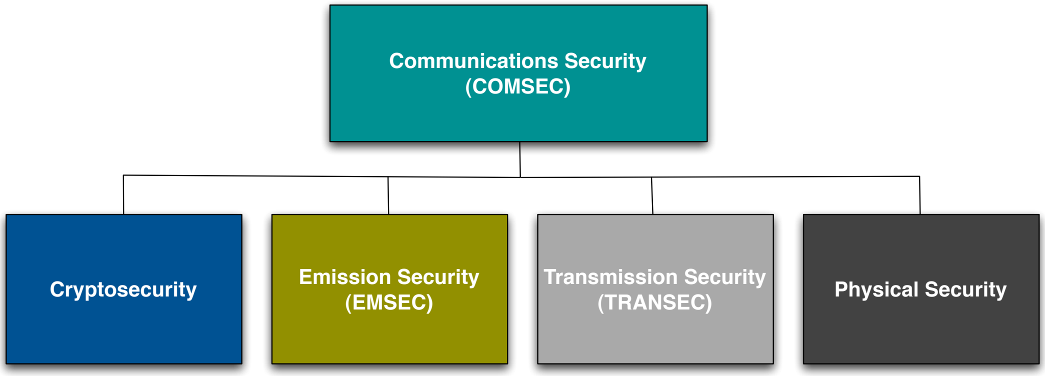
[13] https://www.schneier.com/blog/archives/2016/03/cryptography_is.html

There are three security categories of network encryptors:

- "High Assurance" for classified and sensitive data[14]
- "Standard Assurance" for sensitive data
- "Low Assurance" for somewhat sensitive and non-sensitive data

The classification is dependent on the security level that is provided by a solution. The category "High Assurance" consists of specialized appliances based on a security platform that are certified for classified data. They protect data and network reliably. Devices certified for high security levels are subject to sales and export restrictions. This prompts some vendors to have their devices only certified for lower security levels despite the devices fulfilling the requirements for higher security levels. It is the only way to be able to sell devices to the government, defense and government administration market without being prevented from participation in the business market.
The category "Standard Assurance" also consists of dedicated appliances, but these are only certified for use with sensitive data, not classified data. Such appliances offer all the essential security features and provide protection for data and network.
The "Low Assurance" category is populated to a large degree by integrated solutions that feature up to date encryption algorithms, but don't offer all the essential security features. Most of these solutions come with a certified cryptographic module, but their use should be limited to little sensitive data and networks with low protection requirements. Part of this category are e.g. integrated MACSec solutions and virtual appliances without additional hardware support.

The ultimate goal is communication security, which is the combination of crypto security, emission security, transmission security and physical security.


Communications Security (COMSEC)
Cryptosecurity
Emission Security (EMSEC)
Transmission Security (TRANSEC)
Physical Security

[14] https://en.wikipedia.org/wiki/Classified_information

Crypto security consists of multiple elements: network security, secure keys and a secure encryption device.

Full COMSEC support, which includes emission security (EMSEC) and transmission security (TRANSEC), used to be only available for the military and for governments. This is no longer the case and other organizations can now employ these advanced security features as well.

3.1.1. Secure network

To secure networks, the objective is to encrypt and authenticate as much as possible as simple as possible. There are trade-offs between network security approaches and network compatibility as the most secure approach is to encrypt everything, including the header. This kills network compatibility on the native layer as due to the lack of accessible address information no device between the end devices can process the frames.

Network security for data transport requires a combination of endpoint functionality and additional data carried along in each transmitted frame or packet. Together they can provide confidentiality of the transmitted data, ensure the integrity of the transmitted data, authenticate the transmitted data, and offer resistance against attacks. The overhead is a trade-off for security. Encryption without overhead limits security to confidentiality. The goal is to have as much overhead as necessary and as little as possible**.** Native solutions tend to be the most compatible, the most secure and the most efficient solutions.

IPSec was designed to encrypt the IP layer and what runs on top of it at layer 3. It can protect the IP protocol and everything that runs on top of it, but it can’t protect the underlying Ethernet 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 IPSec.

To protect layer 3 between sites, IPSec needs a tunneled original IP header and to protect layer 2, it needs to encapsulate the entire layer 2 frame. Both mechanisms lead to noticeable overhead and performance degradation. For site-to-site and multi-site Carrier Ethernet networks layer 2 encryption using AES-GCM with 256 bit keys is an optimal solution for the foreseeable future.

Standards and algorithms used and their implementation play an important role for network security. Without secure keys and a secure encryption device, the security provided remains limited.

3.1.2. Secure encryption device

If the network traffic is properly secured, the next targets for attack are the endpoints. It is less complex to secure a dedicated device than a portion of a larger

larger device. Although there are many less access possibilities to a dedicated device than to and within an integrated appliance or a virtual appliance, there is still the requirement to secure every single one of them. The encryption device must be fully secured against attacks from the inside and the outside. This is quite difficult by itself. The more access possibilities, the higher the complexity and the risk of vulnerabilities. Less complexity leads to more security.
Most specialized appliances are based on a security platform, 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. For integrated and virtual appliances it is between difficult and impossible to provide such a security level. There are simply too many external and internal gateways to be secured. The number of security vulnerabilities surfacing in integrated appliances such as routers, switches and firewalls is high. They make the devices prone to attacks and must be patched[15][16][17][18][19]. What becomes known in terms of vulnerabilities is just the tip of an iceberg. On top of the known vulnerabilities, there are the vulnerabilities that are not publicly known yet and constitute an uncontrollable risk. Furthermore the applying of patches in such a device leads to operating cost and network downtime.

3.1.3. Secure keys

Insecure keys compromise any encryption. Key security starts with key generation and continues with key storage and key exchange. Hardware plays again an important role. For generating secure keys true random numbers are needed. Due to the quantity and quality of entropy required, only a hardware-based true random-number generator can provide the necessary randomness. Software-based random-number generators lack the needed entropy source and can only generate pseudo random numbers. It is often the lack of real and sufficient randomness that compromises key security from the beginning[20].
Most dedicated appliances provide hardware-based true random number generation, a fully secured key storage and a secured casing. The protection can include measures against emissions. Any attempt to tamper with the unit will result in the immediate clearing of the key storage and the notification that an attempt at tampering took place. The key storage is tamper proof and the casings are tamper resistant. Such a level of security is hard to achieve with an integrated appliance, such as a switch, a router or a firewall and unachievable with

[15] https://www.cvedetails.com/vulnerability-list/vendor_id-16/Cisco.html
[16] https://www.cvedetails.com/vulnerability-list/vendor_id-874/Juniper.html
[17] https://www.cvedetails.com/vulnerability-list/vendor_id-5979/Huawei.html
[18] https://www.cvedetails.com/vulnerability-list/vendor_id-750/Nokia.html
[19] https://www.cvedetails.com/vulnerability-list/vendor_id-10/opdirt-1/HP.html
[20] http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html

a virtual appliance running in a shared environment.
One fact, that often doesn’t get the attention it deserves: Encryption uses the key in plaintext. The security of the environment in which key is used is thus a decisive factor. Encryption taking place directly on the network interface offers more attack surface and less security than encryption taking place in an area that is protected and not exposed to the exterior.

3.1.4. Transmission security (TRANSEC)

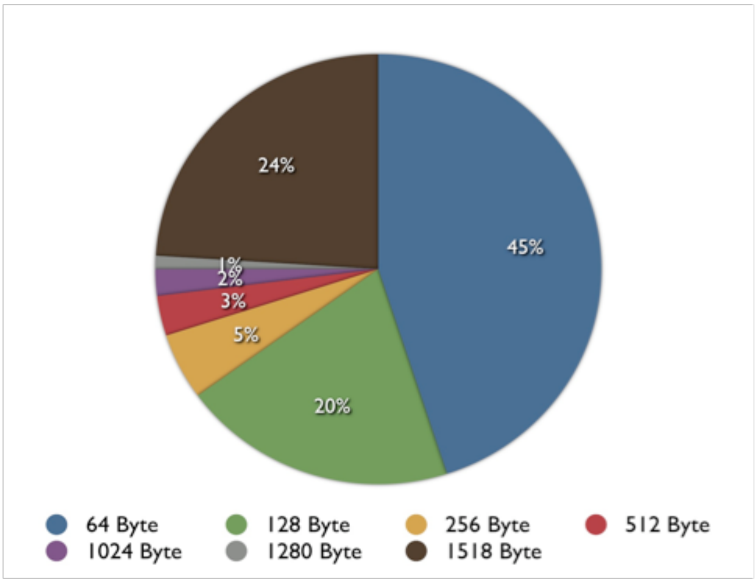
Authenticated encryption provides confidentiality and network integrity, but the network traffic remains visible. Traffic analysis reveals what is happening on the network. The countermeasure is traffic flow security, which obfuscates the network traffic. There are different approaches to implement traffic flow security. One approach uses uniformly sized frames for the transport. First a fixed frame size for the transport frame is determined. All transport frames will use exactly this frame size. The actual network frames are packed into these transport frames and thus tunneled. If two or more consecutive frames fit into the tunnel frame, they will be packed together into the tunnel frame and the remaining space is filled with randomly created dummy network traffic. If the size of a network frame exceeds the size of the maximum payload of the transport frame, the network frame is fragmented and distributed over multiple tunnel frames. This frame-oriented approach comes with noticeable overhead and latency. It main usage scenario is limited to point-to-point connections.
A different approach focuses on the traffic flow and not on the frame size. Instead of filling up frames with dummy network traffic, the dummy network traffic is added to the traffic flow and generates uniform network traffic that completely obfuscates the original network traffic. This approach can support all three different encryption modes – frame, transport and tunnel – and all topologies such as point-to-point, point-to-multipoint and multipoint-to multipoint. When using transport mode the network addresses remain visible, whereas in frame mode they are completely invisible. Tunnel mode reduces the visibility of the network addresses to the network addresses of the encryptors. When using tunnel mode, a combination of variable frame grouping and dummy network traffic insertion can prevent successful traffic analysis without compromising network compatibility. The variable grouping of frames has a positive effect on network efficiency as grouped frames only have to be authenticated once and the interframe gap falls away during transport. The actual IMIX throughput that can be reached is around 99% despite using a tunnel and adding dummy network traffic.

3.2. Efficiency, performance and upgradability

Key contributing factors for efficiency and performance are the size of the security overhead, the key system, the processing speed and the scalability.

3.2.1. Security overhead

The security overhead per frame is generated by the encryption standards and encryption modes. Proper security requires a certain amount of security overhead. Avoiding the need for padding will limit the security overhead. 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[21] when using IPSec/IPv4 and a security overhead of 24-32 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.

The security overhead on layer 2 in a Carrier Ethernet environment hardly has a negative impact on the Maximum Transfer Unit (MTU), as the MTU in a Carrier Ethernet environment has a recommended size of 2000 bytes and nor-

[21] http://packetpushers.net/ipsec-bandwidth-overhead-using-aes/

mally is not smaller than 1600 bytes. This provides even plenty of room for tunnel mode encryption combined with authenticated encryption. For Carrier Ethernet networks supporting only MTUs of 1500 bytes or less there are two options: Adapting the maximum MTU on the uplink on the customer side to the limitations on the carrier side or fragmenting oversized frames before handoff. Some dedicated appliances provide the option to fragment oversized packets in case of a lower MTU on the carrier side.

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. 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.

3.2.2. 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 that 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.
It is not excluded that there will be integrated appliances that use an ASIC or a subsystem with its proper FPGA. E.g. there are ASICs that include most of what is needed for MACSec, but these are either part of the network interface or part of the network processor and provide additional attack surface. Line cards often suffer from limited internal system throughput, preventing the use of the full network bandwidth. E.g. the ASIC-based solution on a line card from a leading network equipment vendor has an IMIX throughput of 90%.

FPGAs combine the versatility of a software solution with the speed and security of hardware: The latency for hardware-supported layer 2 encryptors is measured in microseconds, whereas software-based encryption with IPSec is measured in milliseconds. Between microseconds and milliseconds there is a factor of 1000.

3.2.3. 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 Gate 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.

3.2.4. Cost

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 tend to 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. This applies to vendor- and platform-specific MACSec implementations as well. If the encryption is integrated with the switch/router you are most probably subject to a double vendor lock-in. Changing the vendor at a single site then will exclude that site in terms of encryption from the MAN/WAN, as it is mandatory to use the same vendor for encryption and for switching at all sites. This severely reduces the possibility of cost reductions through a change of suppliers, such as from Cisco to Juniper, HP, Arista, Avaya 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.

3.3. Operational aspects

3.3.1. Ease-of-deployment

Ethernet encryptors are a bump in the wire. They integrate seamlessly into existing networks and provide the required network functionalities. There is no need to reconfigure networks. The setup is quick and practically error-proof. Network downtime is reduced to a minimum. Solutions based on IPSec tend to be more complex, more time-consuming and more error-prone.
Integrated solutions based on MACSec are also simple to configure, but they only provide low assurance protection.

3.3.2. 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 through lower cost of personnel and lower operating cost.
It makes more sense to protect Ethernet-based site-to-site and multi-site networks with Ethernet encryption instead of using IPSec, as it this secures everything layer 2 and above and comes without built-in performance degradation. The same is true for layer 2.5 VPNs (MPLS) that can be efficiently encrypted at layer 2.

From layer 2 there is 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. In the case of direct fiber optical connections accommodating multiple layer 2 protocols authenticated OTN encryption at layer 1 can provide similar benefits, but mostly limited to point-to-point.

Ethernet encryption can also be used to secure IP-based site-to-site and multi-site networks with Ethernet over IP (EoIP). Combined with a sophisticated group key management and traffic flow optimization this is a secure and efficient alternative to GETVPN.

The overall operating cost tends to be lower for layer 2 encryption than for layer 3 encryption due to the simplicity, the completeness of the protection and the lower overhead. The cost advantages increase with higher bandwidths.

3.3.3. Cost savings potential

If the network is properly structured and network carrier has a good offering, there is a dormant cost savings potential. Access line consolidation helps to lower ongoing cost. As hardly any site has more than two completely redundant network accesses, in most cases there is no operational or financial reason to pay for more than two network accesses.

3.3.4. Security certifications: What are they worth?

Vendors often are using security certifications to pretend more "certified" security than the security that is actually provided. Two of the most misused certifications are FIPS and Common Criteria. It is not accidental that FIPS- and Common Criteria-certified products have proven to provide less security than promised and needed. Otherwise there would be no reason for the US administration to keep complaining about successful attacks against US government networks. The FIPS certification is available for different classes and different sectors. Only a very small number of FIPS-certified devices have been thoroughly tested and certified as a complete system. This despite the fact, that often the device boundaries are used and defined as cryptographic boundaries. The Cryptographic Module Validation Program[22] is limited to the cryptographic module. A new validation is only required if changes such as updates are applied to the cryptographic module or if the sunset period of five years has expired without any changes to the validated cryptographic module. It is however not uncommon, that an existing certification is not revoked despite existing vulnerabilities that are known, become known or should be known[23]. FIPS certification is more about meeting clearly defined formal requirements about actual security. FIPS itself is a national specification for the protection of sensitive data and a precondition for access to the US and Canadian government market. It is however not an international security standard. A FIPS certification itself is not a trustworthy proof for fulfilling current security requirements. Vendors of FIPS certified products of course happen to see this differently. Operating products in FIPS mode is a latent security risk.

Common Criteria focuses on security targets and verifies if they are met. The vendor chooses his own security targets to meet. It seems obvious that a vendor defines and chooses those security targets that he is sure to fulfill. In some areas there are pre-defined security targets, but there are none for Ethernet encryp-

[22] http://veridicalsystems.com/blog/secure-or-compliant-pick-one/

[23] http://veridicalsystems.com/blog/immutability-of-fips/

tors. This is the reason why they are no official certifications for Ethernet encryptors on an international level. Most vendors who market their Common Criteria certification only met their self-selected and self-defined security targets. The only profile existing today is limited to MACSec Ethernet encryption for point-to-point connections[24]. It has been developed by NIAP (National Information Assurance Program). The sponsor of the profile is the NSA. The profile is limited to MACSec, is completely based on US standards and enforces specifications that have the potential to limit the security that is provided. The enforced specifications include the use of specific NIST curves for elliptic curve cryptography and the use of random number generators complying with the NIST standard required for FIPS certification. In this profile security boundary equals device boundary and the device is assumed to be secure.

There are some certifications that actually deliver what they promise: Certified security. One of them is the approval for the protection of classified data by the German “Bundesamt für Sicherheit in der Informationstechnik (BSI)”. The test and verification encompasses the entire system including all implementation details and source code of software and hardware. ASIC-based solutions than cannot be properly evaluated do not get approval. Each change requires a new evaluation. If a product has not been updated for a period of five years, the certification is revoked. The BSI limits the validity of the duration of an approval if a product contains algorithms and key lengths that it considers as only sufficient for a shorter period of time, or if the product contains potential vulnerabilities (e.g. in the user interface mechanisms) that could be exploited within the near future.

Certifications and approvals, be that FIPS, Common Criteria, BSI or others, are only granted for certifiable configurations. Only the operation of the device in such a configuration is certified or approved.

