inside-it.ch

PRÄSENTIERT:

LAYER 2-VERSCHLÜSSLER FÜR METRO UND CARRIER ETHERNET

ETHERNET-VERSCHLÜSSLER FÜR METRO UND CARRIER ETHERNET

DIE EINFÜHRUNG

Version 6.04, 24. April 2016

---

www.uebermeister.com
cjaggi@uebermeister.com

ISBN: 978-1-62018-000-6

Kurzzusammenfassung

Netzwerke sind unsicher
Es stellt sich daher nicht die Frage, ob verschlüsselt werden soll, sondern nur, welcher Ansatz der effizienteste und sicherste ist.
Je tiefer der Layer, desto umfassender die Protokolle, die verschlüsselt werden können und desto effizienter der Schutz und die Verarbeitung. Das gesamte Netzwerk lässt sich nur auf Layer 2 mit guter Netzwerkkompatibilität verschlüsseln. Die Verschlüsselungsschicht sollte durch das Einsatzszenario und die Geschäftserfordernisse bestimmt werden.

Glasfaserleitungen sind unsicher.
Verbindungen über Glasfaserleitungen werden oft als „private" Verbindungen betrachtet, weil die Nutzung bis hinunter auf die Bitübertragungsschicht (Physical Layer) dem Kunden exklusiv zur Verfügung steht. „Privat" in diesem Zusammenhang beschränkt sich auf den exklusiven Gebrauch und sollte nicht mit „sicher" verwechselt werden. Weder Glasfasern noch Wellenlängen verfügen über eingebaute Sicherheit. In Tat und Wahrheit ist es ziemlich einfach Glasfaserleitungen anzuzapfen. Ist die Leitung einmal angezapft, so ist der Zugriff auf den gesamten Netzwerkverkehr vorhanden.

Virtual Private Networks sind ohne Verschlüsselung unsicher
Das Wort „Private" ist kein Synonym für „verschlüsselt" oder „sicher", sondern bedeutet nur, dass das Netzwerk logisch von anderen Netzwerken getrennt ist. Effektiv teilt sich das VPN die Infrastruktur mit vielen anderen VPNs und teilweise auch mit normalem Internet-Verkehr. Die Carrier preisen an, dass virtuelle private Netzwerke fast so sicher sind wie Mietleitungen, vergessen aber dabei zu erwähnen, dass Mietleitungen ungeschützt und nicht im Geringsten abgesichert sind.

Empfohlene Schutzmassnahmen
Dass Daten aus Netzwerken abgegriffen werden können, ist unvermeidbar. Wie mittlerweile allgemein bekannt sein dürfte, braucht es dafür nur den nötigen Willen und genügend Ressourcen. Was Fachleute schon länger wussten, ist mittlerweile auch weithin ins Bewusstsein gerückt: Das Abhören von Netzwerken ist gang und gäbe und der Unterschied zwischen staatlichen und kriminellen Organisationen in dieser Hinsicht gering. In der Wahl der Mittel zeigt man sich wenig wählerisch. Grundlage für einen guten Schutz bilden folgende Massnahmen:

(1) sicheres Verschlüsselungsgerät
(2) sichere Schlüssel,
(3) authentisierte Verschlüsselung,
(4) zusätzliche authentisierte Daten, und
(5) Vernebelung des Netzwerkverkehrs (Traffic Flow Security).

Unterschiedliche Schicht – unterschiedlicher Ansatz
Layer 1-Verschlüssler sind dafür ausgelegt, direkte Verbindungen auf der Bitübertragungsschicht abzusichern. Sie können unterschiedliche Layer 2-Protokolle verschlüsseln, die als

Nutzlast mitgeführt werden. Dazu gehören Ethernet, FibreChannel und InfiniBand. Ethernet-Verschlüssler arbeiten auf Layer 2 und sind dafür ausgelegt Layer 2 und die darüberliegenden Netzwerkschichten abzusichern. Sie sind für die Verschlüsselung von Ethernet und MPLS optimiert. Ein Tunneln von IP, das über Ethernet geführt wird, ist unnötig. Das Verschlüsseln von Metro und Carrier Ethernet-Verbindungen ist auf Layer 2 mit Abstand am effizientesten.
Layer 3-Verschlüssler sind für die Verschlüsselung von IP-Nutzlast mit IPSec ausgelegt. Um das ganze IP-Paket inklusive Header IP-Header zu verschlüsseln, muss es getunnelt werden. Will man mittels IPSec einen Ethernet Frame verschlüsseln, so muss dieser zuerst auf Layer 3 gehoben werden. So wird dieser in IP-Nutzlast transformiert, die dann auf Layer 3 verschlüsselt werden kann.

Die Sicherheitsstufen: High Assurance, Standard Assurance und Low Assurance
Welche Sicherheitsstufe man benötigt, hängt einerseits von der Vertraulichkeit und der Sensitivität der Daten ab und andererseits von der Relevanz eines resistenten Netzwerk. Die höchste Sicherheit bieten Lösungen, die auf sich selbst gestellt sowohl für klassifizierte als auch für sensitive Daten zugelassen sind und deren kompletter Source Code (Software und Hardware) im Detail evaluiert wurde. Für sensitive Daten ist Standard Assurance ausreichend. Low Assurance ist für die Fälle, bei denen nur wenig sensitive Daten über das Netzwerk übertragen werden.

Echte High Assurance und Standard Assurance gibt es nur mit dedizierten Appliances
Ohne sicheres Verschlüsselungsgerät und ohne sichere Schlüssel ist die Sicherheit von vornherein kompromittiert.

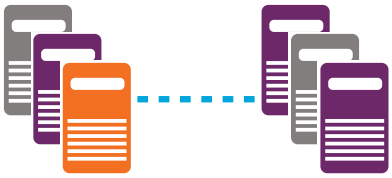
Die Schlüsselverwaltung ist das Kernstück der Netzwerkverschlüsselung
Unzweideutige Authentifizierung der Teilnehmer, sichere Schlüssel, Frame-Format und Verschlüsselungsmodus bilden die Grundlage. Die Schlüsselverwaltung kümmert sich von der Erstellung der Schlüssel über deren Zuweisung bis zu deren Verteilung und Ausserverkehrssetzung. Schlüsselsystem und Schlüsselzuweisung sind ein wichtiger Teilaspekt der Schlüsselverwaltung und massgeblich für die optimale Netzwerkfunktionalität verantwortlich.

Sicherheitszertifikate: Schein oder Sein?
Nicht jedes geprüfte und mit einer FIPS- oder Common Criteria-Zertifizierung ausgestattete Produkt ist sicher. Viele sind es nicht wirklich oder gleich gar nicht. Das sehen die Anbieter von solchen Lösungen natürlich anders und versprechen viel mehr als sie halten können. Für den Schutz von klassifizierten Daten gelten in der Regel strenge Vorgaben. So evaluiert das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) den gesamten Quellcode von Software und Hardware bevor eine Zulassung erteilt wird. In den USA geht das oft mit weniger Aufwand und ist auch entsprechend weniger sicher. Selbst ein sicheres Verschlüsselungsgerät und sichere Schlüssel sind dort des öfteren optional.

So your data is on the move...

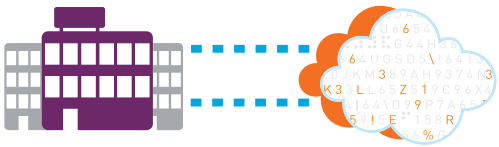
From site to site, or multiple sites...

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

SENETAS.COM

gemalto
security to be free

GEMALTO.COM

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

Inhaltsverzeichnis

1. DAS ABSICHERN VON NETZWERKEN 1
1.1. Unsichere Netzwerke 2
1.2. Ungeschützte Glasfaserleitungen 2
1.3. Ungeschützte Virtual Private Networks (VPN) 3
1.4. Empfohlene Schutzmassnahmen 3
1.4.1. Sicheres Verschlüsselungsgerät 4
1.4.2. Sichere Schlüssel 5
1.4.3. Authentisierte Verschlüsselung (AE) 5
1.4.4. Zusätzlich authentisierte Daten (AAD) 6
1.4.5. Vernebelung des Netzwerkverkehrs (Traffic Flow Security) 7
1.4.6. Absicherung gegen Quantencomputer 7

2. NETZWERKSCHICHTEN UND VERSCHLÜSSELUNG 9
2.1. Unterschiedliche Schicht – Unterschiedlicher Ansatz 9
2.2. OTN-Verschlüsselung auf Layer 1 10
2.3. IPSec-Verschlüsselung auf Layer 3 10
2.3.1. IPSec- Der Standard für Layer 3-Verschlüsselung 11
2.3.2. Das Verwenden von IPSec zur Verschlüsselung von Ethernet 12
2.4. Ethernet-Verschlüsselung auf Layer 2 13
2.4.1. Frame-Modus (Bulk) 14
2.4.2. Transport-Modus 15
2.4.3. Tunnel-Modus 16
2.4.4. SecTags 17
2.5. Die Verschlüsselung von MPLS-Netzwerken 18
2.5.1. Das Verschlüsseln von Ethernet über MPLS/VPLS 20
2.5.2. Das Verschlüsseln von MPLS Interconnect über Carrier Ethernet 21
2.5.3. Das Verschlüsseln von Carrier Ethernet zwischen MPLS-Clouds 22
2.5.4. Das Verwenden von IPSec zum Verschlüsseln von MPLS 24

3. VERSCHLÜSSELUNG: SICHERHEIT, EFFIZIENZ UND OPERATIONELLE ASPEKTE 25
3.1. Sicherheit 25
3.1.1. Netzwerksicherheit 27
3.1.2. Sicheres Verschlüsselungsgerät 27
3.1.3. Sichere Schlüssel 28
3.1.4. Übermittlungssicherheit (TRANSEC) 29
3.2. Effizienz. Leistung und Erweiterbarkeit 29
3.2.1. Sicherheitsoverhead 30
3.2.2. Leistung 31
3.2.3. Erweiterbarkeit/Aktualisierbarkeit 31
3.2.4. Kosten 32
3.3. Operationelle Aspekte 33
3.3.1. Einfaches Installieren und Konfigurieren 33
3.3.2. Betriebsaufwand und Betriebskosten 33
3.3.3. Kosteneinsparungspotential 34