[24] https://www.niap-ccevs.org/Profile/Info.cfm?id=342

atmedia

secure data communication

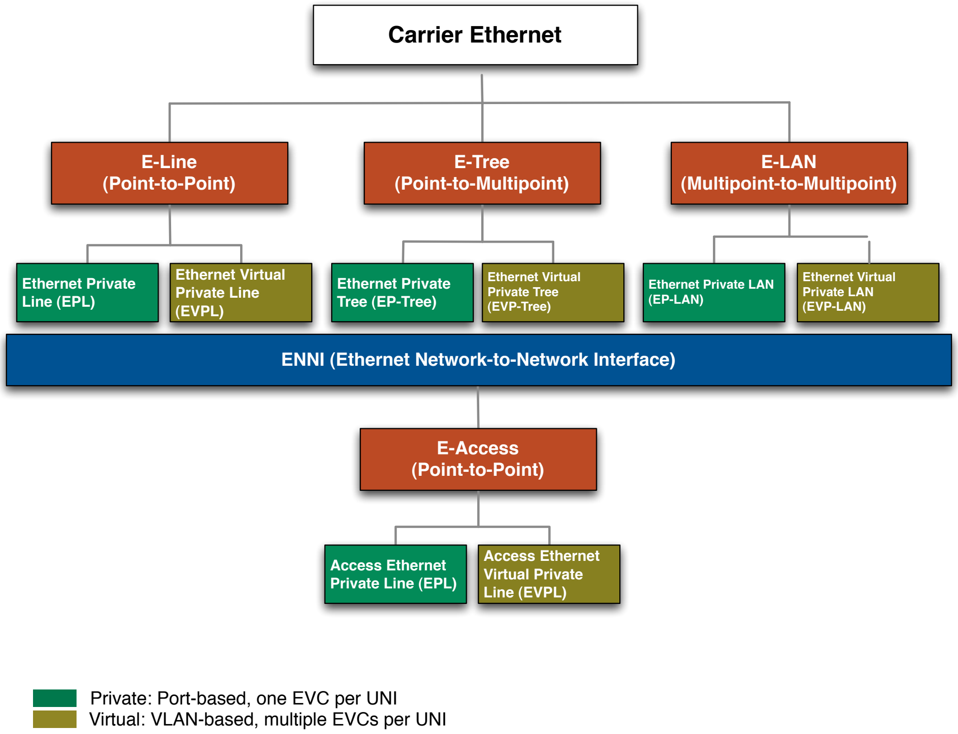
High Assurance Network Encryption

4. Ethernet for Metro and Wide Area Networks: Carrier Ethernet 2.0

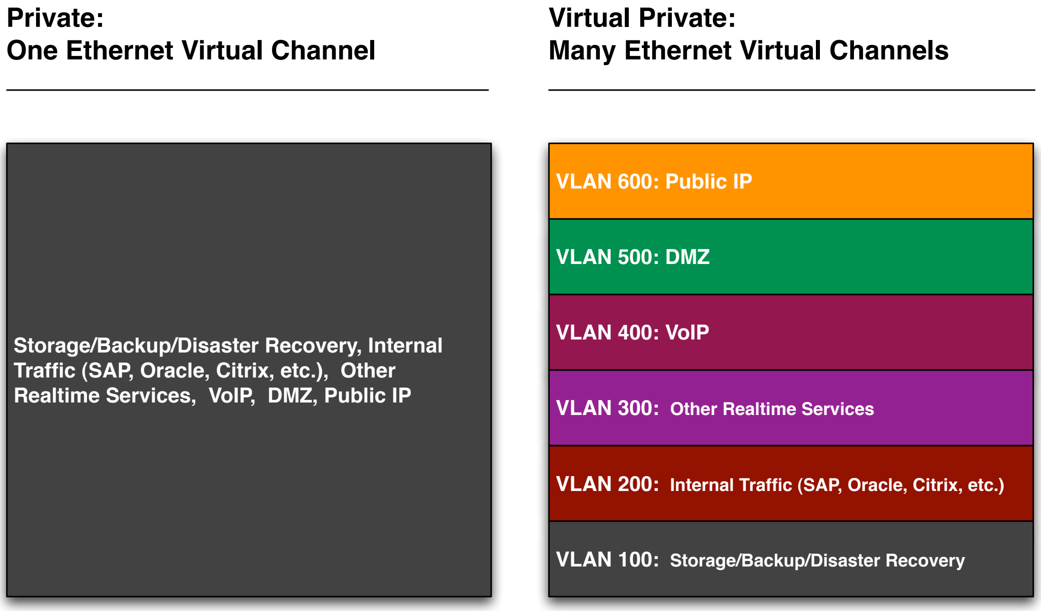
Originally Ethernet is a standard for local area networks (LAN), that is defined, maintained and extended by IEEE. Carrier Ethernet builds on that standard, but is adapted to the needs of metro area networks (MAN) and wide area networks (WAN). Standards body for Metro and Carrier Ethernet is the Metro Ethernet Forum (MEF). Regional and wide area networks differ quite substantially from local area networks and this has implications on the requirements for an encryptor. What is relatively easy to accomplish within a LAN or for a single point-to-point connection, becomes much more complicated due to the different scenarios that have to be supported.

4.1. Carrier Ethernet: Access and topologies

The Metro Ethernet Forum (MEF) defined and standardized three different topologies available for Metro and Wide Area Networks based on the Ethernet networking standard. The initial scenario was limited to a single carrier providing all access and network services. Without a standardized interface to connect the Ethernet networks of carriers and local access providers, the scope of Carrier Ethernet was too limited. Ethernet Network-to-Network Interface (ENNI) standardizes the interconnectivity between different networks.

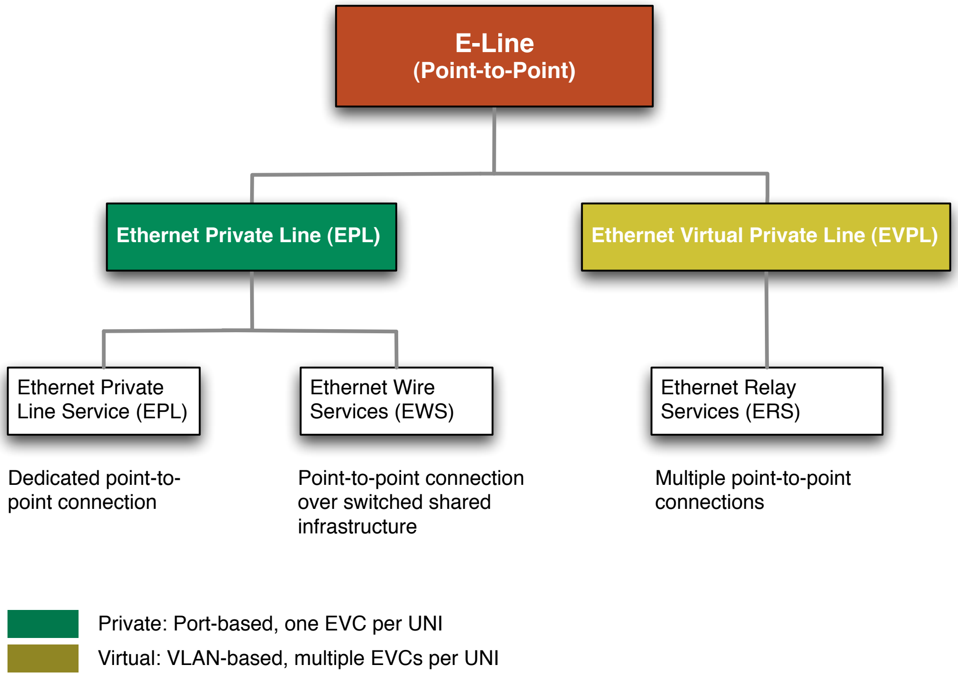

Carrier Ethernet
E-Line
(Point-to-Point)
E-Tree
(Point-to-Multipoint)
E-LAN
(Multipoint-to-Multipoint)
Ethernet Private Line (EPL)
Ethernet Virtual Private Line (EVPL)
Ethernet Private Tree (EP-Tree)
Ethernet Virtual Private Tree (EVP-Tree)
Ethernet Private LAN (EP-LAN)
Ethernet Virtual Private LAN (EVP-LAN)
ENNI (Ethernet Network-to-Network Interface)
E-Access
(Point-to-Point)
Access Ethernet Private Line (EPL)
Access Ethernet Virtual Private Line (EVPL)
🟩 Private: Port-based, one EVC per UNI
🟨 Virtual: VLAN-based, multiple EVCs per UNI

Carrier Ethernet differentiates between “private” and “virtual private” topologies. The port-based private variants are limited to a single Ethernet Virtual Channel (EVC). All untagged and priority tagged frames are assigned to a VLAN-ID and mapped to a single EVC. The VLAN-based virtual private variants support multiple VLANs and multiple EVCs. Each EVC can contain multiple VLANs, as long as they belong to the same class of service (CoS). This provides much more flexibility and allows – in combination with sophisticated group key system – the cryptographic separation of subnets. The increased flexibility of such a combination broadens the application range while concurrently lowering the operating costs.


Private:
One Ethernet Virtual Channel
Storage/Backup/Disaster Recovery, Internal Traffic (SAP, Oracle, Citrix, etc.), Other Realtime Services, VoIP, DMZ, Public IP
Virtual Private:
Many Ethernet Virtual Channels
VLAN 600: Public IP
VLAN 500: DMZ
VLAN 400: VoIP
VLAN 300: Other Realtime Services
VLAN 200: Internal Traffic (SAP, Oracle, Citrix, etc.)
VLAN 100: Storage/Backup/Disaster Recovery

4.2. E-Line (Point-to-Point)

Point-to-point comes in three different variations that correspond to three different usage scenarios. Not all encryptors support all three usage scenarios. The Metro Ethernet Forum (MEF) defined these usage scenarios as different topologies:

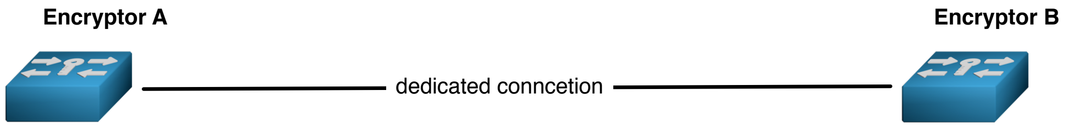

E-Line
(Point-to-Point)
Ethernet Private Line (EPL)
Ethernet Virtual Private Line (EVPL)
Ethernet Private Line Service (EPL)
Ethernet Wire Services (EWS)
Ethernet Relay Services (ERS)
Dedicated point-to-point connection
Point-to-point connection over switched shared infrastructure
Multiple point-to-point connections
🟩 Private: Port-based, one EVC per UNI
🟨 Virtual: VLAN-based, multiple EVCs per UNI

The main differentiation is between port-based and VLAN-based connections (Private Line vs. Virtual Private Line). Port-based connections are further differentiated between dedicated and shared lines.

Shown as network diagrams, these topologies look as follows:

4.2.1. Ethernet Private Line Service

Ethernet Private Line Service offers a direct line between the two encryptors. The line is either based on dark fiber or on xWDM.

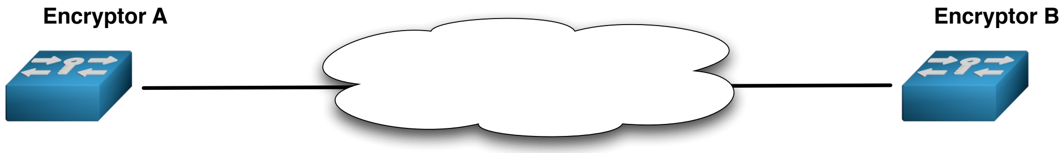


As there are no active network components between the two encryptors, Ethernet Private Line Service is a hop-to-hop scenario. Although any of the encryption modes can be used in this scenario, due to security and efficiency reasons the preferred encryption mode for Ethernet Private Line Service is the bulk mode. It provides frame encryption that covers the entire frame between preamble and interframe gap. Frame mode encryption can be combined with traffic flow security, so that artificial network traffic is added to the actual network traffic and frames are grouped. Actual and artificial network traffic cannot be distinguished as the actual network traffic is hidden within the overall network traffic. For full security, authenticated encryption is still required.

Authenticated OTN encryption at layer 1 can also provide an efficient security solution in this scenario.

4.2.2. Ethernet Wire Service

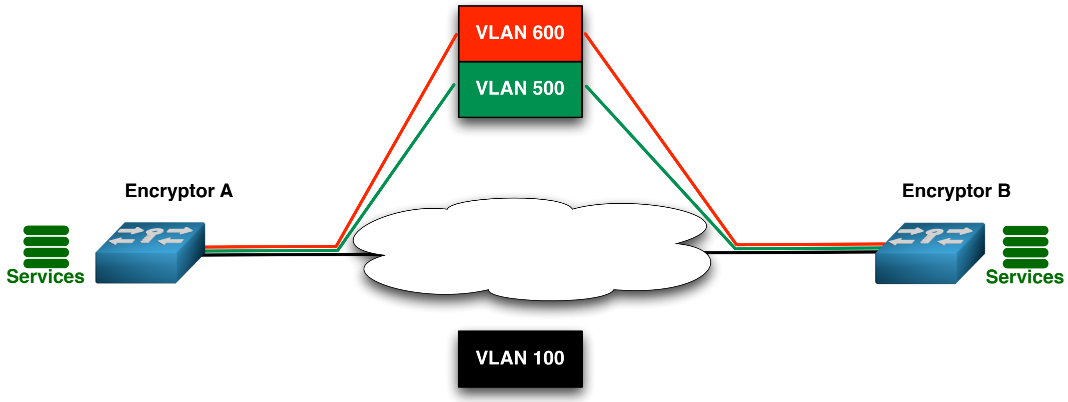
Contrary to Ethernet Private Line Service, Ethernet Wire Service uses a shared infrastructure. This infrastructure can consist of different elements: From a pure layer 2 cloud up to a mixture of layer 2 and layer 3 clouds. Ethernet Wire Service only supports one single service, so that all data traffic is treated the same and is encrypted. A differentiation based on VLAN ID is not possible.



This topology has active network components between the two encryptors, which limits the available encryption mode options to transport mode and tunnel mode.

4.2.3. Ethernet Virtual Private Line Service

Ethernet Virtual Private Service offers multiple services per connection. This provides several advantages. One of them is the consolidation of lines while maintaining multiple services. Ethernet Virtual Private Line Service is VLAN-based: Different VLANs can be assigned to different services. This allows e.g. the encrypted Ethernet interconnection of two sites, while other VLANs provide connection to the private IP-network and the public Internet.

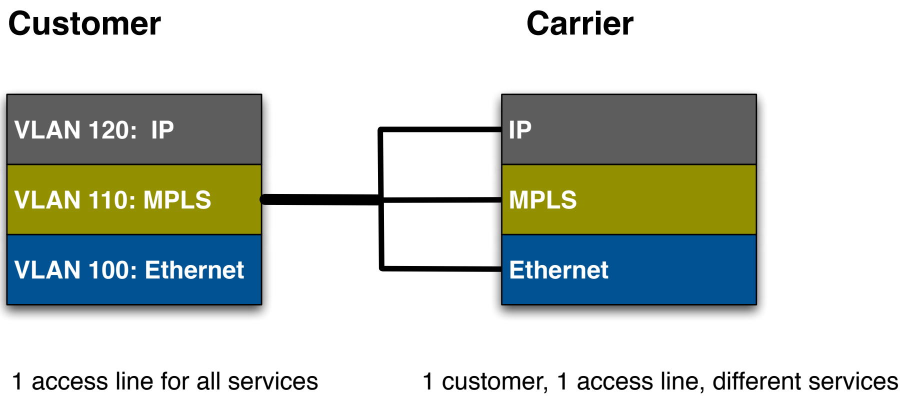


This topology also has active network components between the two encryptors. This limits the available encryption mode options to transport mode and tunnel mode. To secure an Ethernet Virtual Private Line Service, the encryptor has to support selective encryption based on VLAN ID.

4.3. E-Access

What the Metro Ethernet Forum labels as E-Access is the Ethernet access to one or multiple data networks over a local provider. It is the local Ethernet up-ramp for a range of different services (Ethernet, MPLS; IP, etc.). Before the introduction of Ethernet Network-to-Network Interface (ENNI), there was no standardized way to interconnect Ethernet services from different carriers. Without interconnection, the reach of Ethernet services was limited. Using ENNI, local, national and international telecom operators can now interconnect their networks. It is only possible to have a single provider if the telecom operator who operates the regional and wide area network directly provides the local connections as well. Such a scenario is mostly limited to regional and national networks.

Local up-ramps can have additional benefits, such as the consolidation of access lines. Only a very small number of building features more than two completely redundant connections to redundant telecom networks. An extensive amount of different physical connections will hardly improve that. A connection with 10Gb/sec through a single telecom operator is about as redundant as ten separate physical connections with 1Gb/sec each through the same single telecom operator


Customer
Carrier
VLAN 120: IP
VLAN 110: MPLS
VLAN 100: Ethernet
IP
MPLS
Ethernet
1 access line for all services
1 customer, 1 access line, different services

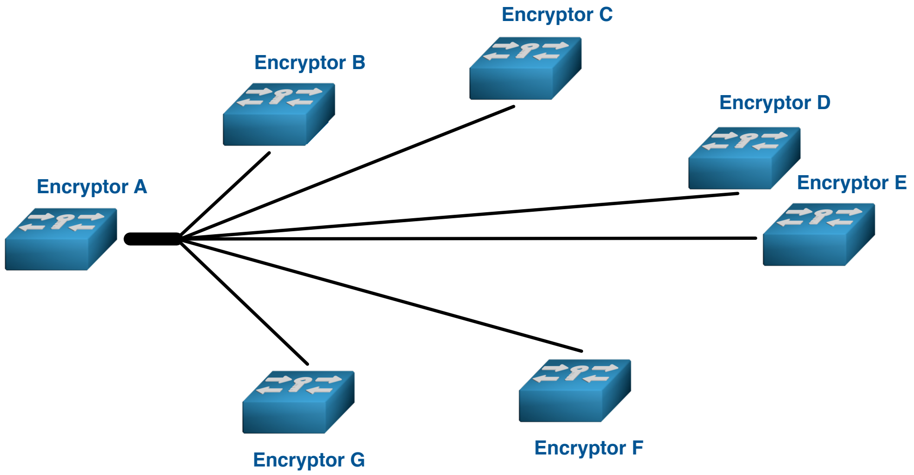
The consolidation of access lines can lead to noticeable cost savings. Not just concerning line cost, but also concerning encryptors. The higher the bandwidth, the lower normally the cost per megabit or gigabit. It is mandatory though, to have a telecom operator who will resolve the different assignments of VLAN-IDs to network types on his side and switch/route to the appropriate network services.