3.4. Sicherheitszertifikate: Schein oder Sein? 33

4. ETHERNET FÜR REGIONALE UND WEITVERKEHRSNETZE: CARRIER ETHERNET 2.0 36
4.1. Carrier Ethernet: Zugang und Topologien..... 36
4.2. E-Line (Punkt-zu-Punkt)..... 36
4.2.1. Ethernet Private Line Service..... 38
4.2.2. Ethernet Wire Service..... 39
4.2.3. Ethernet Virtual Private Service..... 39
4.3. E-Access..... 40
4.4. E-Tree (Punkt-zu-Multipunkt)..... 41
4.4.1. Ethernet Private Tree (EP-Tree)..... 42
4.4.2. Ethernet Virtual Private Tree (EVP-Tree)..... 42
4.5. E-LAN (Multipunkt-zu-Multipunkt, Mesh)..... 43
4.5.1. Ethernet Private LAN (EP-LAN)..... 44
4.5.2. Ethernet Virtual Private LAN (EVP-LAN)..... 45

5. CARRIER ETHERNET: DREISCHICHTENMODELL UND TRANSPORTNETZWERKE 46
4.1. Das Dreischichtenmodell..... 46
4.2. Natives Ethernet und Pseudowires..... 47
4.2.1. Native Ethernet-Formate..... 47
4.2.2. Pseudowires..... 48

6. POSITIONIERUNGSVARIANTEN FÜR CARRIER ETHERNET-VERSCHLÜSSLER.....50
6.1. Hop-by-Hop vs. End-to-End..... 50
6.2. Zwischen Customer Edge (CE) und Provider Edge (PE)..... 51
6.3. Zwischen Customer (C) und Customer Edge (CE)..... 52
6.4. Zwischen Cloud Customer und Customer Edge (CE)..... 52
6.5. Innerhalb einer Cloud..... 52
6.6. Zwischen Provider Edge (PE) und Customer Edge (CE)..... 53
6.7. Zwischen Provider Edge (PE) und Provider (P)..... 53

7. SCHLÜSSELVERWALTUNG, SCHLÜSSELSYSTEME, SCHLÜSSELZUWEISUNG UND NETZWERKTOPOLOGIEN 54
7.1. Schlüsselsysteme..... 54
7.2. Anfangsgeheimnis, Authentifizierung und Signaturprotokoll..... 56
7.3. Schlüsselaustausch..... 57
7.3.1. Symmetrischer Schlüsselaustausch..... 57
7.3.2. Asymmetrischer Schlüsselaustausch..... 57
7.3.3. Austauschfrequenz..... 58
7.4. Schlüsselsysteme..... 59
7.5. Paarweise Schlüssel..... 61
7.5.1. Punkt-zu-Punkt..... 61
7.5.2. Punkt-zu-Multipunkt..... 61
7.5.3. Multipunkt-zu-Multipunkt..... 63
7.6. Gruppenschlüssel..... 64
7.6.1. Punkt-zu-Punkt..... 64
7.6.2. Punkt-zu-Multipunkt..... 65
7.6.8. Multipunkt-zu-Multipunkt..... 66

8. STANDARDS 72
8.1. MACSec/LinkSec 72
8.1.1. MACSec, der „Standard“ für lokale Netzwerke..... 73

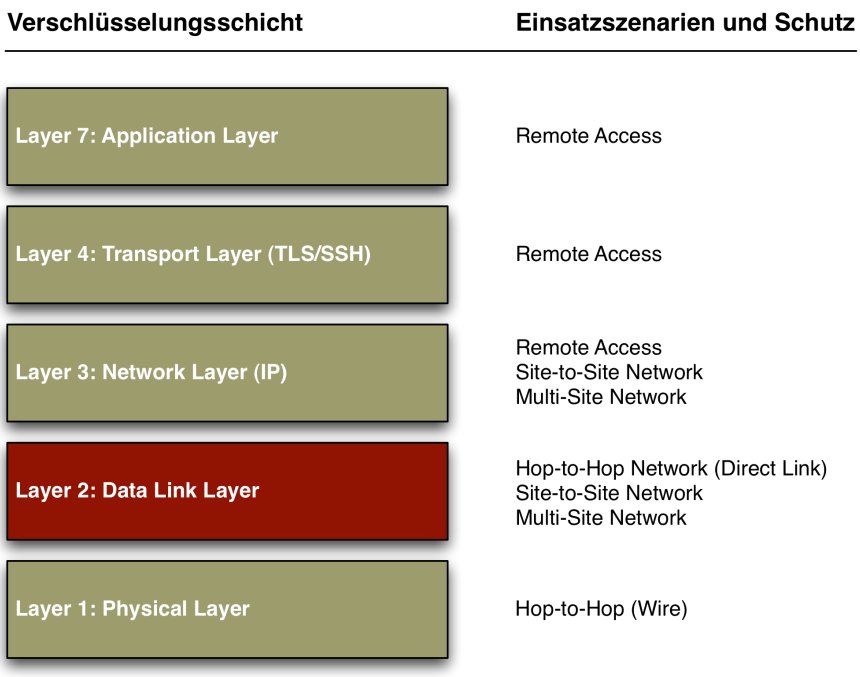
9. EVALUATION 75

10. ZUSÄTZLICHE INFORMATIONSQUELLEN ZU NETZWERKEN UND SICHERHEIT 76
10.1. IPSpace 76
10.2. Packet Pushers 76
10.3. Postmodern Security 76
10.4. ERNW 76
10.5. Carrier Ethernet-Gruppe auf LinkedIn 77

1. Das Absichern von Netzwerken

1.1. Unsichere Netzwerke

Wieso absichern? Netzwerke sind unsicher. Das gilt für optische Netzwerke genauso wie für alle anderen drahtgebundenen und drahtlosen Netzwerke. Die nötigen Anleitungen zum Abhören lassen sich problemlos per Suche im Internet finden und auch die nötigen Utensilien sind ohne grösseren Aufwand beschaffbar. Ohne Verschlüsselung sind Netzwerke über öffentlichen Grund nicht sicher. Es stellt sich daher nicht die Frage, ob verschlüsselt werden soll, sondern nur, welcher Ansatz der effizienteste und sicherste ist.
Je tiefer der Layer, desto umfassender die Protokolle, die verschlüsselt werden können und desto effizienter der Schutz und die Verarbeitung. Das gesamte Netzwerk lässt sich nur auf Layer 2 mit guter Netzwerkkompatibilität verschlüsseln. Die Verschlüsselung des Bitstreams auf Layer 1 reduziert die Netzwerkkompatibilität auf ein Minimum und kommt in der Regel nur bei direkten fiberoptischen Punkt-zu-Punkt-Verbindungen (Dark Fiber oder xWDM)) zum Einsatz. Komplexität, Overhead und Kosten der Verschlüsselung auf den verschiedenen Layer unterschieden sich stark. Es ist daher sinnvoll, nicht alles über den gleichen Leisten zu schlagen, sondern je nach Netzwerk und Einsatzszenario den bestgeeigneten Layer für die Verschlüsselung zu wählen.

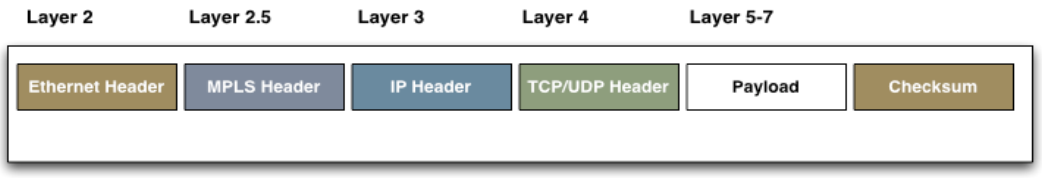


*TLS und SSH bauen zwar auf Layer 4 (TCP) auf, sind aber Layer 7-Protokolle

Das obenstehende Diagramm zeigt die Netzwerk- und Verschlüsselungsschichten und deren bevorzugten Verwendungsbereich. Es ist zwar möglich mittels eines Tunnels tiefere Netzwerkschichten – mit Ausnahme von Layer 1 – als

Nutzlast über eine höhere Netzwerkschicht zu führen und dort als Nutzlast zu verschlüsseln, doch geht das zu Lasten der Netzwerk- und Sicherheitseffizienz Das Tunneln über eine höhere Netzwerkschicht macht nur dann Sinn, wenn das Netzwerk auf der höheren Netzwerkschicht terminiert wird. So muss beispielsweise ein Layer 3-Verschlüssler für das Verschlüsseln von Daten von der Sicherungsschicht (Data Link Layer) diese einzeln zuerst auf die Netzwerkschicht hochheben, um sie dann verschlüsseln zu können. Der Grund liegt in der Beschränkung der Layer 3-Verschlüssler auf Layer 3: Sie können nur IP-Nutzlast verschlüsseln und deshalb muss alles, das verschlüsselt werden soll, IP-Nutzlast sein. Aus diesem Grund muss ein Layer 3-Verschlüssler die Daten von der Sicherungsschicht zuerst in Layer 3-Nutzlast umwandeln, was kontinuierliche Klimmzüge beinhaltet.

Schaut man die unterschiedlichen Layer aus Ethernet-Perspektive an, so folgen auf den Layer 2-Header die Layer 2.5 bis 7. Den Abschluss bildet die Checksumme.



Auf Layer 2 lassen sich Layer 2 und alle Schichten oberhalb davon verschlüsseln, ohne dass ein ressourcenhungriger Mechanismus wie Tunneln oder Einkapselung nötig ist.