4.4. E-Tree (Point-to-Multipoint)

What the Metro Ethernet Forum calls E-Tree is also known as „hub & spoke“, „rooted multipoint“ or „point-to-multipoint“. It comes in two variants, of which one is port-based and the other one is VLAN-based. The latter offers multiple services (Ethernet Virtual Channels) on a single port, the hub-port, so that on that port multiple services – separated by VLAN-IDs – can be used. For the private E-Tree there is also the approach to virtualize the port of the Hub in order to support multiple point-to-point connections within a single Ethernet Virtual Channel. Limited scalability and flexibility make this approach suboptimal and reduce its use preferably to small networks.
For both variants – private and virtual private – the same rules apply: A hub/root may and can only communicate with each spoke/leaf separately, whereas as a spoke/leaf may an can only communicate directly with a hub/root, but not with another spoke/leaf.

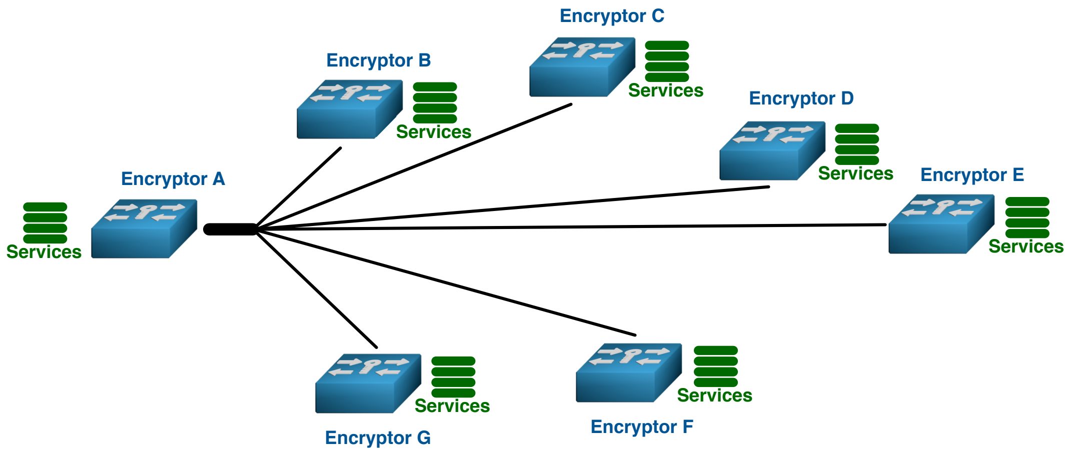
4.4.1. Ethernet Private Tree (EP-Tree)

An Ethernet Private Tree can be operated over dedicated or shared lines. Dedicated lines are mostly used in MAN environments as the cost of dedicated lines tend to be based on distance. There is no special Metro Ethernet Forum topology defined for using E-Tree over dedicated lines.

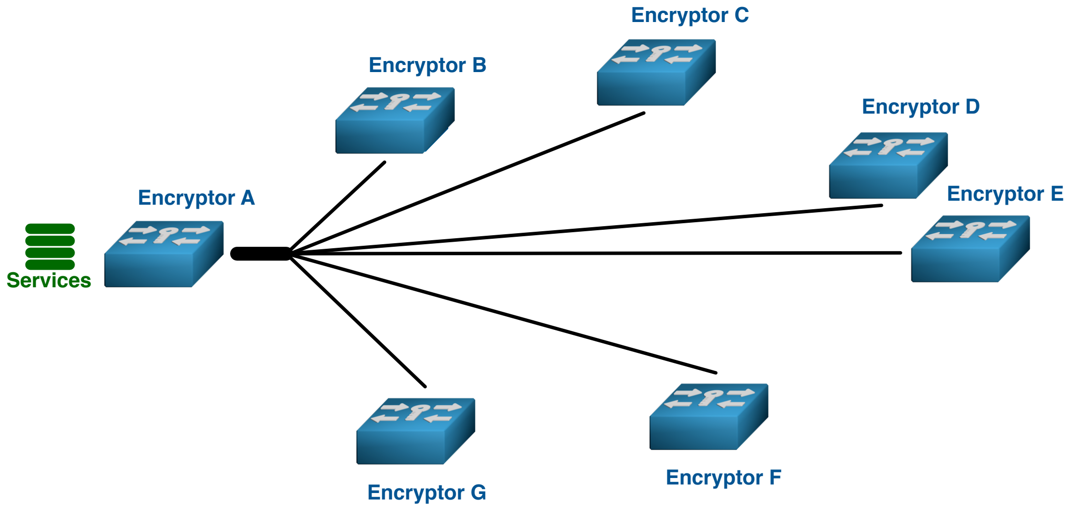


4.4.2. Ethernet Virtual Private Tree (EVP-Tree)

At the User Network Interface (UNI) Ethernet Virtual Private Tree offers multiple services that are separated by VLAN ID. The Ethernet Virtual Tree is only one of those services. For the EVP-Tree certain rules apply: Root can only communicate with other roots and with each of the leafs separately, the leafs can only communicate with the root(s).



One of the available possibilities is to define the hub as Ethernet Virtual Tree while limiting the communication of the spokes to the connection with the hub. This allows the hub to communicate with other hubs while excluding the spokes from access to that communication.



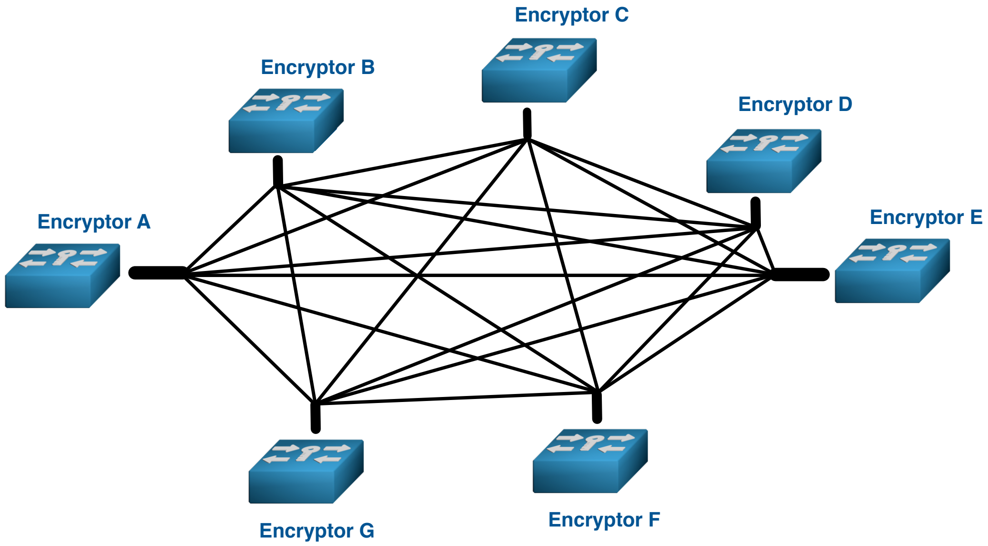
It is also possible to use multiple hubs within an E-Tree scenario.

4.5. E-LAN (Multipoint-to-Multipoint, Mesh)

Also known as mesh, any-to-any and multipoint-to-multipoint networks, Ethernet LAN Services support the communication of any member with every other member without any restriction. What looks like a LAN is in fact a metropolitan- or wide-area network and behaves like one. Distance leads to latency, which can make a huge difference. Additionally the network is not controlled by the customer, but by one or many telecom operators. In terms of functionality however, E-LAN offers the same possibilities as a LAN.

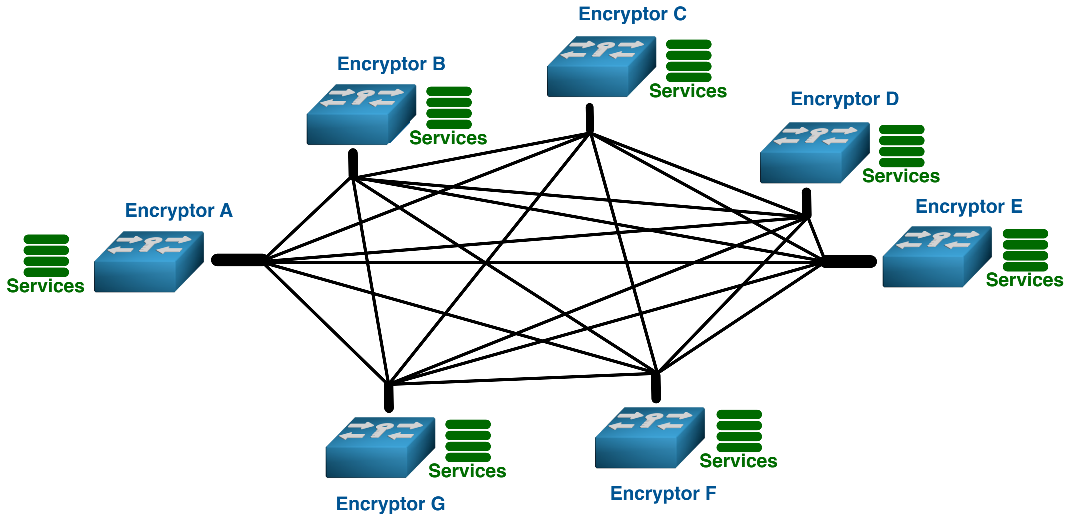
4.5.1. Ethernet Private LAN (EP-LAN)

An Ethernet Private LAN can be operated over dedicated lines or a shared infrastructure. Dedicated lines are mostly used in MAN environments as the cost of dedicated lines tend to be based on distance. Additionally, the cost for the needed redundancy has to be paid by the customer and the number of necessary lines increases disproportionally high with each site added. There is no special Metro Ethernet Forum topology defined for using E-LAN over dedicated lines.



4.5.2. Ethernet Virtual Private LAN (EVP-LAN)

At the User Network Interface (UNI) Ethernet Virtual Private LAN offers multiple ser-vices that are separated by VLAN ID. Multipoint-to-Multipoint is only one of those services. For that service there is one rule: Everybody can communicate with everybody. De-pendent on the key system and the key assignment policy, the separation by VLAN allows an EVP-LAN topology to support all LAN topologies (point-to-point, point-to-multipoint, multipoint-to-multipoint) in parallel.



Virtual Private E-LAN offers by far the most configuration options, but not all of the currently available encryptors support all those configuration options. Basic feature requirements are cryptographic separation by VLAN, selective encryption by VLAN ID and a sophisticated group key system.

Layer 2 encryptors secure connections between two or more sites in a transparent way. They can secure layer 3 and layer 2 networks running over Carrier Ethernet connections. When using layer 2 networks special emphasis must be put on ensuring that network issues at one site don't propagate to other sites. VLANs that are stretched over multiple sites can become a major issue in case of a bridging loop causing flooding, as the problem at one site is shared within the broadcast and failure domain. Oversized VLANs with a high number of MAC and IP addresses can have their own issues, even without bridging loops[25][26][27].

A layer 2 encryptor for Carrier Ethernet secures the connection between two or more sites. Such connections can be terminated with a switch (layer 2) or a router (layer 3). An internal termination at layer 3 most of the time is the better solution[28].

[25] http://ethancbanks.com/2014/07/01/the-ethernet-switching-landscape-part-07-data-center-interconnect-dci/
[26] http://blog.ipspace.net/2016/02/vlans-and-failure-domains-revisited.html
[27] http://blog.ipspace.net/2016/03/spanning-tree-protocol-stp-and-bridging.html
[28] http://blog.ipspace.net/2012/07/the-difference-between-metro-ethernet.html

SENETAS

SENETAS LAYER 2 ENCRYPTORS

HIGH-ASSURANCE ENCRYPTION FOR CARRIER ETHERNET, METRO AND WIDE AREA NETWORKS.

SUPPORT FOR ALL ETHERNET NETWORK PROTOCOLS AND TOPOLOGIES.

From 100 Mbps to 10 Gbps and 10 x 10 Gbps multi-link up to 100 Gbps.
FIPS, Common Criteria, NATO and CAPS certified.

Contact Senetas: **info@senetas.com** | Senetas encryptors: **www.senetas.com**

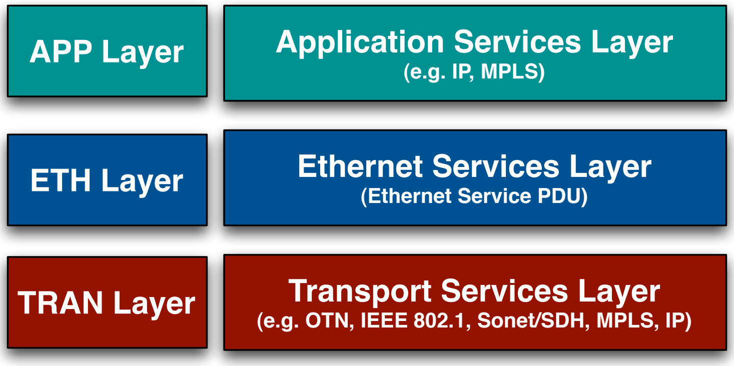
gemalto
security to be free

Senetas encryptors are globally distributed and supported by Gemalto under its SafeNet brand.

5. Carrier Ethernet: Three-Layer Model and Transport Networks

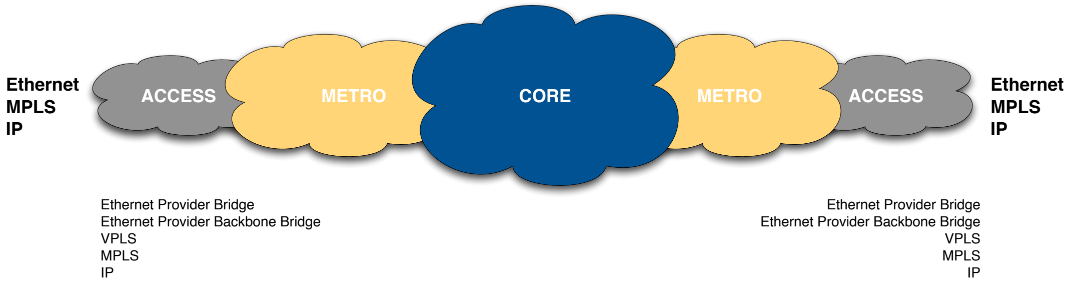
5.1. The three-layer model

The model used by the Metro Ethernet Forum is based on three layers. The MEF concentrates its efforts on the middle layer, the Ethernet services.



The three layer model shows the environment which an encryptor should be able to support. IEEE 802.1 (Ethernet) is only just one of many different transport options and each of the upper network protocols (MPLS and IP) of the Application Services Layer can in turn serve as transport layer. It is actually quite complex to fully support and secure Carrier Ethernet-based networks. .

Each of the MEF-topologies requires a transport network, that meets the requirements of the respective Ethernet service. Transport networks are not necessarily native Ethernet, as Ethernet can be transmitted over other transport networks, such as OTN, Sonet/SDH, IP and MPLS. The term Carrier Ethernet describes any transport network that is used for the transport of the Ethernet frames. The transport networks used within a MAN or WAN are not necessarily homogeneous. Depending on the placement of the encryptors and transport networks used, the original Ethernet frame can be encapsulated or tunneled. The delivered frame will be identical to the frame sent.



5.2. Native Ethernet and pseudowires

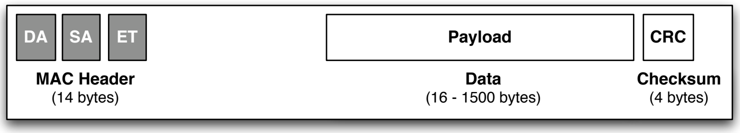
Native wired Ethernet networks are defined by the IEE 802.3 standards. They describe what is commonly known as Ethernet networks. Depending on the IEE 802.3 standard used the Ethernet frame contains additional information. The larger and more shared the network, the more information is needed in the frame.

Contrary to native networks pseudowires are not physical network connections, only logical connections. The Ethernet frames are carried as payload over the transport network provided by the logical network connection. The most common types of pseudowires on the Transport Services Layer are MPLS (often the MPLS-TP variant), OTN and IP.

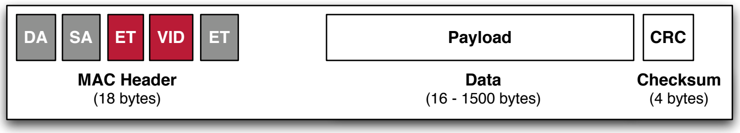
5.2.1. Native Ethernet formats

Native frame formats depend on the network and the position within the network. On the customer side (customer edge) it might look different than on the carrier side (carrier edge).

In an Ethernet scenario one will see mostly "normal" Ethernet II frames and Ethernet II frames with VLAN tag. The frames – without encryption – look as follows when handed over to the MAN/WAN transport network.



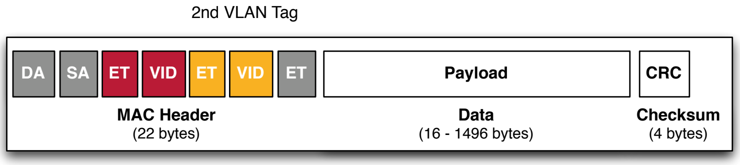
Ethernet II frame



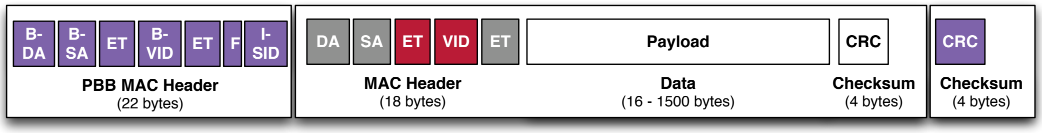
Ethernet II frame with VLAN tag

These are the most common frame formats that are encountered by an encryptor located at the customer edge in an Ethernet scenario.

On the carrier side additional information is added to the frame to ensure the necessary scalability in terms of MAC addresses.



QinQ: Ethernet II frame with hierarchical VLAN tag (IEE 802.1Q)



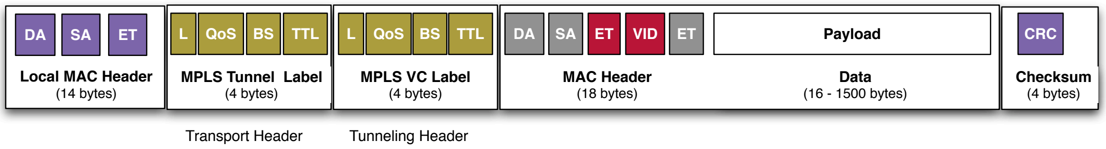
Mac-in-Mac: Ethernet II frame tunneled over Ethernet (IEEE 802.1ah)

QinQ (also known as PB - Provider Bridge) adds an additional VLAN tag on the carrier side, whereas Mac-in-Mac (also known as PBB – Provider Backbone Bridge) tunnels the original frame. These frame extensions on the carrier side are only temporary for the duration of the transport over the carrier network. They are completely transparent for the customer, who neither sees nor notices them.

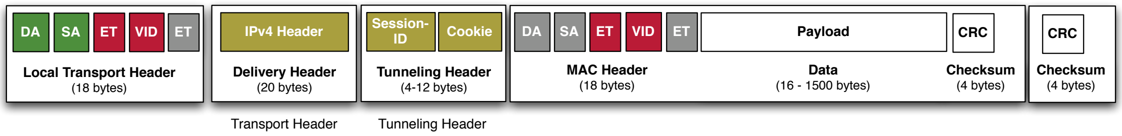
http://en.wikipedia.org/wiki/Ethernet
http://en.wikipedia.org/wiki/IEEE_802.1Q (QinQ)
http://en.wikipedia.org/wiki/IEEE_802.1ah (Mac-in-Mac)

5.2.2. Pseudowires

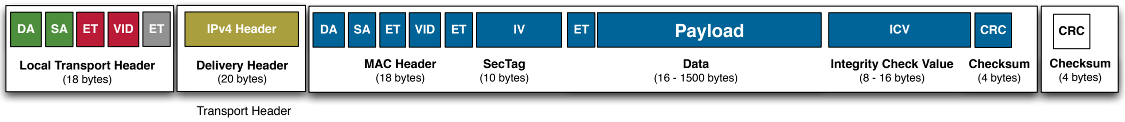
A pseudowire is the emulation of a connection-oriented layer-2 service over a packet-oriented network. On a pseudowire, the original frame is only payload and uses a different transport network than its own. Often the transport network is a combination of MPLS, IP, OTN and Sonet/SDH. For the customer the pseudowire is completely transparent, as the carrier provides him with an Ethernet access with guaranteed performance characteristics and he sees nothing but his own Ethernet network.
However, there are scenarios in which the encryptor itself has to create a pseudowire. Most often this concerns single connections within an Ethernet MAN or WAN that can only be transported over an IP network. In such a case the encryptor encrypts the Ethernet frame and adds an IP header in front of it. This allows for an efficient encryption on layer 2
The most common formats are Ethernet over MPLS (EoMPLS) and Ethernet over IP (EoIP).



Frame Ethernet over MPLS (EoMPLS)



Frame Ethernet over IP (L2TPv3)



Frame encrypted Ethernet over IP (EoIP)

If Ethernet uses such a transport network, attacks against the transport network can cause the non-arrival of frames at the destination site and the infiltration of additional frames.

http://en.wikipedia.org/wiki/VPLS
http://en.wikipedia.org/wiki/MPLS

Pseudowires also provide attack surface:

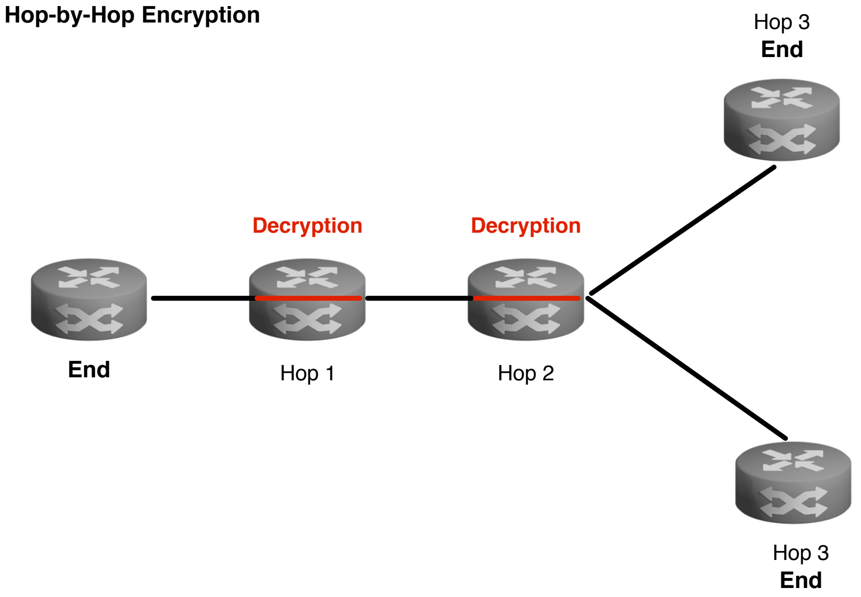
https://www.ernw.de/download/ERNW_MPLS-Carrier-Ethernet.pdf
https://www.blackhat.com/presentations/bh-europe-09/Rey_Mende/BlackHat-Europe-2009-Mende-Rey-All-Your-Packets-wp.pdf
http://www.blackhat.com/presentations/bh-europe-09/Rey_Mende/BlackHat-Europe-2009-Mende-Rey-All-Your-Packets-slides.pdf

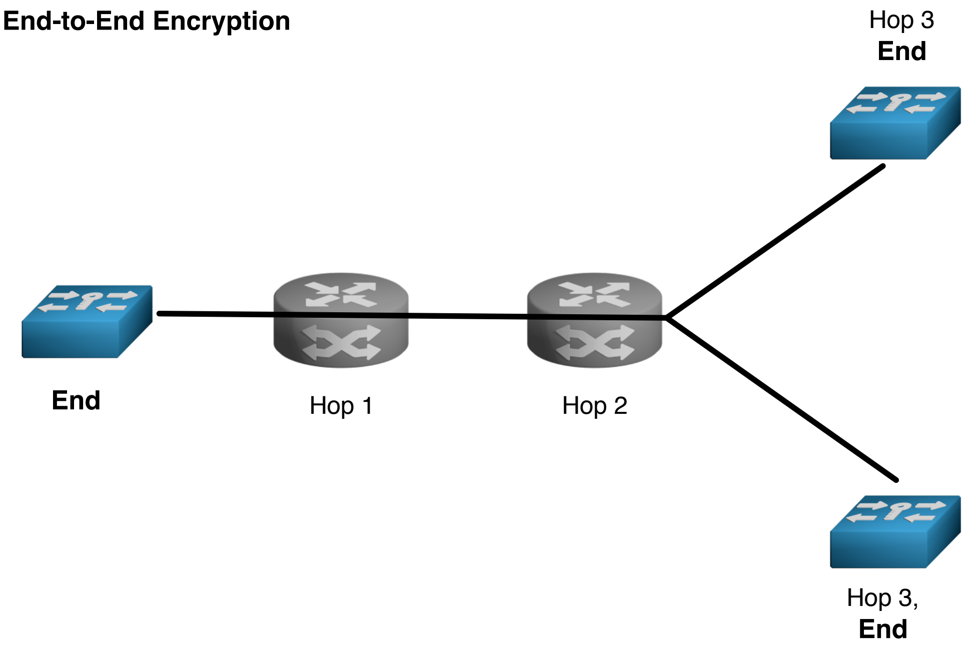
6. Position of the Encryptors

Ethernet encryptors secure connections between sites. Such a site can be a data center, corporate headquarters, a manufacturing site, a branch office, or any type of site that needs to be interconnected and integrated into a MAN or WAN. The network can also encompass Private and Community Clouds. The encryptors are normally positioned at the intersection between a proprietary network and a shared network. The positions shown are of logical nature and do have an impact on product requirements

6.1. Hop-by-hop vs. end-to-end

The flexibility concerning positioning location in the network is to a large degree defined by the basic principle used and the functionality of the encryptor in terms of conditional encryption and conditional encryption offset. A hop-by-hop encryption is an encryption between two nodes that are one hop apart. At each hop the data is decrypted, processed in unencrypted form, re-encrypted and sent to the next hop. End-to-end encryption works differently: The data remains encrypted and secure during the entire transmission between sender and receiver even if there are multiple hops in-between.

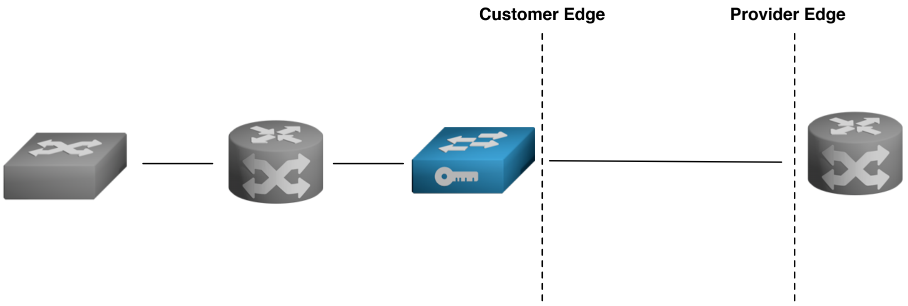




In a local area network (LAN) a hop-by-hop encryption can be preferable, but in a MAN or WAN environment it should only be considered as an option if the next hop is also the endpoint of the connection. The usage scenario and the flexibility of hop-by-hop encryption solutions are severely limited. Using tunnels can create an adjacency, but tunneling usually comes with increased overhead and higher latency. End-to-end encryptions is more efficient and more flexible.

6.2. Between Customer Edge (CE) and Provider Edge (PE)

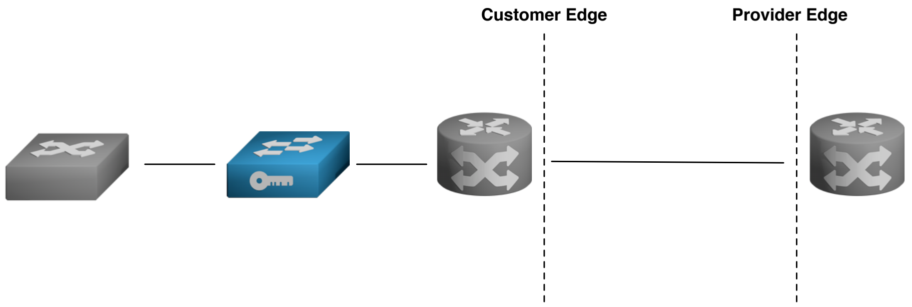
The encryptor creates a borderline between the local network at a site and the network of the telecom operator. This is the most frequent scenario.



The first hop, i.e. the first active network component after the encryptor, is a device owned and controlled by the telecom operator. There is little incentive to include that into one's own network and it is probably not a smart idea to have all data present in unencrypted form on that device.

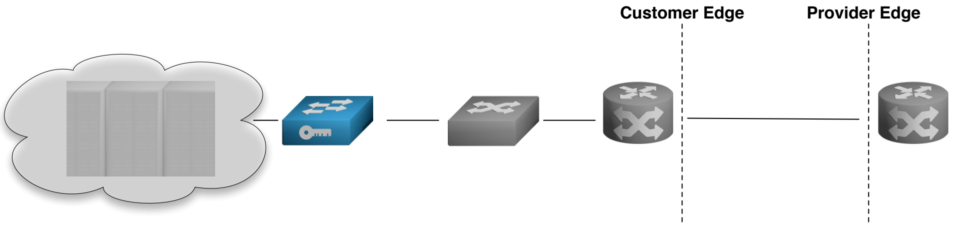
6.3. Between Customer (C) and Customer Edge (CE)

It is also possible to shift the encryptor deeper into the local area network.

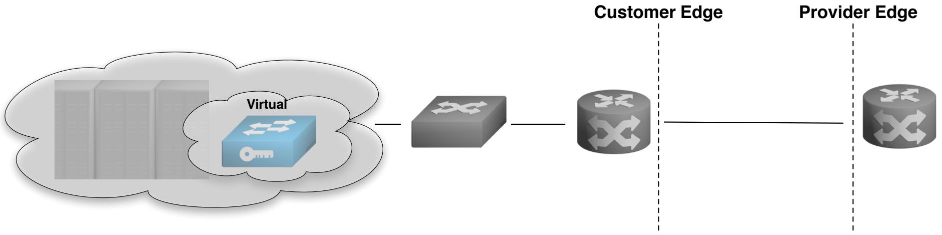


6.4. Between cloud Customer and Customer Edge (CE)

To secure the connection with a private or a community cloud, an encryptor can be positioned directly in front of the cloud.

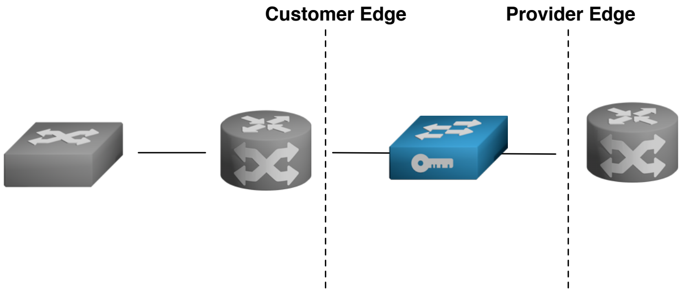


6.5. Within a cloud



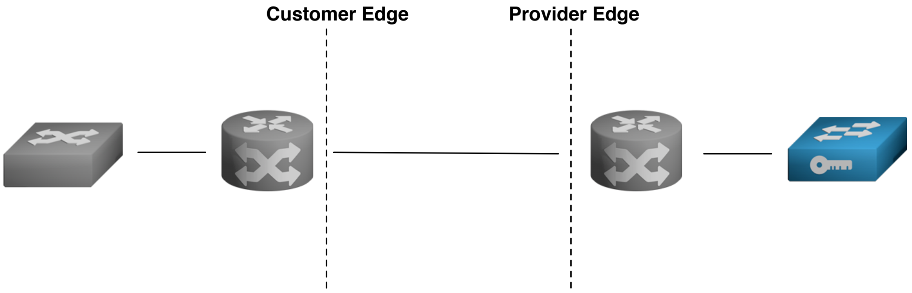
Using a virtual appliance to secure an Ethernet connection within a cloud is only appropriate in a very limited number of scenarios. In a virtualized environment key security is hardly existent. Without additional hardware protection all encryption keys used by the virtual appliance remain accessible. There are two ways to improve the situation: (1) Adding a secure key storage such as a smartcard to the cloud hardware, and (2) using one of the other encryption appliances as Hardware Security Module (HSM) for the virtual appliances. Even then, one gaping security weakness remains: Encryption keys are always used in plaintext for the encryption process. Unless the cloud is completely secured, it is not a safe operating environment and thus not a safe encryption device.

6.6. Between Provider Edge (PE) and Customer Edge (CE)



This setup is primarily found in two different scenarios. One is the encryption of an MPLS network at layer 2 if the customer uses his own routing tables, and the other one is encryption supplied by a telecom operator as managed service.

6.7. Between Provider Edge (PE) and Provider (P)

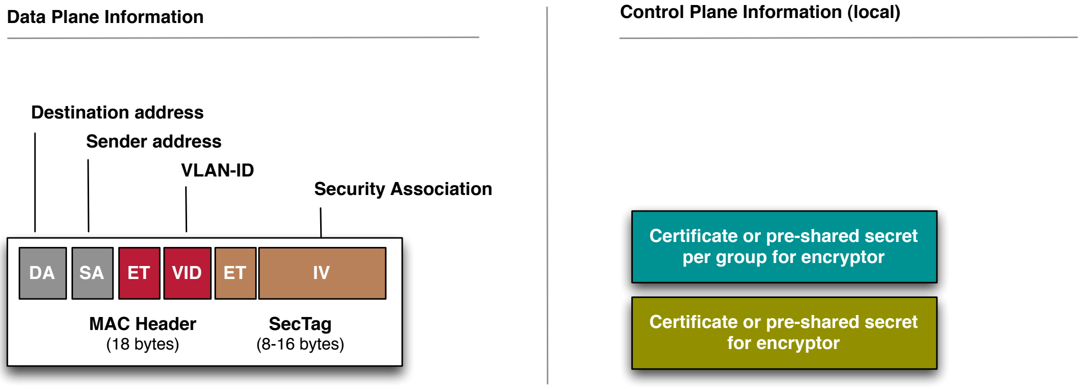


This is also a scenario that might be proposed by a telecom operator who offers encryption as managed service. As the data remains completely unprotected until it reaches the encryptor on the provider side, such a scenario should be avoided.