1.2. Ungeschützte Glasfaserleitungen

Verbindungen über Glasfaserleitungen werden oft als „private“ Verbindungen betrachtet, weil die Nutzung bis hinunter auf die Bitübertragungsschicht (Physical Layer) dem Kunden exklusiv zur Verfügung steht. „Privat“ in diesem Zusammenhang beschränkt sich auf den exklusiven Gebrauch und sollte nicht mit „sicher“ verwechselt werden. Weder Glasfasern noch Wellenlängen verfügen über eingebaute Sicherheit. In Tat und Wahrheit ist es ziemlich einfach Glasfaserleitungen anzuzapfen. Ist die Leitung einmal angezapft, so ist der Zugriff auf den gesamten Netzwerkverkehr vorhanden. Das freut die einen und ärgert die anderen. Das probate Mittel dagegen: Verschlüsselung zwecks Absicherung von Netzwerk und Daten. Glasfaserleitungen schützt man am besten entweder auf der Bitübertragungsschicht (Physical Layer) oder auf der Sicherungsschicht (Data Link Layer). Die Verschlüsselung auf Layer 1 erlaubt die Absicherungen mehrer verschiedener Layer-2-Protokolle, wie Ethernet, FibreChannel und InfiniBand, während die Verschlüsselung auf Layer 2 ein einzelnes Layer 2-Protokoll schützt. In beiden Fällen ist das am weitesten verbreitete obere

Bandbreitenlimit zur Zeit 10 Gb/sec, so dass die Verschlüsselung einer 10G Ethernet Punkt-zu-Punkt-Verbindung über eine optische Verbindung sowohl auf Layer 2 wie auch auf Layer 1 effizient erfolgen kann. Es gibt mittlerweile schon für beide Layer erste Installationen mit höheren Bandbreiten und auch erste Verschlüsselungslösungen, die diese Bandbreiten unterstützen. Dabei handelt es sich um Bandbreiten von 40 Gb/sec respektive 100 Gb/sec.

1.3. Ungeschützte Virtual Private Networks (VPN)

Ohne Verschlüsselung sind Virtual Private Networks unsicher. Das Wort „Private" ist kein Synonym für „verschlüsselt" oder „sicher", sondern bedeutet nur, dass das Netzwerk logisch von anderen Netzwerken getrennt ist. Effektiv teilt sich das VPN die Infrastruktur mit vielen anderen VPNs und teilweise auch mit normalem Internet-Verkehr. Die Carrier preisen an, dass virtuelle private Netzwerke fast so sicher sind wie Mietleitungen, vergessen aber dabei zu erwähnen, dass Mietleitungen ungeschützt und nicht im Geringsten abgesichert sind.

Nur SSH- und SSL-VPNs kommen aufgrund des Transports über normale öffentliche IP-Netzwerke mit eingebauter und aktiver Verschlüsselung. Aufgrund von Fehlern in der Implementierung der Verschlüsselung und Verletzung elementarster Sicherheitsgrundlagen sind viele dieser Netzwerke aber einfach angreifbar[1][2][3][4][5][6].

IP-VPNs sind nicht zwangsläufig verschlüsselt, selbst wenn IPSec angewendet wird. IPSec kennt zwei Modi: Beim einen wird nur authentisiert und beim anderen wird authentisiert und verschlüsselt. In Bezug auf Schlüsselsysteme deckt der IPSec-Standard nur Punkt-zu-Punkt-Verbindungen ab. Für Multipunkt-Verbindungen gibt es hingegen keinen Standard. MPLS befindet sich auf Layer 2.5 und verfügt über keinen eigene Verschlüsselungsfunktionalität. Es muss deshalb von Layer 2 aus oder auf Layer 3 verschlüsselt werden. Ebenfalls keinen Standard, dafür geeignete Lösungen, gibt es für Ethernet-VPNs auf Layer 2 und OTN auf Layer 1.

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

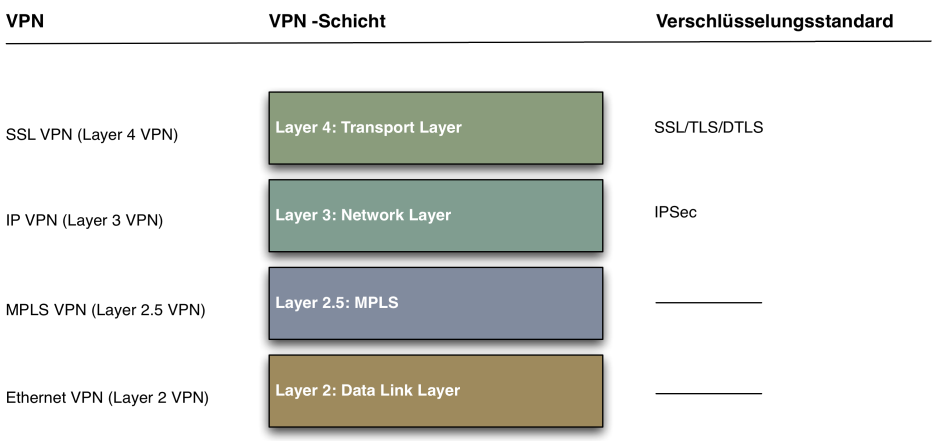
[2] http://www.securityweek.com/default-ssh-keys-expose-ciscos-virtual-security-appliances

[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



Um die Daten und das Netzwerk zu schützen, gibt es keinen anderen Weg als das VPN zu verschlüsseln. Als zusätzlicher Bonus winkt dafür nebst dem Schutz die Compliance mit wichtigen Vorschriften. Für ein Ethernet-VPN braucht es Ethernet-Verschlüssler, die das Netzwerk auf Layer 2 verschlüsseln. Ein MPLS-VPN liegt auf einer Zwischenschicht zwischen Layer 2 und Layer 3. Die Verschlüsselung eines MPLS-Netzwerks kann entweder mittels eines Ethernet-Verschlüsslers, der MPLS erkennt, auf Layer 2 verschlüsselt werden, mit einem IPSec-Verschlüssler auf Layer 3 oder mit einem Layer 2-Verschlüssler, der sowohl Ethernet als auch Ethernet über IP (EoIP) kann, auf Layer 2 und 3.

1.4. Empfohlene Schutzmassnahmen

Dass Daten aus Netzwerken abgegriffen werden können, ist unvermeidbar. Wie mittlerweile allgemein bekannt sein dürfte, braucht es dafür nur den nötigen Willen und genügend Ressourcen. Was Fachleute schon länger wussten, ist mittlerweile allgemein bekannt: Das Abhören von Netzwerken ist gang und gäbe und der Unterschied zwischen staatlichen und kriminellen Organisationen in dieser Hinsicht ist gering. In der Wahl der Mittel zeigt man sich wenig wählerisch. Nebst dem „passiven“ Mithören unerwünschter Dritter gibt es zudem eine Vielzahl an Möglichkeiten, Netzwerke aktiv anzugreifen. Dies lässt sich mit den geeigneten Mitteln unterbinden.

1.4.1. Sicheres Verschlüsselungsgerät

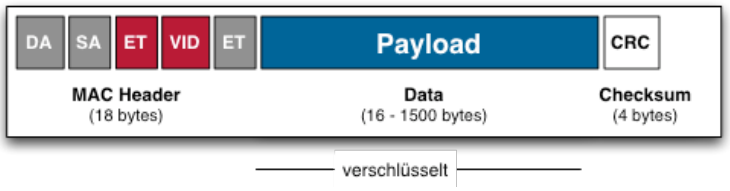
Sicherheit braucht Schutz nach innen und nach aussen. Ist das Verschlüsselungsgerät nicht komplett abgesichert, so ist es ein optimales Einfallstor. Am einfachsten ist das Abhören nämlich, wenn man Zugriff auf das Verschlüsselungsgerät und die Schlüssel erlangt.

1.4.2. Sichere Schlüssel

Unsichere Schlüssel sind ein einfacher Weg, um Netzwerkverkehr abhören zu können. Sichere Schlüssel fangen mit der Erstellung des Schlüssels mittels echter Zufallszahlen und der Länge des Schlüssels an, und benötigen auch eine sichere Lagerung und Verteilung des Schlüssels. Schlüssellängen unter 256-Bit sind kritisch. Von vornherein geschwächte Schlüssel führen zu einer dermassen grossen Verringerung der Sicherheit, dass diese nur noch äusserst bedingt gegeben ist. Oft haben dabei staatliche Organisationen und Institutionen ihre Hände im Spiel[7]. Solche geschwächte Verfahren propagieren sich durch die Verwendung in Programmier-Bibliotheken weiter und finden sich in tausenden Programmen wieder.

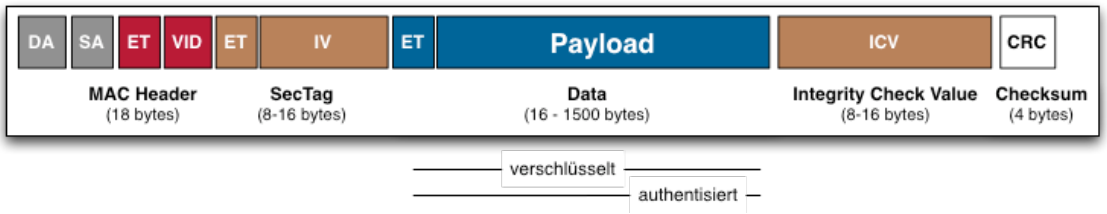
1.4.3. Authentisierte Verschlüsselung (AE)

Authentisierte Verschlüsselung kombiniert die Verschlüsselung der Nutzlast mit einem Initialisierungsvektor vor, und einem Message Authentication Code (MAC) hinter der verschlüsselten Nutzlast. Letzterer ist für die Authentisierung und den Integritätsschutz verantwortlich und basiert auf einem vereinbarten geheimen Schlüssel und der übermittelten Nachricht. Der Sender erstellt aus der zu übermittelnden Nachricht einen MAC. Dies erfolgt mittels eines MAC-Algorithmus, der wiederum den geheimen Schlüssel verwendet. Der MAC wird dem zu übermittelnden Frame als Tag hinter der Nutzlast hinzugefügt. Der Empfänger verwendet den selben geheimen Schlüssel und den gleichen MAC-Algorithmus für die Berechnung eines MAC für die erhaltene Nachricht. Der Vergleich des selbst berechneten MAC mit dem erhaltenen MAC zeigt auf, ob die Nachricht von einem authentisierten Sender stammt und auf dem Transport nicht kompromittiert wurde. Die gewährte Sicherheit ist abhängig von der Länge des MAC, der auch als Integrity Check Value (ICV) bezeichnet wird. Eine Länge von 16 Bytes bietet die nötige Sicherheit.