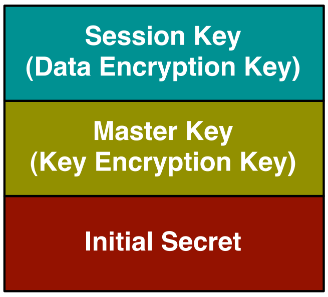
7. Key Management, Key Systems, Key Assignments and Network Topologies

7.1. Key management

Key management takes care of the generation, the exchange, storage and assignment of keys. The generation of session keys is a multi-layer process and requires an initial for each participating encryptor. The pre-distributed initial secret is the basis for the authentication and the key build-up.

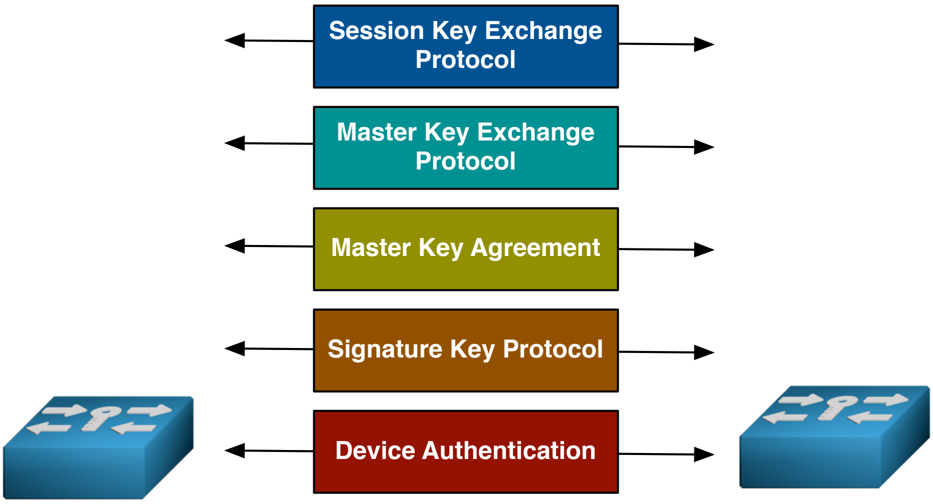

Data Plane Information
Control Plane Information (local)
Destination address
Sender address
VLAN-ID
Security Association
DA
SA
ET
VID
ET
IV
MAC Header
(18 bytes)
SecTag
(8-16 bytes)
Certificate or pre-shared secret per group for encryptor
Certificate or pre-shared secret for encryptor

A simplified view of the key build-up shows that for the encryption the following elements are needed: An initial secret for authentication and for signing, a master key (key encryption key) to encrypt the session key (data encryption key) and a session key to encrypt the data.

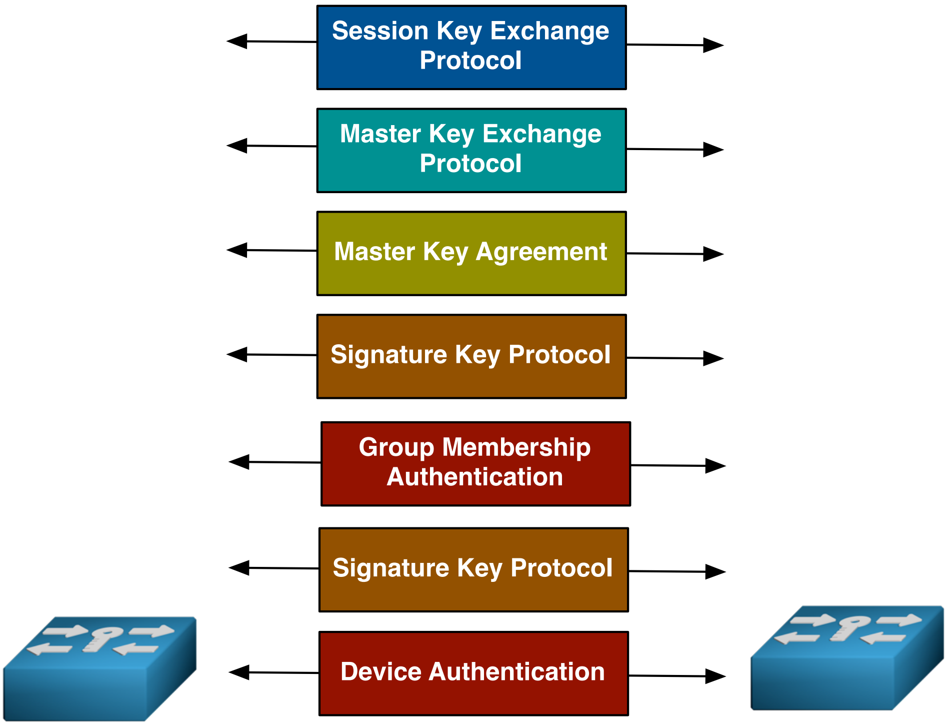


It starts with establishing who may communicate with whom. The connectivity association is the foundation for the security association that determines how the connected devices communicate securely. This is accomplished using an initial secret and a key agreement protocol. The initial secret can be a pre-shared key or a certificate. In the case of elliptic curve cryptography the curve domain is also an initial secret that needs to be present.

In the build-up from initial secret to session key, multiple complex processes take place. Each of them needs to be secure by itself and in the sequence it is being used.



The complexity is even higher for group key systems as not only the device, but also the group memberships needs authentication. This requires an additional initial secret specific to that group.


Session Key Exchange Protocol
Master Key Exchange Protocol
Master Key Agreement
Signature Key Protocol
Group Membership Authentication
Signature Key Protocol
Device Authentication

When looking at group key systems, a focus should be set on verifying that layered connectivity and security associations are supported: Next to the mutual authentication of devices and the device-based connectivity and security association also separate connectivity and security associations must be supported for each group.

The first challenge is to get the initial secrets onto the encryptors in a secure way.

7.2. Initial secret, authentication and signature protocol

Communication needs more than a single party. The participating encryptors thus need to find each other, recognize each other and authenticate themselves mutually. The authentication is based either on certificates (asymmetrical process) or on pre-shared secrets (symmetrical process).

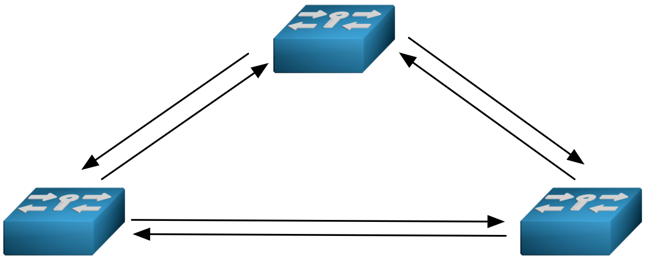
http://en.wikipedia.org/wiki/Shared_secret
http://en.wikipedia.org/wiki/X.509

Authentication using pre-shared secrets can be done between a pair of encryptors, between all members of a network, per group or per pair of encryptors in a group.

There are different approaches to authentication. An often-used approach is a port-based network access control based on IEEE 802.1x. An additional external authentication server provides the support of protocols such as RADIUS and EAP. This is more or less the standard approach used by certificate-based systems. The security level of the external infrastructure used should be at least the same as the one of the encryptor.
A common alternative is the use of an integrated network access control that is based on a combination of access control lists, pre-distributed initial secret and additional authentication mechanisms. This approach doesn't require external services and servers.

Once that is accomplished there is a connectivity association between each of the participating encryptors on which security associations can be established.

Connectivity Association



Establishment of permitted device connectivity

Authentication through certtificate or pre-shared key/pre-shared secret

The initial secretes, pre-shared secret or certificate, are used for signing in order to allow the recipient to verify the sender. The key exchange uses them to sign the keys or partial keys that are exchanged to ensure that they are coming from the correct remote device.

http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/RSA
http://crypto.stackexchange.com/questions/14654/digital-signature-using-symmetric-key-cryptography

The combination of the signature and the corresponding signature protocol is the basis for the key exchange.

7.3. Key exchange

There are two different approaches to key exchange: One is symmetrical and the other on is asymmetrical.

7.3.1. Symmetrical key exchange

In a symmetrical approach, all keys are directly derived from each other. First, a shared secret is entered into the encryptor. Then the encryptor generates internally a master key and encrypts the master key with the shared secret. The session key is also generated by the encryptor and is encrypted with the master key. Master key and session key are transmitted to the other encryptor in encrypted form. The big issue with this approach is the shared secret. If that shared secret ever becomes known, then all previously recorded data communication can be decrypted.

http://en.wikipedia.org/wiki/Symmetric_key_algorithm
http://en.wikipedia.org/wiki/Symmetric_key_management

7.3.2. Asymmetrical key exchange

In an asymmetric approach the partial keys are generated completely inside the encryptor, without any user having access to it. After exchanging the partial keys both sides calculate the same shared secret. Contrary to a symmetric approach, nobody knows the shared secret. Subsequently the encryptor internally generates the master key and encrypts it with the shared secret. The encryptor also generates the session key and uses the master key to encrypt it. The transmission of the master and session keys from one encryptor is always encrypted.

Common asymmetrical approaches are Diffie-Hellman and RSA. Diffie-Hellmann uses in its basic variant the discrete logarithm problem, which comes with the disadvantage of needing very long partial keys to be really secure. A more state-of-the-art variant is the use of Diffie-Hellman with elliptic curve cryptography (ECC), which provides better security with shorter partial keys. The security of ECC is highly dependant on the curves used. Among experts the security of the NIST curves is severely doubted. Therefore it is preferable to have a choice of curves and not be limited to NIST curves. Brainpool curves and custom curves, such as Safecurves, are a good alternative. The generation of secure elliptic curves is highly complex and also the proper implementation of elliptic curve cryptography is non-trivial. There are also speed differences between the different elliptic curves, but for multisite networks they do not really matter.

http://en.wikipedia.org/wiki/Diffie-Hellman
http://en.wikipedia.org/wiki/RSA
http://en.wikipedia.org/wiki/Elliptic_Curve_Diffie-Hellman
http://safecurves.cr.yp.to/index.html
http://www.ecc-brainpool.org/links.htm
https://tls.mbed.org/kb/cryptography/elliptic-curve-performance-nist-vs-brainpool

Asymmetrical approaches sign the partial keys that are exchanged to ensure that the correct remote station sends them. There are different ways to accomplish this: Either by using a certificate (X.509) in combination with appropriate procedures (RSA, DSA or ECC) or by encrypting the partial keys with a pre-shared secret.

7.3.3. Exchange frequency

The more frequently the sessions keys in use are replaced, the lower the probability that the key will be compromised. The security of the key does not only depend on the secrecy of the key, but also depends on the process used and the parameters chosen. The length of the counter and the ICV play an important role. E.g. in counter mode the key has to be changed before the counter starts back at 0. It is therefore required that the system automatically changes the session key after a given number of minutes.
The same is true for the key encryption key (master key), which is used to encrypt the session keys. The exchange frequency is lower as it is only used to encrypt the session key and thus is used less often and encypts less data. The regular exchange of master keys should take place automatically after a certain period of time. .

Key Type	Change Frequency
Session Key (Data Encryption Key)	every 1 - 60 minutes
Master Key (Key Encryption Key)	every 1 -24 hours
Initial Secret	every 12 - 24 months

7.4. Key systems

Ethernet frames come in three different variants, depending on the number of recipients of a frame:

- Unicast for the communication of one MAC address with a single other MAC address
- Multicast for the communication of one single MAC address with multiple MAC addresses
- Broadcast for the communication of one single MAC address with all other MAC addresses

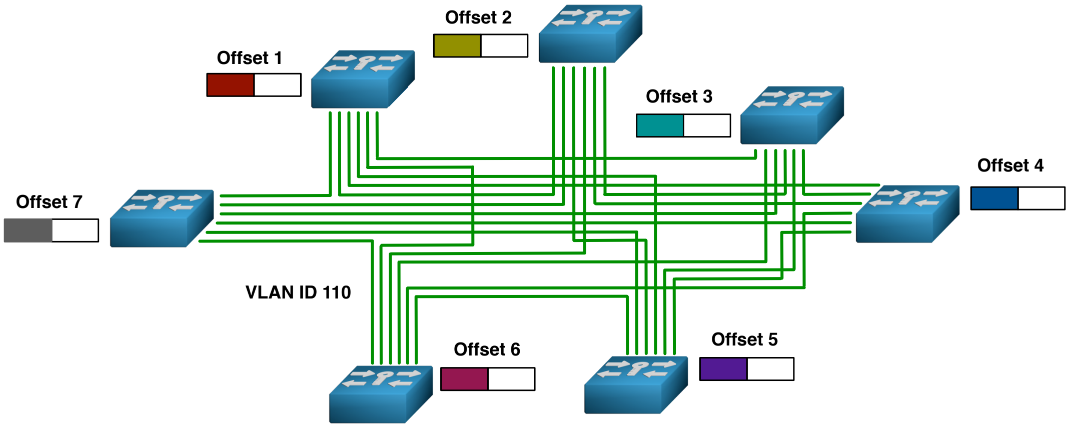
There are different approaches to ensure that next to unicast frames also multicast and broadcast frames are properly encrypted.

In key management there are two main approaches to keys and their assignment: Pairwise keys and group keys.

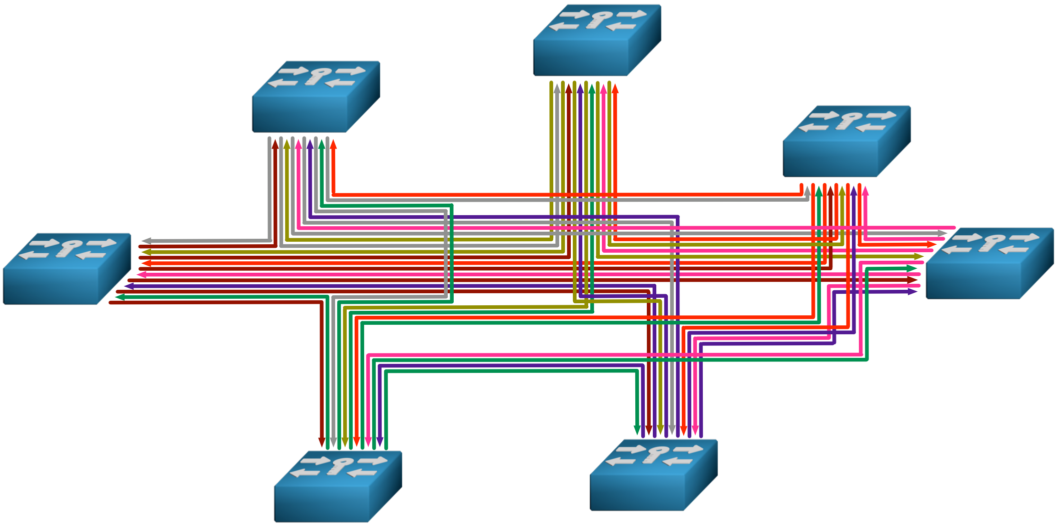
For a pairwise key system a network consists of a multitude of point-to-point connections. Each encryptor is connected with each other encryptor by a point-to-point connection. Traditional pairwise key systems use pairwise unidirectional keys for the connection between two encryptors.

Group key systems are based on group membership and use a different key per group. Group membership can be e.g. based on VLAN-ID, multiple VLAN-IDs, MAC addresses and multicast group membership. The communication of each group is encrypted using the same key for all group members. Each group has its separate key. An encryptor can support multiple groups by using a different key for each group. Group keys can be either bidirectional or unidirectional.

When using bidirectional group keys, all group members use the same group key for the entire network traffic within the same group.



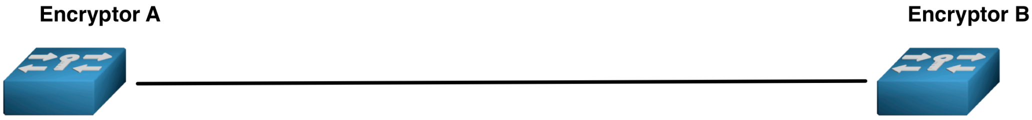
In a unidirectional key system a group key is just used in one for the outgoing network traffic from one encryptor to the other group members. Each group member uses his own group key to encrypt the outgoing network traffic to the group members.



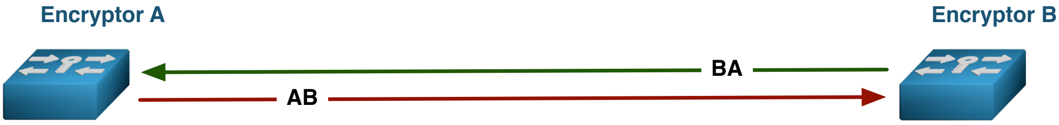
7.5. Pairwise keys

7.5.1. Point-to-point

For a pairwise key system point-to-point connections consist of a link whose endpoints are defined by the two encryptors A and B.