Verschlüsselung ohne Authentisierung

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



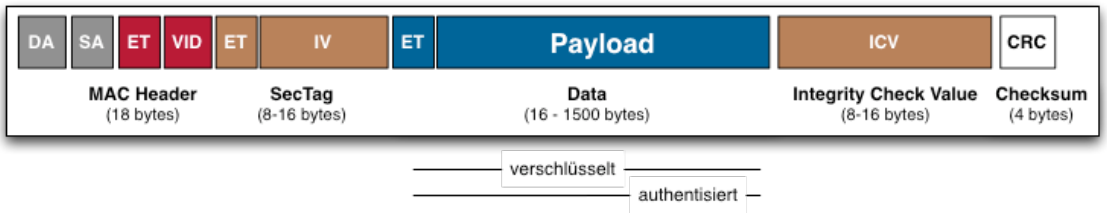
Verschlüsselung mit Authentisierung

Der Initialisierungsvektor (IV) stellt zusammen mit einem fortlaufenden Counter sicher, dass eine Nachricht nur ein Mal gesendet werden kann. Der Zähler (Counter) etabliert auch die einzuhaltende Reihenfolge der Frames. Pro verwendetem Schlüssel kommt ein Zählerstand nur einmal vor. So werden Replay-Attacken und andere Angriffe abgewehrt, die auf dem Einspeisen von Frames in das Netzwerk basieren. Der Initialisierungsvektor stellt sicher, dass die Kombination von Initialisierungsvektor und Schlüssel einmalig ist. Da Carrier Ethernet meist über Transportnetzwerke geführt ist, kann es durchaus dazu kommen, dass beim Transport die Reihenfolge nicht genau eingehalten wird. Deshalb braucht es die Möglichkeit festzulegen, um wie viel sich die Reihenfolge maximal verschieben darf.

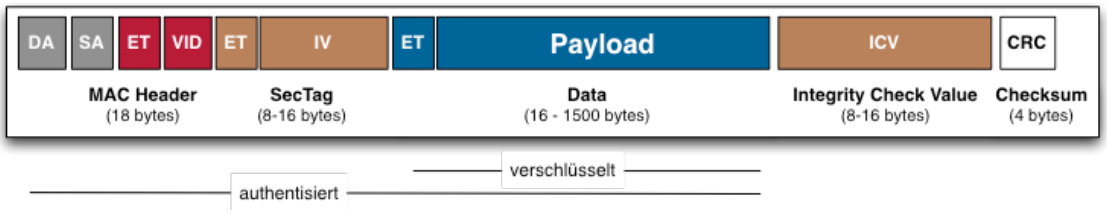
http://en.wikipedia.org/wiki/Authenticated_encryption
http://en.wikipedia.org/wiki/Message_authentication_codes
http://de.wikipedia.org/wiki/Message_Authentication_Code

1.4.4. Zusätzliche authentisierte Daten (AAD)

Nachrichten bestehen aus der Nutzlast und dem vorgelagerten Header. Aus Sicherheitsgründen sollte deshalb nicht nur die Nutzlast zu authentisieren, sondern auch sämtliche Bereiche des Headers, die sich auf dem Transport nicht ändern sollen. Je nach Frame-Format kann das der ganze Header sein oder nur ein Teilbereich. Diese Funktionalität ist unter dem Begriff „Additional Authenticated Data“ (AAD) bekannt. In Kombination mit der authentisierten Verschlüsselung wird der Begriff AEAD (Authenticated Encryption with Associated Data“ verwendet.



Frame mit authentisierter und verschlüsselter Nutzlast



Frame mit authentisierter und verschlüsselter Nutzlast und AAD

1.4.5. Vernebelung des Netzwerkverkehrs (Traffic Flow Security)

Das Abhören eines Netzwerks gibt Aufschluss über die Netzwerknutzung. Das ermittelte Nutzungsmusters macht das Bewegungsprofil des Netzwerkverkehrs ersichtlich und gibt Anhaltspunkte, was wann auf dem Netzwerk abläuft[8]. Mittels Netzwerkverkehrsanalyse lassen sich auch direkte Ruckschlüsse auf den übertragenen Klartext (Plain Text) ziehen.
Dem kann man entgegenwirken, indem man die Netzwerknutzung vernebelt. Das einfache Erzeugen und Übermitteln von belanglosem Zusatzverkehr ist dabei nicht genügend, da immer noch genug wertvolle Rückschlüsse für die Nutzungsanalyse gezogen werden können. Gute Traffic Flow Security benötigt die Kombination von gruppierten Frames und belanglosem Zusatzverkehr. So wird sowohl die Grösse der übermittelten Frames als auch der effektive Netzwerkverkehr vernebelt.

1.4.6. Absicherung gegen Quantencomputer

Schon seit Jahren droht das Damoklesschwert des Einsatzes von Quantencomputern zum Knacken der Verschlüsselung. Hauptangriffspunkte bilden der asymmetrische Schlüsselaustausch und die Verschlüsselung mit zu kurzen Schlüsseln. Um dem wirksam entgegenzuwirken braucht es aber weder eine quantenbasierte Schlüsselerstellung noch eine quantenbasierte Schlüsselverteilung. Man kann solche Technologien verwenden, muss aber nicht. Es genügt die Kombination von asymmetrischem mit symmetrischem Schlüsselaustausch und einer Schlüssellänge für symmetrische Schlüssel von 256 Bit. Als von Quantencomputern potentiell angreifbar gelten die aktuellen asymmetrischen Schlüsselaustauschverfahren wie RSA und Diffie-Hellman. Bei statischen Netzwerkverbindungen besteht die Möglichkeit, den asymmetrischen Schlüsselaustausch mittels etablierter Methoden wie AES-MAC symmetrisch zu verschlüsseln. Dabei wird ein 256 Bit AES-Schlüssel zur Signatur der Teilschlüssel verwendet.[9] Bei der Verwendung von AES (Advanced Encryption Standard) vermag der Einsatz eines Quantencomputers die relative Sicherheit nur etwa auf die eines 128 Bit-Schlüssels zu reduzieren. Selbst ein Quantencomputer ist da noch unpraktikabel lange Zeit mit dem

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

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

da noch unpraktikabel lange Zeit mit dem Versuch beschäftigt, den Schlüssel zu knacken.
Wie das in 5-10 Jahren aussehen wird, weiss heute niemand. Man darf aber getrost davon ausgehen, dass die Absicherungsmöglichkeiten mit den Angriffsmöglichkeiten Schritt halten. Insbesondere wird seit langem an Post-Quantum-Algorithmen gearbeitet[10]. Es ist jedoch sowohl heute wie auch in Zukunft einfacher und erfolgsversprechender direkt die Endgeräte anzugreifen.

[10] https://de.wikipedia.org/wiki/Post-Quanten-Kryptographie


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. Netzwerkschichten und Verschlüsselung

2.1. Unterschiedliche Schicht – unterschiedlicher Ansatz

Layer 1-Verschlüssler sind dafür ausgelegt, direkte Verbindungen auf der Bitübertragungsschicht zu verschlüsseln. Gängiger Layer 1-Standard ist heutzutage Optical Transport Network (OTN), das bereits grossteils SONET/SDH abgelöst hat und SONET/SDH-Frames transportieren kann. Layer 1-Verschlüssler können unterschiedliche Layer 2-Protokolle verschlüsseln, die als Nutzlast mitgeführt werden. Dazu gehören Ethernet, FibreChannel und InfiniBand.
Ethernet-Verschlüssler arbeiten auf Layer 2 und sind dafür ausgelegt Layer 2 und die darüberliegenden Netzwerkschichten abzusichern. Sie sind für die Verschlüsselung von Ethernet und MPLS optimiert. Ein Tunneln von IP oder MPLS, die über Ethernet geführt werden, ist unnötig. Verschlüsselung ist dann am effizientesten, wenn sie auf dem nativen Layer oder darunter erfolgt. Ethernet lässt sich aber auch auf Layer 2 verschlüsseln und dann über ein Layer 3-Netzwerk transportieren. Das macht dann Sinn, wenn die Sicherheit der Layer 2-Verschlüsselung gewünscht ist und die Verbindung auf Layer 3 terminiert. Dazu wird der verschlüsselte Ethernet-Frame über IP getunnelt. Ohne zusätzliche Verkehrsoptimierungsmassnahmen führt der zusätzliche Overhead allerdings zu Mehrverkehr und so zu Einbussen bei der effektiven Durchsatzrate. Als Massstab gilt dabei der Internet Mix (IMIX), der zwecks Vergleichbarkeit einen genormten durchschnittlichen Netzwerkverkehr mit unterschiedlichen Paketgrössen darstellt[11].
Layer 3-Verschlüssler sind für die Verschlüsselung von IP-Nutzlast mit IPSec ausgelegt. Um das ganze IP-Paket inklusive Header IP-Header zu verschlüsseln, muss es getunnelt werden. Will man mittels IPSec einen Ethernet Frame verschlüsseln, so muss dieser zuerst auf Layer 3 gehoben werden. So wird dieser in IP-Nutzlast transformiert, die dann auf Layer 3 verschlüsselt werden kann. Wird für die Verschlüsselung von MPLS-Netzwerken IPSec verwendet, so wird IPSec das original IP-Paket tunneln, das die MPLS-Nutzlast konstituiert, Tunnels führen zu Overhead und zu Rechenaufwand. Doppelte Tunnels, wie sie beim Tunneln eines Layer 2-Frames über IP und Verschlüsselung mit ESP IPSec Tunnel-Modus anfallen, sind nicht mehr als eine Notlösung für den Fall fehlender Layer 2-Infrastruktur und fehlender Alternativen. Im Vergleich zum Tunneln von verschlüsseltem Ethernet über IP bietet das Tunneln von Ethernet über IP und Verschlüsselung mit IPSec weniger Sicherheit und weniger Effizienz.