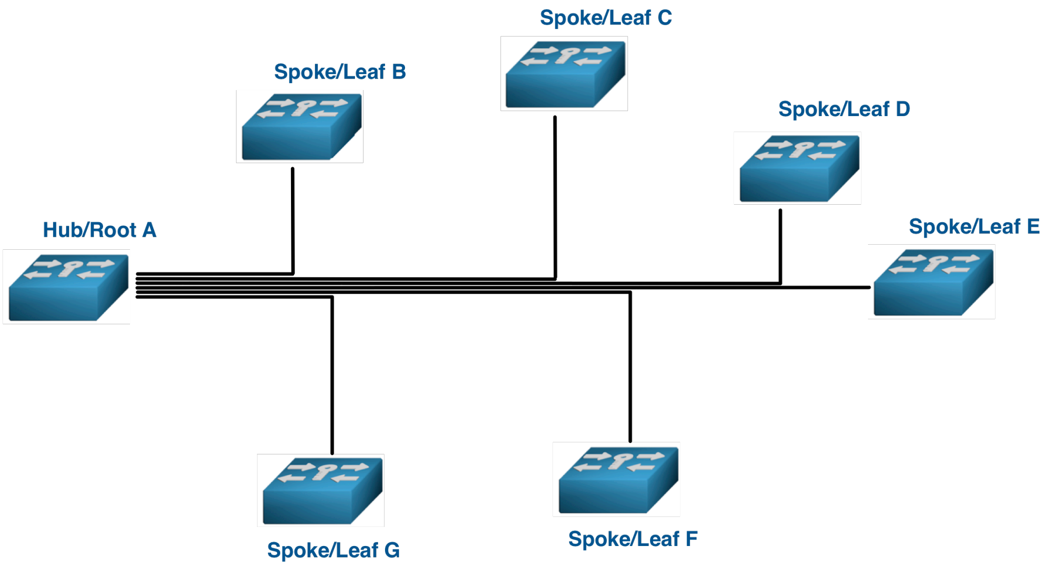


For the encryption of the data flowing from A to B the encryptor uses key AB. In the opposite direction, from B to A, the encryptor uses key BA. This is the most common approach for pure point-to-point scenarios.

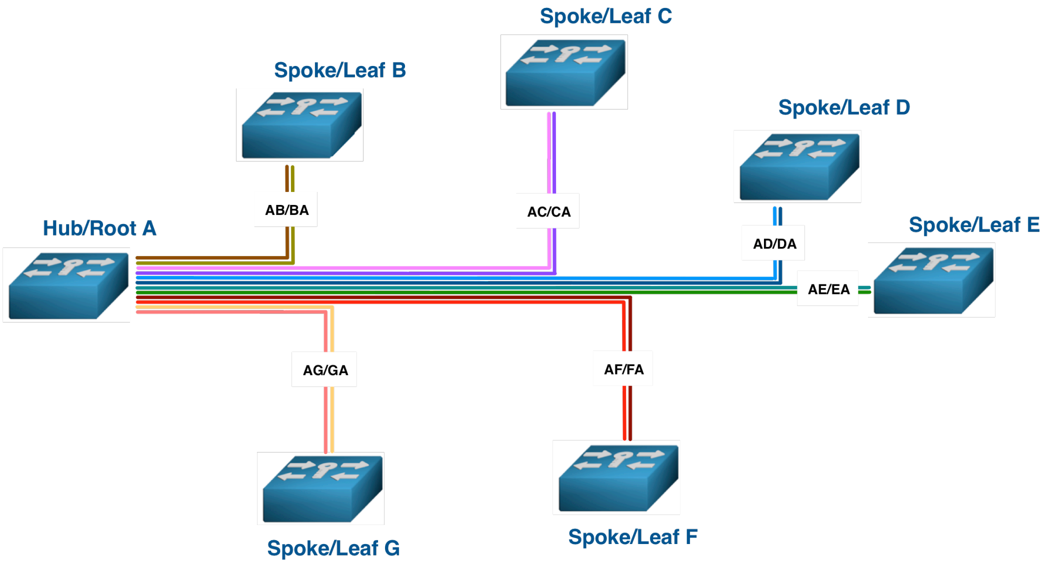


7.5.2. Point-to-multipoint

Point-to-multipoint connections are equivalent to multiple point-to-point connections that have a common starting point but are independent of each other. On one side there is the hub that forms a common starting point and on the other side there are the spokes with their individual endpoints. The communication of the spokes is limited to communication with the hub. There is no communication between the spokes.



For each individual connection between hub and spokes there is a unique key pair.



The assignment of the encryption keys to the individual frames is based on MAC address tables that are maintained by each encryptor. They store all local and remote MAC addresses of the WAN. The encryptor looks up the table to find out behind which other encryptor the destination or sender address is located. If the encryptor is receiving a frame it looks behind which other encryptor the sender address is located. The key is assigned based on the two encryptors involved and the traffic direction. Each direction has its own key.

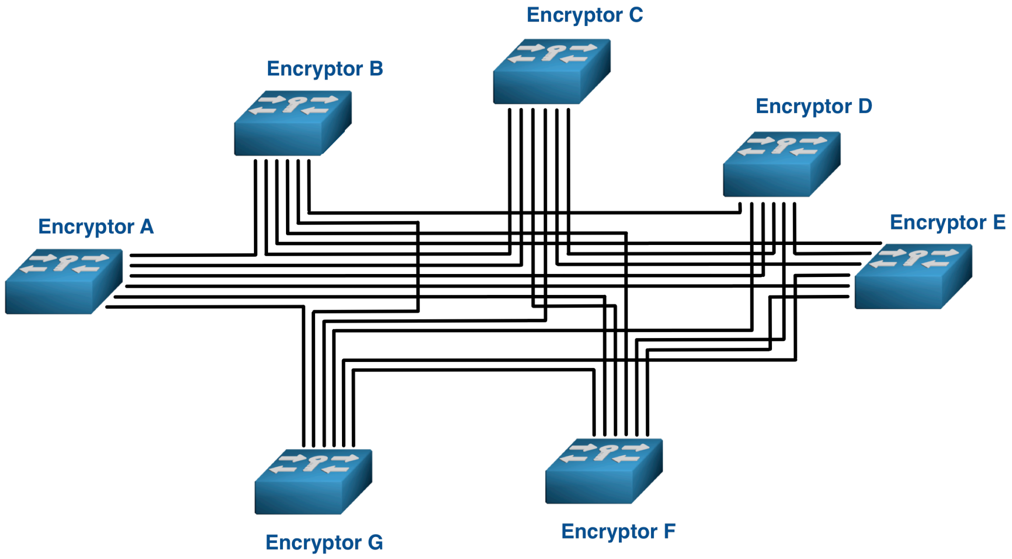
Pairwise key systems are designed for point-to-point connections and function only with unicast frames, as unicast frames are limited to a single destination. Multicast and broadcast frames have a single sender, but multiple destination addresses. This spells trouble for pairwise key systems as there are no pairwise keys for a frame with multiple destinations. By definition a pair is limited to two and that means that there can only be a single destination. E.g. there is no key available for encryptor A to encrypt a multicast frame for two different destination encryptors (B and C) and that would also be available for the destination encryptors to decrypt the frame. Without key there is no encryption.

There are four different solution approaches for this problem: (1) Leave multicast and broadcast frames unencrypted, (2) replicate multicast and broadcast frames for every connection and then treat them as unicast frames, (3) add a specialized key system take care of multicast and broadcast frames, and (4) use a key system that can handle unicast, multicast and broadcast frames.

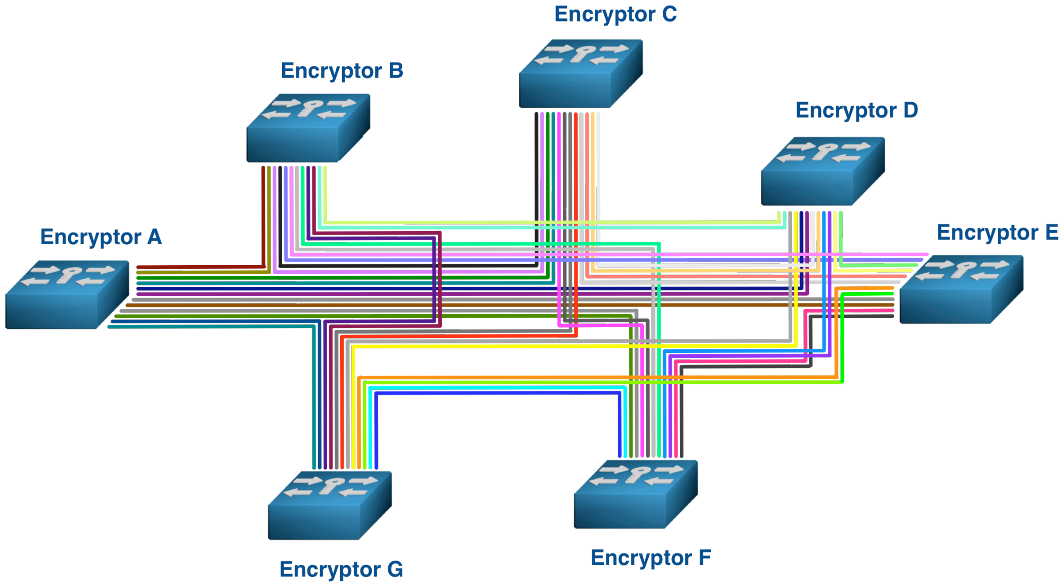
The first approach – exempting multicast and broadcast frames from encryption – leads to an inacceptable result, as there would be no security for multicast and broadcast frames. The second approach – the replication of the multicast and broadcast frames across all connections – leads to a substantial surplus load for the network. This causes either higher operating costs or a reduced network performance. Neither of those two effects can be considered desirable. The third solution – the use of a second key system – results in two different and competing key systems, but solves the problem concerning multicast and broadcast frames. Depending on the frame type the responsibility lies with one key system or the other. A group key system is used for the multicast and broadcast frames, while the pairwise key system handles the unicast frames. The fourth approach is the preferred solution: A group key system that can handle unicast, multicast and broadcast frames.

7.5.3. Multipoint-to-multipoint

Multipoint-to-multipoint allows all connected sites to directly communicate with each other. This scenario is also known under the terms „mesh“ or „any-to-any.



Pairwise key systems also treat multipoint-to-multipoint topologies the same way they treat point-to-point connections. For every connection between two encryptors there is a different key pair. The allocation of the key to the frame is facilitated by the encryptor's MAC tables, which store the local and remote MAC addresses of the WAN. The encryptor consults the table to learn behind which encryptor the sender or destination address is located. This is the information needed to find out between which two encryptors the frame needs to be encrypted and to assign the correct key.



The solution approaches are the same ones as for point-to-multipoint topologies: (1) leave multicast and broadcast frames unencrypted, (2) replicate multicast and broadcast frames across all connections and then treat them as unicast frames, (3) use an additional specialized key system for multicast and broadcast frames, and (4) use a key system that can handle unicast, multicast and broadcast frames. The preferred solution remains the fourth one: The use of a group key system for unicast, multicast and broadcast frames.

7.6. Group Keys

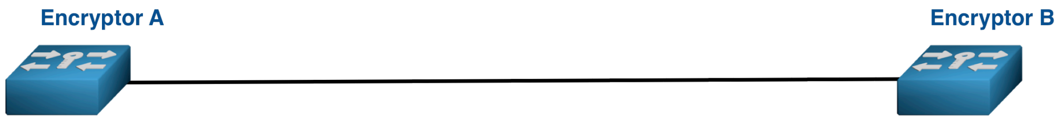
Group keys are based on the principle that for the communication within a defined group the same key is used to encrypt the communication. The membership in one group does not exclude a member from concurrent membership in other groups. For the communication within different groups different keys are used. Keys are unique to a group and separate the groups cryptographically. Exclusion is attained by not providing the required initial secret for a group. Group membership management provides the foundation for the strong cryptographic separation of the different groups, which is a basic requirement for multi-tenancy and for fulfilling certain regulatory guidelines. A group consists of two or more members.

Group key systems are based on group membership and use a different key per group. There are different ways to define a group. A group can e.g. consist of a VLAN or multiple VLANs. In such a definition the group is bidirectional. Each group member uses the same key to encrypt and decrypt frames. A group can also be defined to consist of the recipients of a sender's frames. In such a definition the group is unidirectional. Each encryptor uses a different key to encrypt frames and the recipient uses the key provided by the sender to decrypt the frames coming from that sender. An encryptor can support multiple groups. For each of those groups he uses a different key and in the case of unidirectional groups for each group he uses as many keys as there are members in the group.

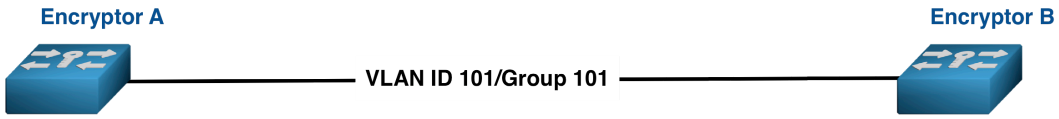
For Ethernet networks it seems to be a natural fit to organize the groups according to VLAN-IDs as corporate networks tend to limit the broadcast domains by using VLANs and use those VLANs also to segment the network. A group key encryption that uses the VLAN-IDs for group membership reinforces that segmentation and establishes a cryptographic separation of the VLANs.

7.6.1. Point-to-Point

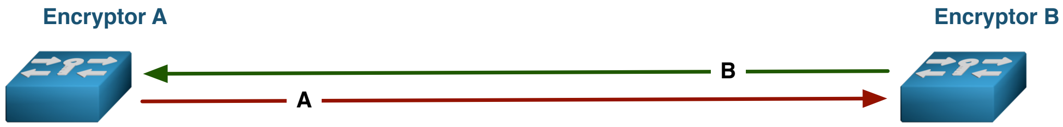
Group key systems treat point-to-point connections either as single group or as two different groups.



A bidirectional key system sees the connection as a single group and uses a single group key.

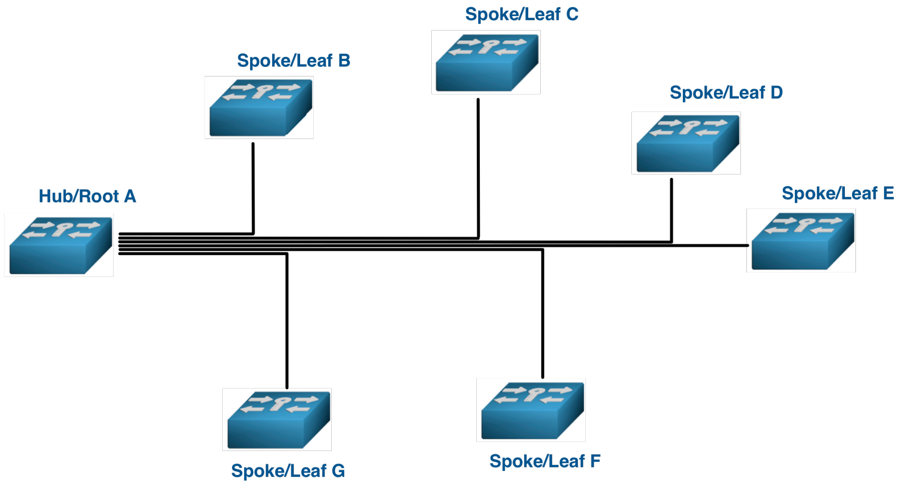


A unidirectional key system sees the connection as two groups and uses one group key for each direction.

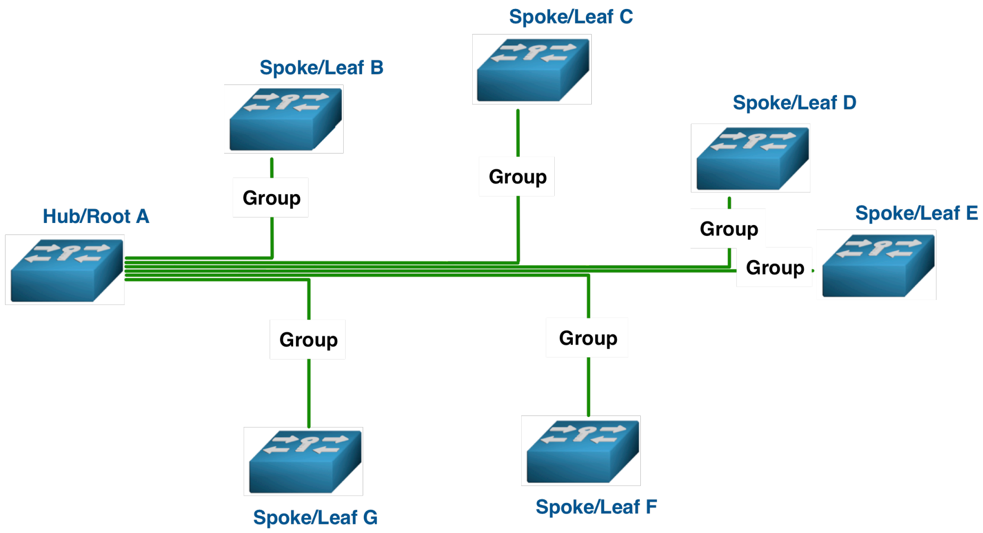


7.6.2. Point-to-Multipoint

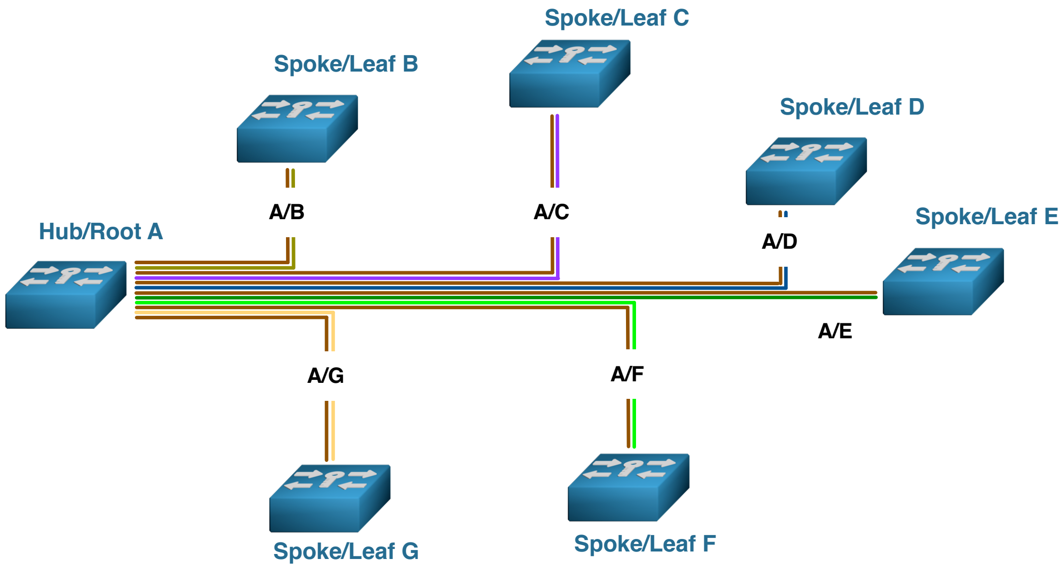
For point-to-multipoint scenarios there are two different approaches. One treats the network as a single group and the other one treats the network as a combination of different groups. Depending on the capabilities of the underlying transport network, the key system will have the full responsibility of keeping the different hub-to-spoke connections separated.