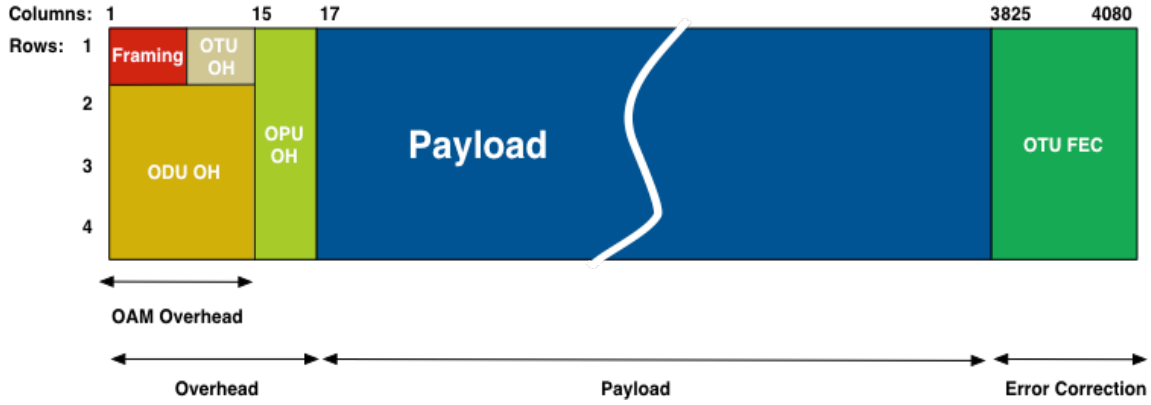
Der nachstehende Vergleich von Verschlüsselung auf Layer 1, Layer 2 und Layer 3 bezieht sich auf die native Verschlüsselung auf dem jeweiligen Layer

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

für Ethernet-Netzwerke. Er zeigt, wie ein verschlüsselter Frame oder ein verschlüsseltes Paket während des Transports aussieht und beinhaltet.

2.2. OTN-Verschlüsselung auf Layer 1

Das Optical Transport Network (OTN), wie von der International Telecommunications Union-Telecom (ITU-T) in G.872.5 beschrieben, ist die Bitstreamschicht des Netzwerks zwischen zwei Hops. ITU-T G.709 definiert die Netzwerkschnittstelle. Ein G.709-Frame besteht aus drei Elementen: Dem Overhead, der Nutzlast und der Fehlerkorrektur.



Der Ethernet-Frame ist OTN-Nutzlast, weshalb die Verschlüsselung der OTN-Nutzlast den kompletten Ethernet-Frame verschlüsselt.
Die meisten Layer 1-Verschlüssler verzichten auf authentisierte Verschlüsselung und damit auf Replay- und Integritätsschutz. Sie sind darauf beschränkt mittels Nutzlastverschlüsselung Vertraulichkeit zu gewähren. Der Grund dafür liegt in der Komplexität der Integration der nötigen Elemente in den beschränkten Platz, der zur Verfügung steht. Auf höheren Netzwerkschichten kann eine volle Authentisierung einfacher implementiert werden, da genügend Platz zur Verfügung steht.

Für die OTN-Standards zeichnet sich die International Telecommunication Union (ITU) verantwortlich. Einen offiziellen Verschlüsselungsstandard gibt es zur Zeit nicht.

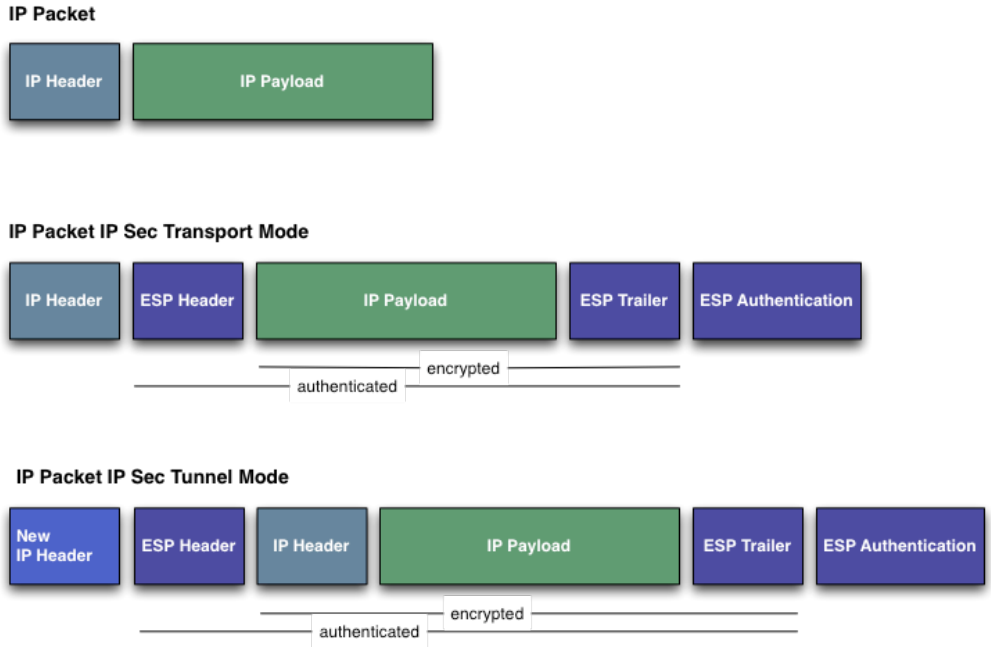
2.3. IPSec-Verschlüsselung auf Layer 3

Für die Standortvernetzung wird bei Verschlüsselung auf Layer 3 in der Regel der IPSec ESP Tunnel-Modus verwendet. Dieser bringt je nach verwendetem Verschlüsselungsstandard einen Paketoverhead von 58–73 Bytes. Diese Zahlen beziehen sich auf IPv4, denn bei IPv6 ist der Overhead um mindestens 20 Bytes grösser. Bei den kleinen Paketen von 64 Bytes, welche einen immer grö-

sseren Anteil des Netzverkehrs ausmachen, kann dies zu einer Verdoppelung der Paketgrösse und entsprechender Netzwerkbelastung führen. Der prozentuale Zuwachs nimmt bei grösseren Paketen ab. Wird die Verschlüsselung von Layer 3 auf Layer 2 verschoben, so sind die IP-Pakete auf Layer 2 reine Nutzlast und können ohne Overhead auf Paketebene verschlüsselt werden. Die authentisierte Verschlüsselung erfolgt dann auf Layer 2 und bringt nur einen Verschlüsselungsoverhead von 24-32 Bytes mit sich. Die Grösse des Overheads ist abhängig von der Implementierung und der Skalierbarkeit. Mit einem Overhead von 26 Byte können beide vollauf gewährleistet werden.

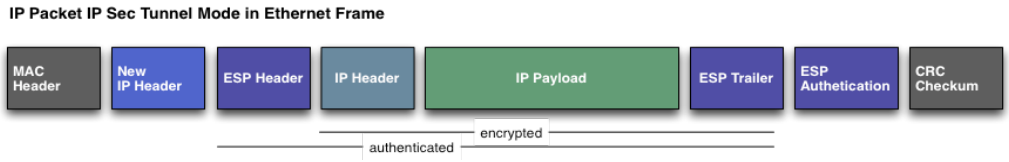
2.3.1. IPSec – Der Standard für Layer 3-Verschlüsselung

Betrachtet man ein IP Paket mit seiner Nutzlast im IPSec ESP Transport und Tunnel Modus, so zeigen sich die Ineffizienzen durch den Verschlüsselungsmodus auf Paketebene deutlich.



Am Anfang steht ein IP-Paket, wie es auf Layer 3 transportiert wird. Es besteht aus einem IP-Header und der Nutzlast.
Im Transport Modus wird nur die Nutzlast verschlüsselt, der ursprüngliche IP-Header bleibt bestehen und ungeschützt und der Verschlüsselungsoverhead bleibt halbwegs im normalen Bereich. In der Regel wird aber der Tunnel Modus verwendet, bei dem auch der IP-Header verschlüsselt und dem Paket ein neuer IP-Header hinzugefügt wird. Damit kann zwar das gesamte ursprüngliche IP-Paket verschlüsselt werden und es findet auch gleichzeitig eine Network Address Translation (NAT) statt, doch drückt sich das auch im Verschlüsselungsoverhead aus. Dieser nimmt entsprechend um 20 Bytes (IPv4) respektive 40 Bytes (IPv6) zu.

Für den Transport auf Ethernet wird das verschlüsselte IP Paket mit einem MAC Header und einer CRC Checksum versehen.

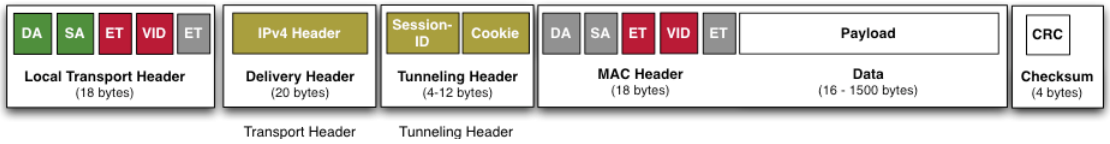


Für Ethernet ist das ganze im IPSec ESP Tunnel Modus verschlüsselte IP Paket reine Nutzlast. Entsprechend kann eine Transport Modus-Verschlüsselung auf Layer 2 ohne Paketoverhead die Nutzlast genauso gut verschlüsseln wie IPSec im ESP Tunnel Modus. IPSec ESP Modus bietet mittels Encapsulating Security Payload (ESP) Vertraulichkeit, Authentisierung des Datenursprungs, Integrität und einen Schutz vor Replay-Attacken. Zur Aufrechterhaltung einer gleichwertigen Sicherheit braucht es äquivalente Mechanismen auf Layer 2. Ein Teil des Overheads, der auf Layer 3 generiert worden wäre, verschiebt sich auf Layer 2. Allerdings mit deutlich weniger Overhead und mehr Flexibilität in Bezug auf die Netzwerkfunktionalität als IPSec auf Layer 3.

Auf Layer 3 spielt es eine Rolle, ob man IPv4 oder IPv6 verwendet. Zwar verwenden beide IPSec als Verschlüsselungsstandard, aber für die L3-Verschlüssler ist es relevant, ob IPv4 oder IPv6 verschlüsselt wird. Auf Layer 2 spielt es keine Rolle, ob die Nutzlast aus IPv4 oder IPv6 besteht.

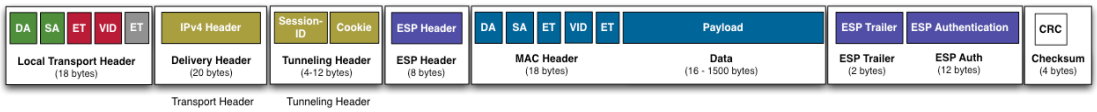
2.3.2. Das Verwenden von IPSec für die Verschlüsselung von Ethernet

Es ist durchaus möglich, Ethernet mittels IPSec zu verschlüsseln. Um das zu bewerkstelligen muss der Ethernet-Frame auf Layer 3 hinaufbefördert werden damit er zur IP-Nutzlast wird. Sobald der Ethernet-Frame IP-Nutzlast ist, kann er auf Layer 3 mittels IPSec verschlüsselt werden. Da IP über Ethernet transportiert wird, ist das Resultat Ethernet, das über IP transportiert wird, das selbst wieder über Ethernet transportiert wird. Es ist genauso ineffizient, wie es tönt. Wird beispielweise L2TPv3 für den Transport von Ethernet über IP verwendet, so verursacht bereits die Einkapselung einen Overhead von 50 Bytes.



L2TPv3-Frame über Ethernet

Die IPSec-Verschlüsselung fügt dem nochmals 38-53 Bytes hinzu. Da L2TPv3 bereits einen Tunnel erzeugt erfolgt die Verschlüsselung im ESP Transport Mode[12]. Ohne Tunnel fällt auch der entsprechende zusätzliche Overhead weg.



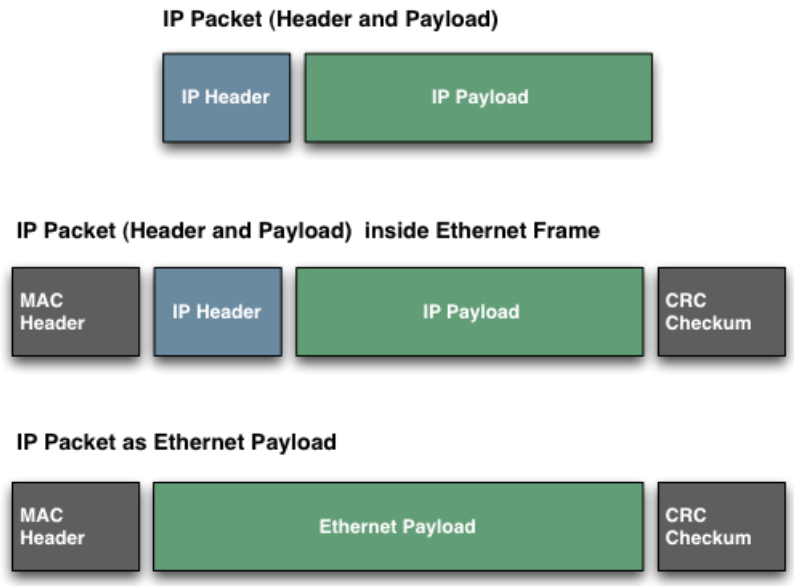
Mit IPSec verschlüsselter L2TPv3 Frame über Ethernet

2.4. Ethernet-Verschlüsselung auf Layer 2

Im Vergleich zur Verschlüsselung von Ethernet mittels IPSec hat die Verschlüsselung auf Layer 2 mit nativer Ethernet-Verschlüsselung massive Vorteile in Bezug auf Sicherheit und Effizienz.

Beginnen wir mit wieder mit einem Paket, wie es auf Layer 3 transportiert wird. Es besteht aus einem IP-Header und der Nutzlast. Für den Transport auf Layer 2 auf Ethernet wird das IP Paket mit einem MAC Header und einer CRC Checksum versehen. Gleich wie das verschlüsselte IP-Paket ist auch das unverschlüsselte IP-Paket auf Layer 2 reine Nutzlast

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



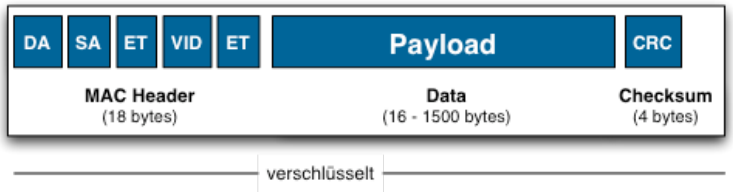
Eine Verschlüsselung im Transport-Modus auf Layer 2 verschlüsselt das ganze IP-Paket inklusive IP-Header ohne dass ein Tunneln nötig ist. Das Tunneln mit IPSec ESP Tunnel Mode allein generiert dagegen einen vermeidbaren Overhead von 20-40 Bytes und führt zudem noch zu einer erhöhten Latenz.

Analog zu IPSec gibt es auch bei der Ethernet-Verschlüsselung unterschiedliche Verschlüsselungsmodi. Diese sind jeweils auf unterschiedliche Anwendungsszenarien und Sicherheitsbedürfnisse ausgerichtet. Grundsätzlich gilt, dass ohne authentisierte Verschlüsselung und zusätzlich authentisierte Daten (AAD) die gewährte Sicherheit von vornherein eingeschränkt ist. Die nachfolgenden Ausführungen beziehen sich auf Ethernet-Verschlüsselung im Allgemeinen und nicht auf MACSec, welches nur ein stark limitiertes Subset von Ethernet-Verschlüsselung bietet.

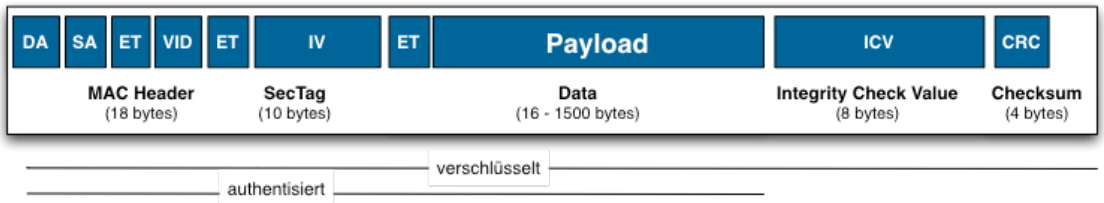
Für die Verbindung von Standorten wird vorzugsweise eine End-to-End-Verschlüsselung verwendet. Eine Hop-by-Hop-Verschlüsselung funktioniert nur in einer beschränkten Anzahl von Szenarien, da sie die Angrenzung (Adjacency) der beteiligten Geräte verlangt.

2.4.1. Frame-Modus (Bulk)

Beim Frame-Modus wir der gesamte Frame verschlüsselt, inklusive aller Adressinformationen und der Checksumme. Das Anwendungsszenario ist auf reine Punkt-zu-Punkt-Verbindungen zwischen zwei Verschlüsslern über eine dedizierte Verbindung beschränkt. Das entspricht der Voraussetzung einer Hop-by-Hop-Verschlüsselung, bei der das Angrenzen der beiden Geräte (Adjacency) Bedingung ist.



Verschlüsselung im Frame-Modus

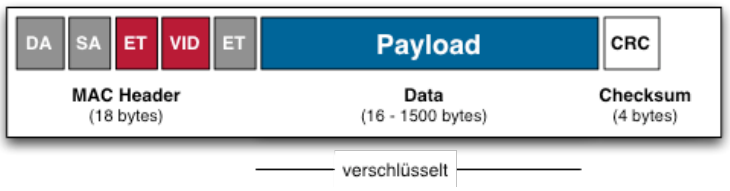


Authentisierte Verschlüsselung im Frame-Modus

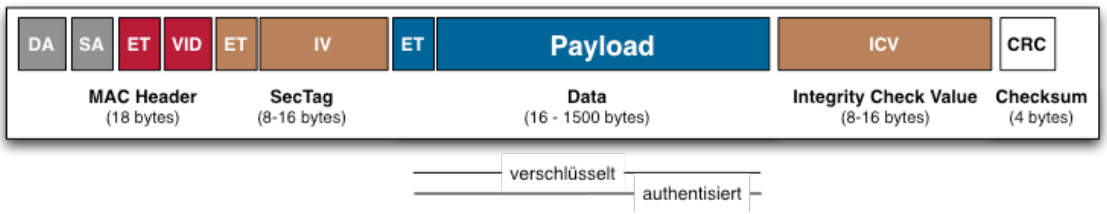
Bei der Frame-Verschlüsselung (auch Bulk Encryption oder Link Encryption genannt) wird der ganze Ethernet-Frame samt seiner Nutzlast zwischen Preamble und Interframe Gap verschlüsselt. Bei einer Verschlüsselung auf Layer 3 müsste dafür der ganze Ethernet-Frame getunnelt und dann mit IPSec verschlüsselt werden, was zu massivem Overhead führt. Da sämtliche Adressinformationen mitverschlüsselt werden, beschränkt aber der Frame-Modus auf Layer 2 die möglichen Einsatzszenarien auf Hop-by-Hop, Ohne Authentisierung gilt auch der Frame-Modus nicht als sicher.

2.4.2. Transport-Modus

Der meistgenutzte Verschlüsselungsmodus ist der Transport-Modus. Der Grund dafür liegt in der vollen Netzwerkkompatibilität, die durch die Begrenzung der Verschlüsselung auf die Nutzlast erreicht wird.



Verschlüsselung im Transport-Modus



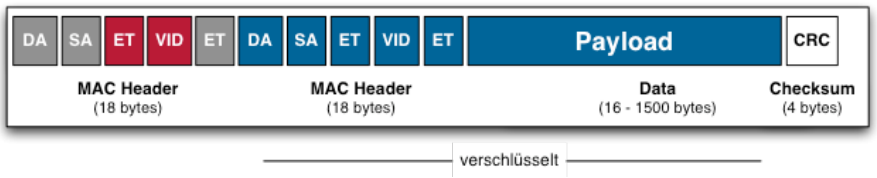
Authentisierte Verschlüsselung im Transport-Modus

Beim Transport-Modus gibt es zwei verschiedene Modi, wobei der erste Modus zwar AES verwendet, aber nur die Nutzlast verschlüsselt. Ausser Vertraulichkeit werden so keine Sicherheitsfunktionen geboten. Der andere, zeitgemä-

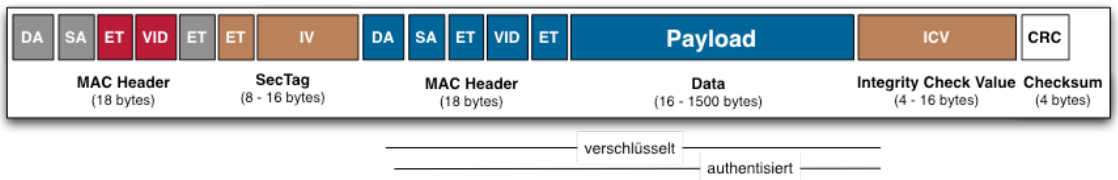
sse Modus stellt unter Verwendung von AES-GCM nebst der Nutzlastverschlüsselung auch die erforderliche Authentisierung inklusive explizitem Replay- und Integritätsschutz bereit. IPSec verwendet bei der Verschlüsselung auch im Transport-Modus immer ESP. Deshalb muss bei einem Vergleich zwischen IPSec und nativer Ethernetverschlüsselung zwecks Vergleichbarkeit auch die Ethernet-Seite die entsprechenden Schutzvorkehrungen unterstützen.
Der unauthentisierte Transport-Modus kann im übrigen nur dann ohne Overhead betrieben werden, wenn man den EtherType eines anderen Netzwerkdienstes verwendet. Korrekterweise müsste ein eigener oder ein dafür reservierter EtherType verwendet und der originale Ethertype zusammen mit der Nutzlast verschlüsselt werden. Das verursacht aber einen Overhead von zwei Bytes. Wenn also ein Hersteller in seinem Marketing gross hervorhebt, dass seine Verschlüsselung keinen Overhead erzeugt, dann verletzt er bei Verwendung des Transport-Modus unter Umständen vornherein die Verhaltensregeln auf dem Netzwerk und spart auch an der Sicherheit. Der verharmlosende Name für das Nutzen eines fremden EtherTypes nennt sich „EtherType Mutation“ oder „EtherType Transformation“.