If a bidirectional group key system is used and the entire network is treated as a single group, then a single group key will be used for the encryption of the entire data traffic within the network. All encryptors can decrypt all frames.

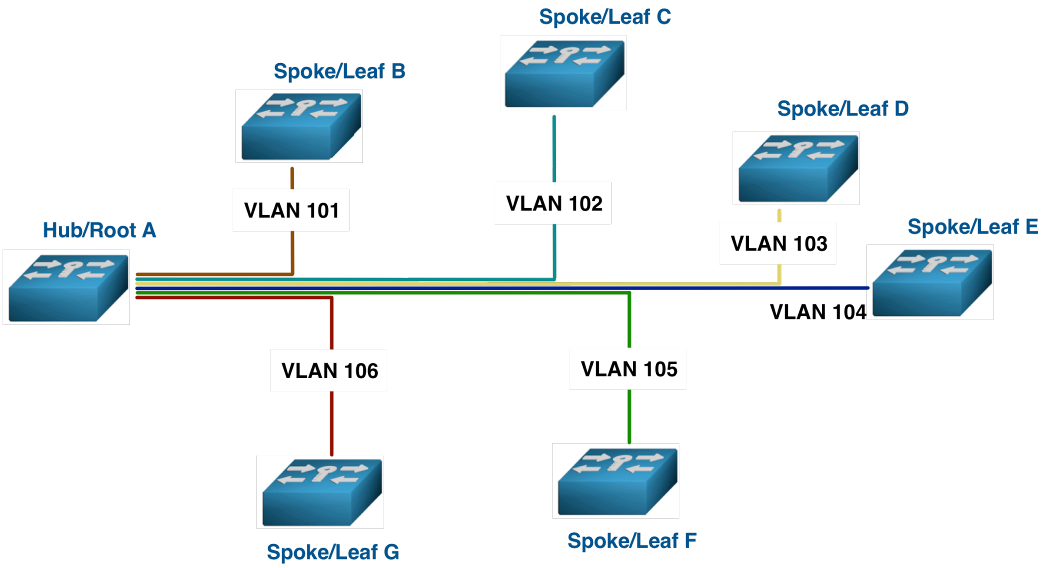


It looks different, if a bidirectional group key system is used. All encryptors can decrypt the frames transmitted by the hub/root, but not the frames transmitted by the other encryptors.

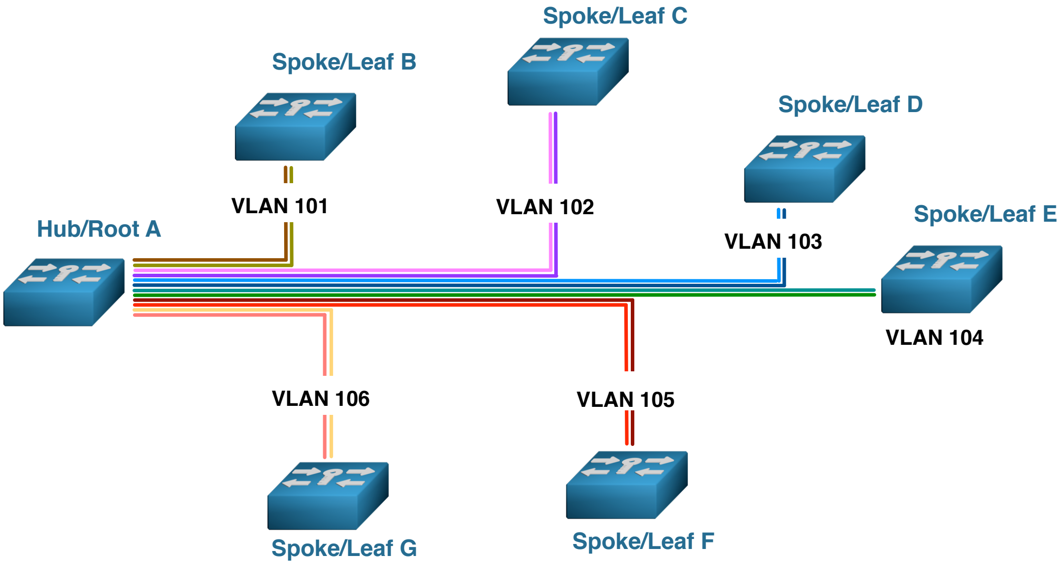


In the context of MANs and WANs group keys are often used to structure the network according to the business needs. The point-to-multipoint network is broken up into single point-to-point connections. Each of them constitutes its own group. The result is that each connection is cryptographically separated from each other connection. Such a separation is also a prerequisite for multi-tenancy.

In a bidirectional group key system the simplest way would be to use a separate VLAN-ID for each connection of the hub/root with another site.

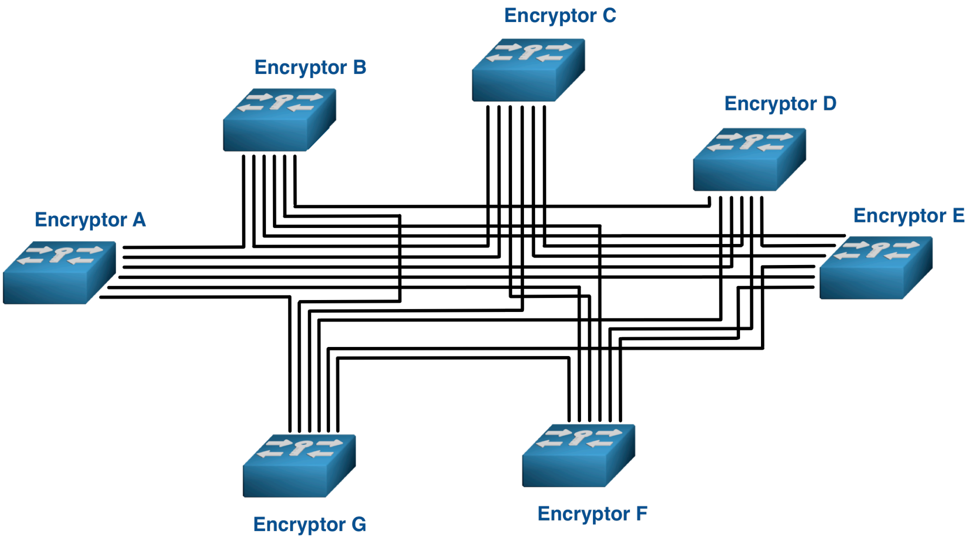


When doing the same with an unidirectional group key system the result shows a separation by VLAN-ID and pairwise keys between the hub/root and the spoke/leafs.



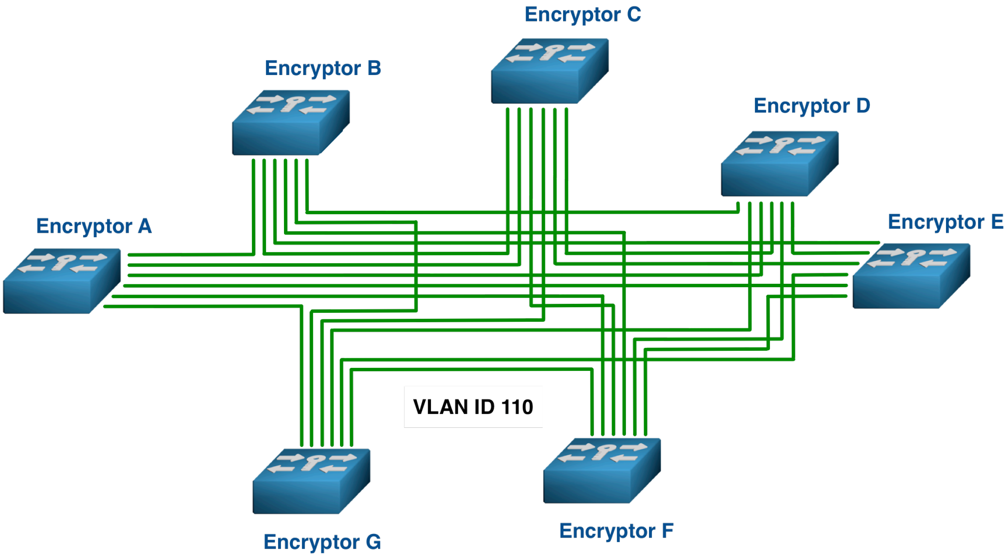
7.6.3. Multipoint-to-Multipoint

In a multipoint-to-multipoint network each point can communicate with all other points.

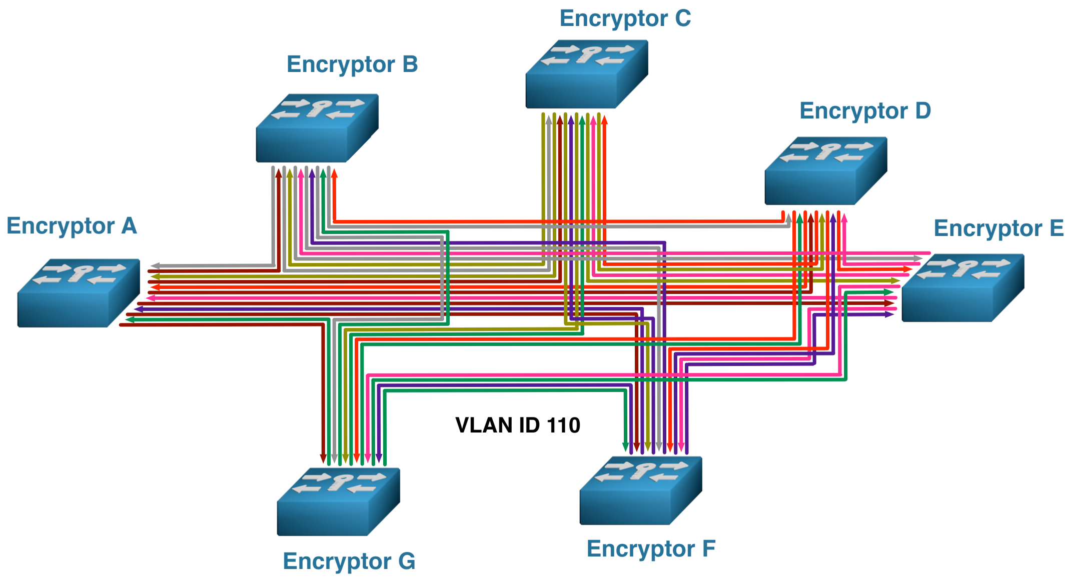


The entire network can be treated as a single group.

In a bidirectional group key system each encryptor uses the same group key to encrypt outgoing traffic. There is a single group key.

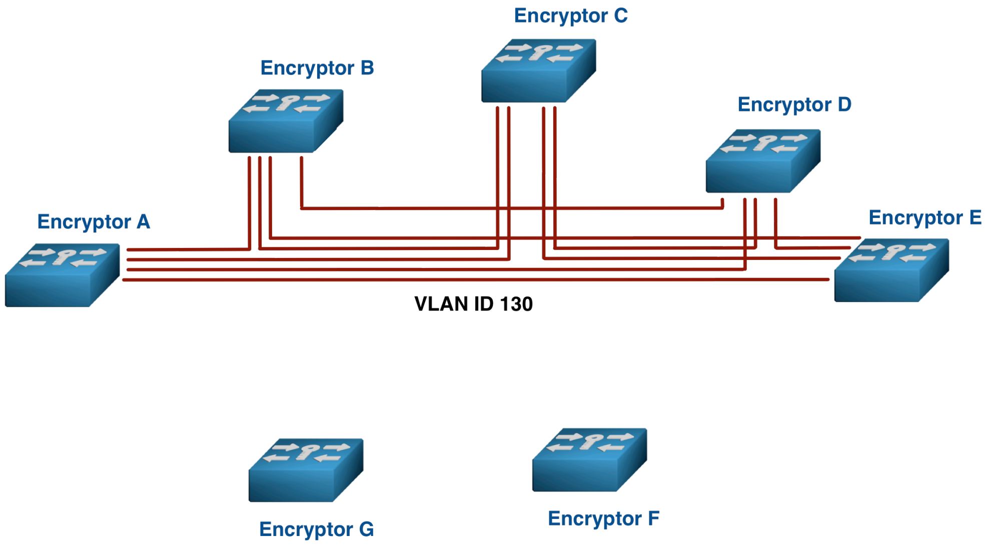


In a unidirectional group key system each encryptor uses its own group key for the outgoing network traffic and the group key of the sending encryptor for the incoming network traffic.

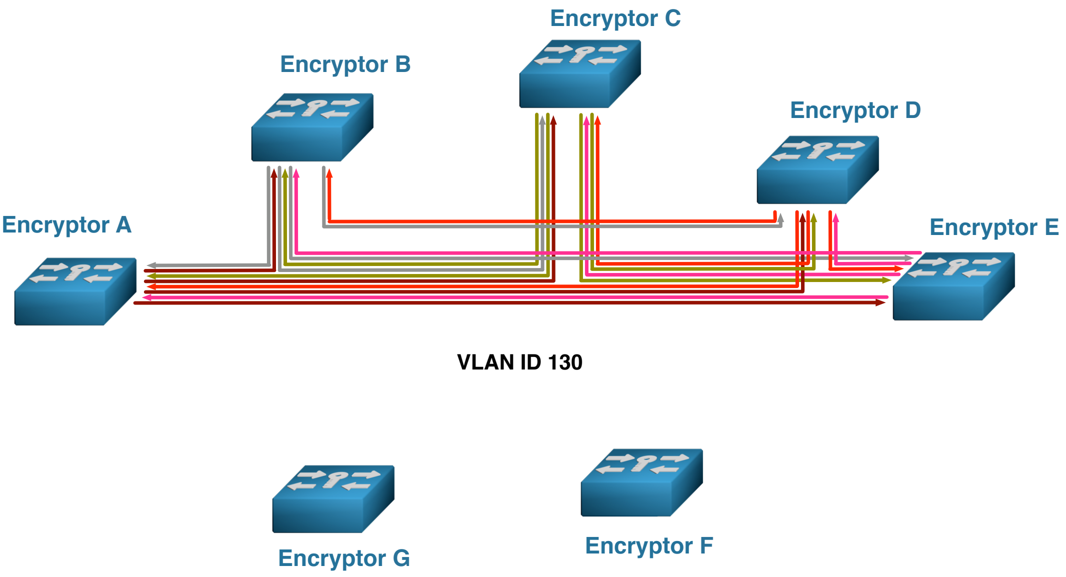


A group can also cover just a subset of the network.

In a bidirectional group key system all encryptors in that group will use the same group key for encrypting outgoing and decrypting incoming frames.

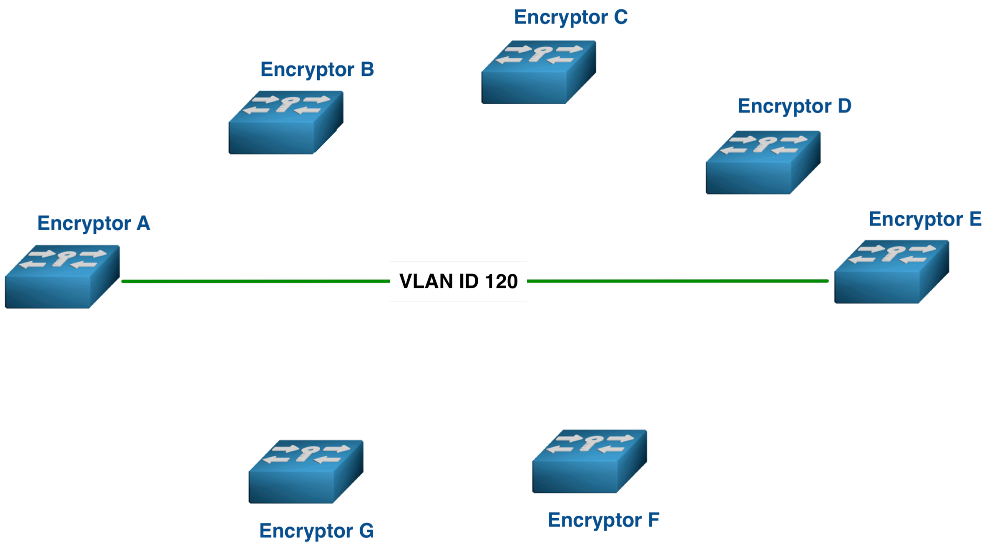


In a unidirectional key system each encryptor in the group will use his group key for encrypting outgoing frames and the individual group keys of the other encryptors for decrypting the incoming traffic.

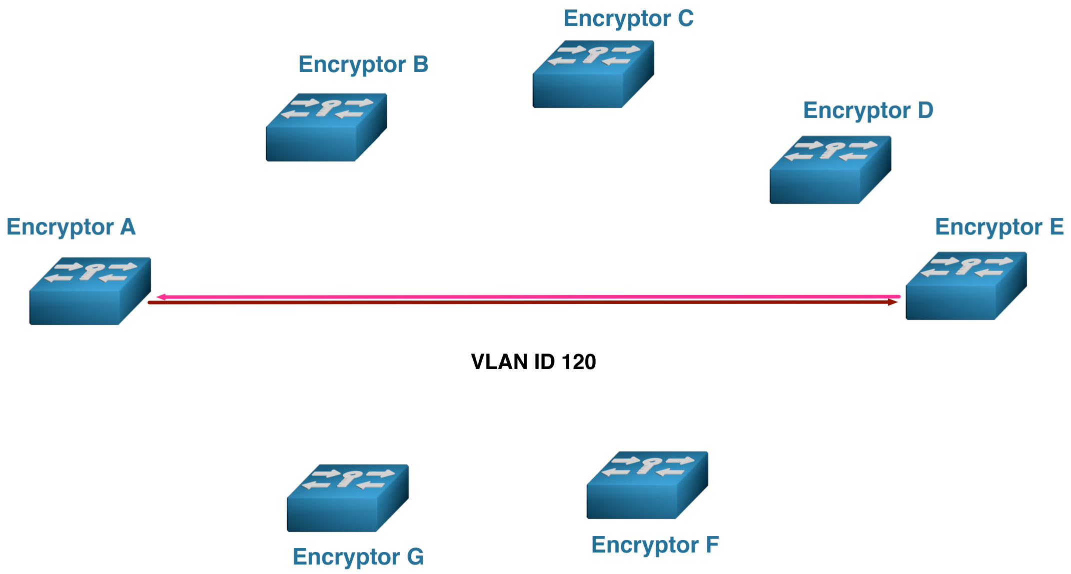


The subset can consist of a single point-to-point connection within the network.

A bidirectional group key system treats this as a single group with one group key.



A unidirectional group key system treats this as two groups with one group key for each direction.



A group key server distributes the group keys to the group members. Per group an additional authentication can take place. Pre-shared secrets or certificates can be used to either authenticate between two group members or authenticate between all group members. The selected authentication scheme decides the mechanism for the distribution of the group keys. If the authentication is pairwise, unicast is used. If the authentication is groupwise, broadcast to all group members can be used. The combination of additional authentication per group and restrictive distribution of initial secrets allows a granular group membership control.

Group key servers in a network can work independently of each other. Group key systems normally use a redundant key server setup or are set up in a distributed way. The key server takes care of providing the right group keys to each encryptor, so that the group members can communicate across sites. Another task of the key server is to ensure that a new key is generated and put in use if there is any change in the membership of the group. With the new key the old data traffic cannot be decrypted and with the old key the new data traffic cannot be decrypted.

In a bidirectional group key system each encryptor can serve as key server and as backup key server. There can be multiple levels of backup group key servers. In large networks often a combination of external and integrated key servers is used to provide extensive standby redundancy.

In a unidirectional group key system normally each encryptor serves as group key server for his group keys. Thus the loss of a network connection of a site compromises only the data exchange of that site with the other sites. Each site constitutes its own failure domain. All other group key servers communicating with that site will have to change their group keys though, due to the change of membership of their groups. External key servers are also an option for unidirectional group key systems, but a distributed approach has distinct advantages.

Protect data center and site-to-site connections from eavesdropping

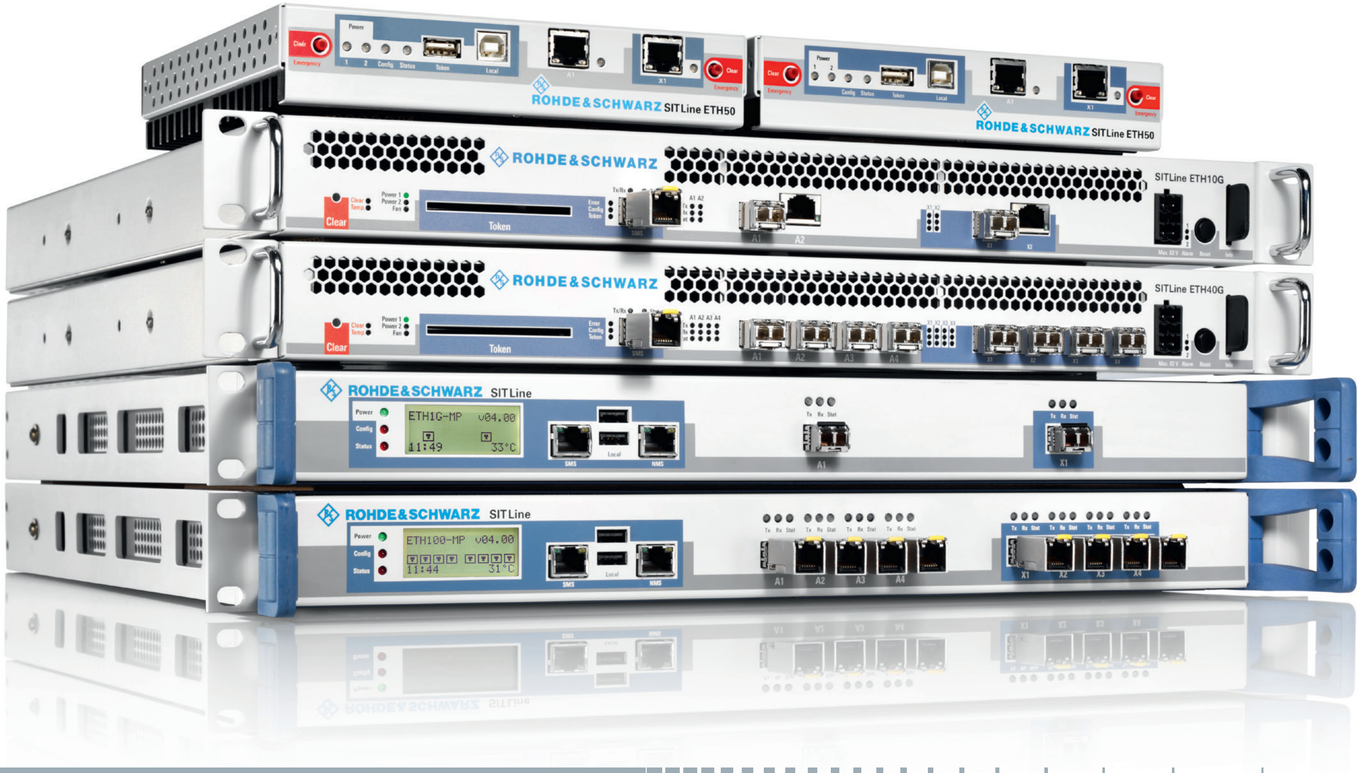
SecurITy
made
in
Germany

When connecting sites and data centers, confidential information leaves your secured and trusted grounds. Big Data, Mobility and Globalization are driving the amount and the value of your data in motion. But optical and electrical lines can easily be tapped.

R&S®SITLine ETH encrypts your data before transmission – highly efficient, real-time, government-approved.

- Ethernet encryptor appliances for outstanding manageability and security
- Up to 40 Gbit/s throughput per device
- Support for network topologies using landline, radio relay and satellite links
- Approved for German and NATO RESTRICTED classification levels

More information:
cybersecurity.rohde-schwarz.com



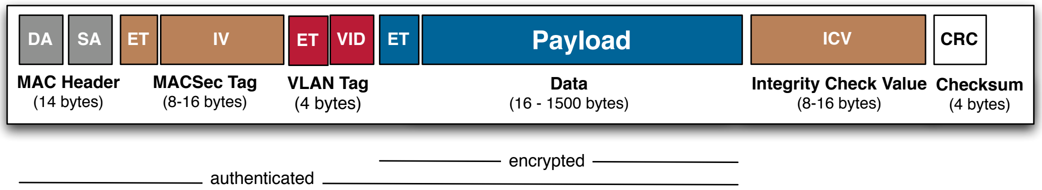
ROHDE&SCHWARZ
Cybersecurity

8. Standards

There is no standard for the encryption of Metro and Carrier Ethernet networks. The only agreement is on the use of authenticated encryption and support for AES-GCM.
However there is MACSec, an IEEE standard for the encryption of local area networks, whose application range has been extended to metro area networks (MAN). Obviously there are fundamental differences between a local area network and a wide area network that have a major impact on functionality and security requirements.

8.1. MACSec/LinkSec

The IEEE has developed and published a standard for the encryption of Ethernet at layer 2 for local area networks (LAN): IEEE 802.1ae (MACSec). After a failed first try at standardization (IEEE 802.1af) authentication and key management for MACSec are standardized by IEEE 802.1X-2010. MACSec uses a special transport mode, which has been optimized and limited for local are networks (LAN). It uses AES-GCM and thus features authenticated encryption (AE) and additional authenticated data (AAD).



MACSec frame

MACSec (also known as LinkSec) is a transport mode encryption and puts the SecTag right after the destination and sender address. It was designed to protect internal local area networks and to be limited to hop-by-hop scenarios. Only devices with MACSec support are able to recognize the format. The original usage scenario consists of MACSec-capable devices that are next to each other on the network. Each MACSec device secures the connection to an adjacent MACSec device and thus protects the link between the two devices. It decrypts the incoming frames, so they can be processed within the device, before encrypting them again and sending them out. Unprotected frames are a requirement for the network device to be able to process a frame within the device. Each active network device between the sender and the destination address counts as hop and will decrypt, process and re-encrypt the frame. This obviously limits its usefulness in most MAN and WAN scenarios. MACSec

Key Agreement (MKA) provides support for point-to-point and point-to-multipoint scenarios and unidirectional group keys.

8.1.1. MACSec, a “standard” for local area networks

MACSec has been specified for usage inside a local area network and should preferably only be used in such an environment. The IEEE is well aware of the limited suitability of MACSec for Metro and Carrier Ethernet scenarios. As it doesn’t fit, there are desperate attempts to make it somehow fit. One of the primary goals of MACSec was to make it so cheap, that it would only have a marginal impact on the product cost of the device it is embedded in. The pre-installed hardware support would then allow vendors to make easy money by selling software licenses. To make it really inexpensive, a lot of compromises were necessary in terms of security, scalability and functionality. There are many endeavors to add needed functionality to MACSec. IEEE and many vendors now also consider basics, which have been part of specialized Carrier Ethernet security appliances for many years, such as definable encryption offsets and definable replay windows, a necessity. Those basics are not part of the standard, though. Some vendors have also made changes to the key management. The resulting lack of interoperability does cause problems. A leading network equipment vendor even offers two incompatible versions of MACSec: MACSec for LAN and MACSec for WAN. A couple of vendors are also pushing for support of end-to-end encryption in MACSec and due to the current lack of support are introducing their own proprietary “enhancements”. MACSec’s hop-by-restrictions can also be circumvented by tunneling MACSec frames over an overlay network. Such a tunneling on the customer increases overhead and latency and is not needed when using a solution that is fit-for-purpose. Vendors using proprietary enhancements continue to use the MACSec Ethertype, despite the MACSec standard not supporting these “enhancements”. MACSec as an interoperable standard has failed, interoperability is more often specific to vendor and device than not.
For Metro and Carrier Ethernet MACSec implemented as integrated solution remains limited to scenarios with low security and functionality requirements. MACSec itself is a viable solution for LANs and infrastructure, but often lacks the security, functionality and flexibility requirements for MANs and WANs.

MACSec is completely based on US security standards, which is definitely an issue for non-US governments, administrations and organizations. The forced use of NIST curves and NIST random number generation are not necessarily a good idea for a security standard. Customers tend to be better off with a solution that supports higher and more trustful standards. If MACSec is implemented as part of a network ASIC on the network interface, additional challenges come into play, as implementations errors and strategically placed backdoors can be used to gain access.

By now, there are incompatibilities even within the published standard. The default cipher for MACSec is AES-GCM with a key length of 128 bit. In 2011 the IEEE published an amendment to the original MACSec specifications, which standardizes the use of AES-GCM with a 256 bit key. Another shortcoming that has been addressed is the limitation of the counter to four bytes. This limitation requires frequent session key changes when used in high-bandwidth environments. A counter length of four bytes is not considered to be future-proof.

Only those parts of MACSec that are supported and used by all network devices exactly the same way are interoperable. Just the addition of 256 bit keys will in most cases require a change of hardware. Each of the needed future extensions will have the same effect. This is an operational nightmare, which eliminates all cost-savings that MACSec promised to bring.

The following links point to descriptions of MACSec and the published standards. They describe the intended usage scenarios and are a confirmation of the issues listed above.

http://en.wikipedia.org/wiki/IEEE_802.1AE
http://download.intel.com/corporate/education/emea/event/af12/files/kahn.pdf
http://en.wikipedia.org/wiki/802.1X

http://standards.ieee.org/getieee802/download/802.1AE-2006.pdf
http://standards.ieee.org/getieee802/download/802.1AEbn-2011.pdf
http://standards.ieee.org/getieee802/download/802.1AEbw-2013.pdf

For decades, there has been a close collaboration between IEEE and NSA. This recently led to the development of specifications (ESS) for a NSA Ethernet encryption appliance, which is based on MACSec, but necessarily interoperable with the published standards. As a dedicated appliance with extended security functionalities it is a high assurance solution, if implemented correctly. IEEE has also started to work on a specification for an encryption appliance. Ethernet Data Encryption (EDE) picks up some of the enhancements of ESS. Depending on the implementation it can be anything between a low assurance and a high assurance solution based on US security standatds. Compared with what is available in terms of layer 2 encryption appliances for years now, neither ESS nor EDE can be considered as industry leading.

http://www.ieee802.org/1/files/public/docs2013/ae-seaman-macsec-hops-0213-v02.pdf
http://www.ieee802.org/1/files/public/docs2013/ae-seaman-ede-0713-v02.pdf
http://cryptome.org/2013/09/nsa-ethernet-security.pdf

https://www.iad.gov/ncsmo/ Unter ESS Team/Documentation
http://www.ieee802.org/1/pages/802.1aecg.html

Specialized appliances tend to be more secure and more flexible in terms of usage scenarios than MACSec appliances. If the objective is to secure a Carrier Ethernet network, the best solution is always the one that fits the bill in terms of security, network support and network behavior. MACSec is not the standard to secure Carrier Ethernet networks and there are many better and more secure solutions available..

9. Evaluation

This document is an introduction to securing Metro and Carrier Ethernet networks. When evaluating different solutions there are many different features and performance characteristics to take into consideration, which are not listed in this document. Among the solutions available on the market there are some that offer all the security and network functionality possible, some that offer a majority of them and some that only cover a subset. Essential for the security is the complete system including its implementation and not single features and characteristics taken out of context.
The combination of SecTag content, key management, key system and support for variable encryption and replay window offsets shows just a limited picture of how a solution actually works.

Next to security, network support and efficiency the suitability for different usage environments, such as managed services, plays a major role.

The following documents provide additional information:

http://www.uebermeister.com/files/inside-it/2014_Evaluation_Guide_Encryptors_Carrier_and_Metro_Ethernet.pdf

http://www.uebermeister.com/files/inside-it/2015_market_overview_Ethernet_encryptors_for_Metro_and_Carrier_Ethernet.pdf

10. Additional information sources for networks and security

Network encryption requires knowledge of networking and encryption technologies. A well-structured and segmented network is the foundation for an efficient protection. It is difficult to find good vendor-independent information. Therefore below a couple of internationally renowned sources that offer excellent information.

10.1. IPSpace

Ivan Pepelnjak is one of the leading network experts and regularly publishes blog posts about network technologies. Security is covered as well. For many subject areas there are also webinars.

http://www.ipspace.net
http://blog.ipspace.net

10.2. Packet Pushers

Podcasts from Greg Ferro and Ethan Banks covering network technologies and network hard- and software. Very technical and very profound.

http://packetpushers.net/

10.3. Postmodernsecurity

Michele Chubirka aka Mrs. Y is a renowned IT security expert and security architect.

http://www.postmodernsecurity.com

10.4. ERNW

Enno Rey and his crew were among the first ones worldwide who looked at Carrier Ethernet security and were able to show how vulnerable transport networks can be. ERNW is also the organizer of the well-known yearly Troopers conference. On their Insinuator blog they cover security issues.

http://www.insinuator.net/

https://www.ernw.de/
https://www.troopers.de/

10.5. Carrier Ethernet Group on LinkedIn

Vishal Sharma is a well-known and widely respected telecom expert. He started the Carrier Ethernet group on LinkedIn and does a great job at moderating 10’000+ expert members.

https://www.linkedin.com/groups/77819

On his company blog he covers data networks and telecom issues:

http://www.metanoia-inc.com/blog/