2.4.3. Tunnel-Modus

Wie auf Layer 3 gibt es auch auf Layer 2 einen Tunnel-Modus. Er wird dann eingesetzt, wenn der gesamte Original-Frame verschlüsselt werden muss und ein Multihop-Szenario vorhanden ist. Das Tunneln auf Layer 2 führt zu einem Overhead von 18 Bytes und marginal erhöhter Verarbeitungszeit, reduziert aber die sichtbaren Netzwerkadressen auf die Adressen der Verschlüssler und limitiert so die für Traffic Analysis nutzbaren Metadaten. Auch im Tunnel-Modus stehen sowohl nichtauthenisierte und authentisierte Verschlüsselung zur Verfügung. Auf den Einsatz authentisierter Verschlüsselung darf auch hier nicht verzichtet werden.



Verschlüsselung im Tunnel-Modus

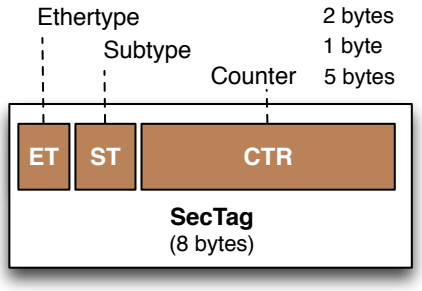


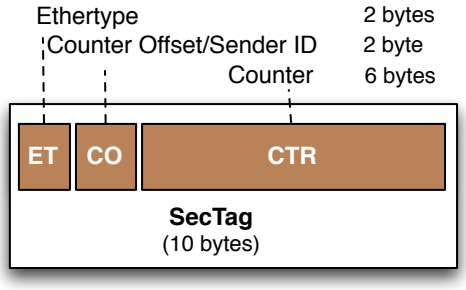
Authentisierte Verschlüsselung im Tunnel-Modus

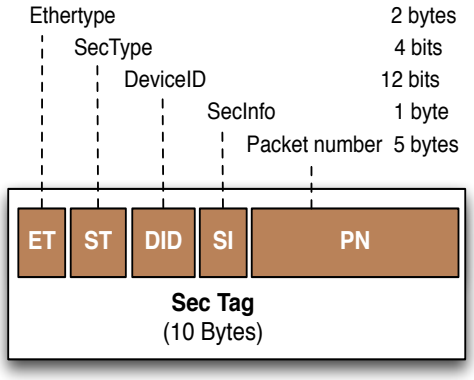
2.4.4. SecTags

Das SecTag beinhaltet den für die verschlüsselte Nutzlast verwendeten Ethertype und den für die Verschlüsselung benötigten Initialisierungsvektor. Der Inhalt des Initialisierungsvektors ist abhängig von den Informationen, welche die Schlüsselverwaltung benötigt. In der Regel ist das der Counter und die Zuweisung des Counters auf einen Sender. Je nach Hersteller ist die Grösse des Counters und die Anzahl möglicher Zuweisungen anders ausgestaltet. Auch in der Anzahl zusätzlich mitgeführter Informationen gibt es Unterschiede. Je länger der Counter, desto weniger oft wir ein Schlüsselwechsel erzwungen. Je grösser der Adressraum für Zuweisungen, desto mehr Mitglieder kann eine Gruppe haben. Minimal sind 1 Byte für die Zuweisung, was 256 Gruppenmitglieder erlaubt, und 5 Byte für den Counter notwendig. 2 Byte für die Zuweisung und 6 Byte für den Counter erhöhen die Skalierbarkeit und bieten erweiterte Reserve für höhere Netzwerkbandbreiten und grössere Gruppen.

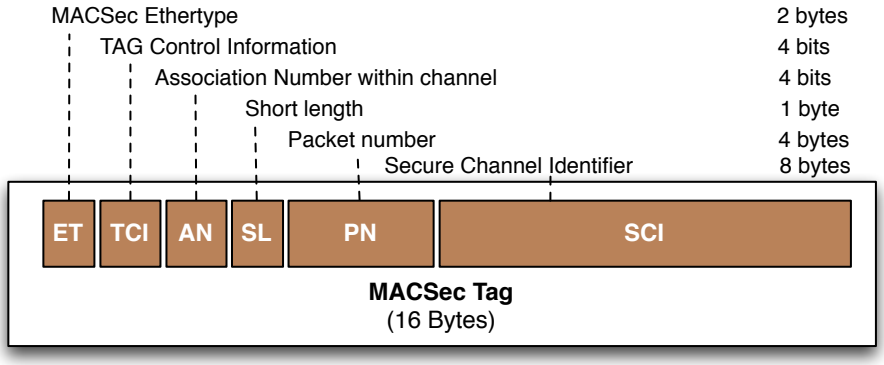
Die entsprechenden SecTags sehen so aus:





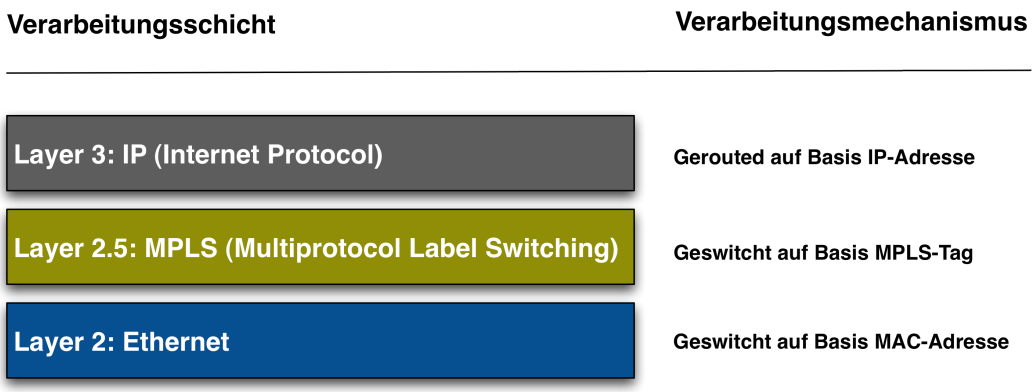


Das SecTag von MACSec umfasst 16 Bytes, ohne dabei funktionale Vorteile aufzuweisen. Der durch MACSec auf Frame-Basis erzeugte Overhead liegt 6-8 Bytes höher als bei anderen Verschlüsselungslösungen, welche auch AES-GCM auf Layer 2 verwenden.



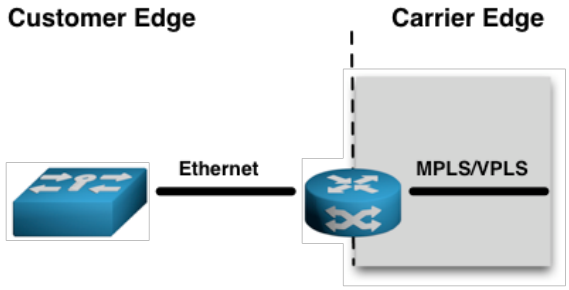
2.5. Verschlüsselung von MPLS-Netzwerken

Über Ethernet werden nicht nur Nutzdaten und Daten von Layer 3 aufwärts transportiert, sondern auch MPLS. MPLS steht für Multiprotocol Label Switching und liegt zwischen Layer 2 und Layer 3. Es ist ein Layer 2.5-Protokoll, das die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz erlaubt.



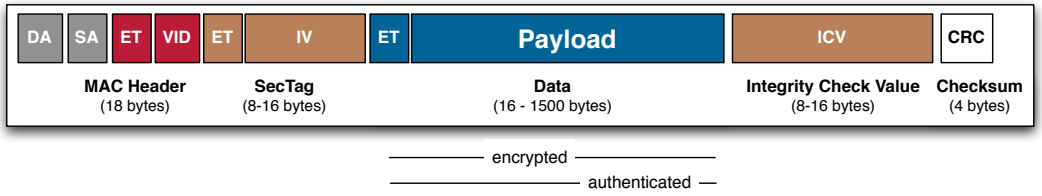
MPLS kann unterschiedlichsten Datenverkehr transportieren, darunter auch IP-Pakete und Ethernet Frames. Ethernet-Verschlüssler sollten MPLS so weit wie möglich unterstützen. Je nach Position des Verschlüsslers im Netzwerk wird eine andere Unterstützung benötigt.

Wird MPLS als reines Transportnetzwerk für Ethernet-Frames verwendet, so ist es für den Kunden vollständig transparent. Sichtbar ist nur Ethernet und auch die Verschlüsselung beschränkt sich auf Ethernet.

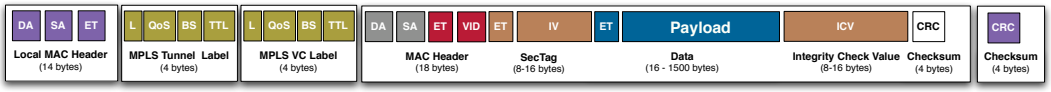


Verwendung von MPLS/VPLS für den Transport von Ethernet-Frames

Beim diesem Szenario handelt es sich um ein normales Ethernet-Szenario und die Verschlüsselung beschränkt sich auf die Ethernet-.

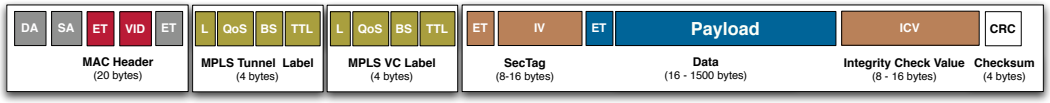


Ethernet-Verschlüsselung im Transport-Modus vor Übergabe an MPLS-Netzwerk



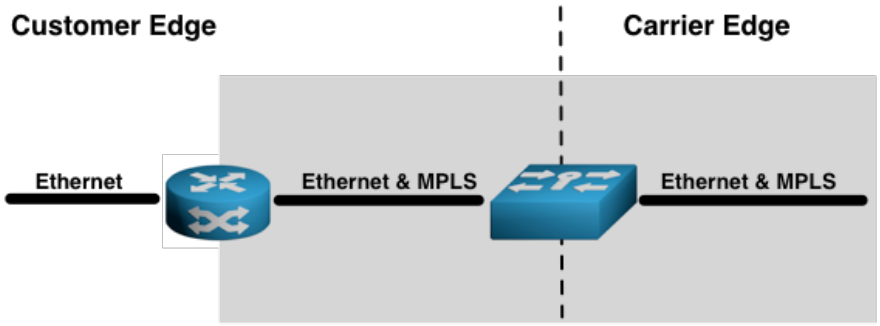
Ethernet over MPLS (EoMPLS)

Es gibt aber zwei Arten der Nutzung von MPLS: Nebst dem Transport von Ethernet-Frames über MPLS kann auch MPLS direkt genutzt werden, wobei im Frame ein MPLS-Tag eingefügt wird. Das hat Auswirkungen auf den Inhalt der Frames:

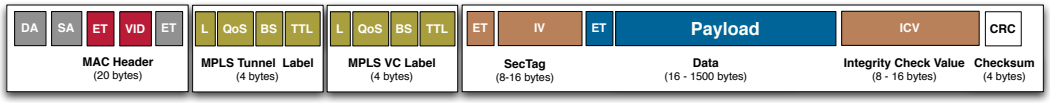


Authentisierte Verschlüsselung im Transport-Modus mit eingefügtem MPLS-Tag

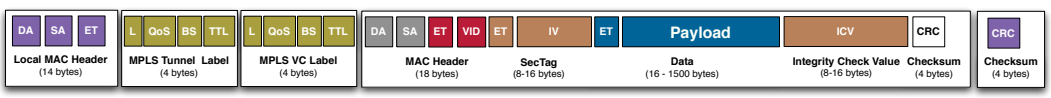
Anders sieht es aus, wenn der Verschlüssler zwischen dem MPLS-Router und dem Ethernetanschluss des Telekomanbieters steht.



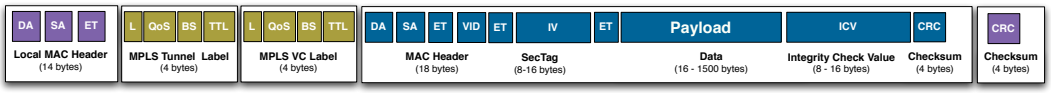
Ein Verschlüssler, der nach dem MPLS Switch/Rozter positioniert ist, hat es meist mit mehr Szenarien zu tun als ein Verschlüssler, der vor dem MPLS/VPLS Swich/Router positioniert ist. Die Verschlüsselung darf hier erst nach dem MPLS-Tag erfolgen.
Können Frames mit MPLS-Tag von der normalen Ethernet-Verschlüsselung ausgenommen werden und kann der Verschlüssler Ethernet over IP (EoIP), so können sämtliche MPLS-Szenarien unterstützt werden. Dies umfasst sowohl MPLS über Ethernet als auch MPLS über IP und geht soweit, dass der Ethernet-Verschlüssler auch nur über IP-Netzwerke erreichbare MPLS-Destinationen voll unterstützt, sowohl in Bezug auf Auslieferungsformat als auch auf Schlüsselverteilung. Zusätzlich zur Unterstützung von Ethernet over IP (EoIP) sind zur Kompensation des durch das Tunneln erhöhten Overheads Verkehrsoptimierungsmassnahmen auf Frame-Ebene nötig. So kann ein durchschnittlicher IMIX-Durchsatz von über 96% erreicht werden. Ein grosser Vorteil der Verschlüsselung von IP/MPLS-Netzwerken auf Layer 2 liegt im gewährten Komplettschutz, der Vertraulichkeit, Integritätsschutz, Entdecken von Eindringlingen, Verhindern von Eindringlingen, einen Layer 2-Firewall und Resistenz gegen DDoS-Attacken umfasst. Dies bringt speziell bei breitbandigen Anschlüssen Einfachheit und Kosteneinsparungen mit sich.
Die nachstehenden Beispiele beschränken sich auf MPLS über Ethernet (MPLSoE), bei dem MPLS auf Layer 2 terminiert wird. Dies ist eine Funktion, die sich rein auf Layer 2 beschränkt und keine Unterstützung von EoIP voraussetzt. Dabei gibt es folgende Verschlüsselungsoptionen:



Ethernet-Frame mit eingefügtem MPLS-Tag



Ethernet-Frame mit Transport-Modus-Verschlüsselung transportiert über MPLSoE



Ethernet-Frame mit Frame-Modus-Verschlüsselung transportiert über MPLSoE

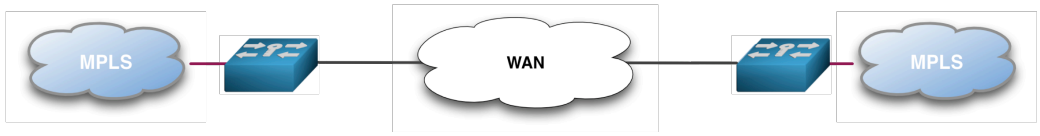
2.5.1. Ethernet über MPLS/VPLS

Beim Transport von Ethernet-Frames über MPLS muss der Verschlüssler den Ethernet-Header unverschlüsselt lassen und sich auf die Nutzlast beschränken, da MPLS auf die Header-Informationen angewiesen ist.

Die Voraussetzungen für den Transport über MPLS sind sowohl beim Transport- wie auch beim Tunnel-Modus erfüllt, denn es braucht keine direkte Unterstützung von MPLS, sondern nur Transparenz.
Der Transport von Ethernet über MPLS kann auf zwei unterschiedliche Arten erfolgen: Bei einem durchgängigen Ethernet-Netzwerk setzt MPLS sein Tag zwischen den Ethernet Header und die Nutzlast und benötigt Teile der Informationen des Ethernet Headers, der deshalb unverschlüsselt bleiben muss. Bei Transport über unterschiedliche Layer 2-Netzwerke, enkapsuliert MPLS den Originalframe und macht ihn somit zur Nutzlast. Das MPLS-Tag wird vor die Nutzlast gesetzt und ein lokaler Ethernet Header und eine lokale Checksum hinzugefügt.

2.5.2. MPLS Interconnect

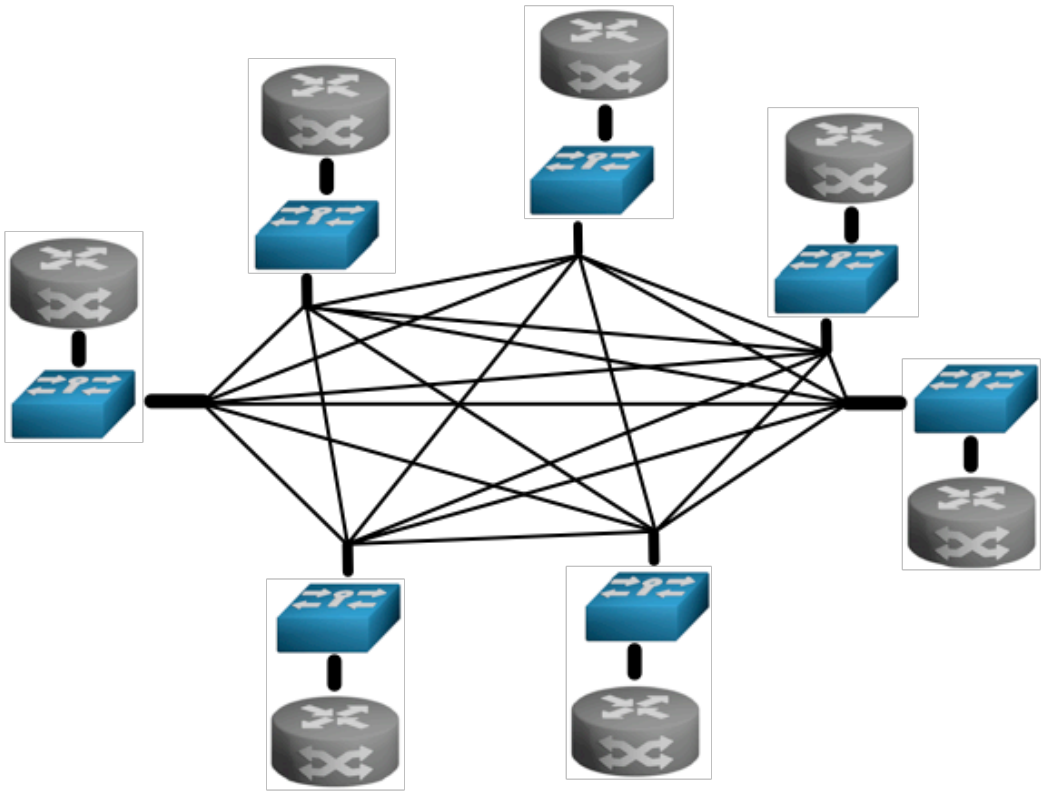
In einem Szenario, bei dem die Verbindung von lokalen MPLS-Wolken über ein WAN verschlüsselt werden soll, muss der Verschlüssler das Frameformat erkennen und sich entsprechend anpassen. Der Frame ist entweder ein Ethernet-Frame mit MPLS Tag oder ein Ethernet-Frame mit MPLS-Tag, bei dem der Original-Frame enkapsuliert als Nutzlast transportiert wird. In beiden Fällen darf nur die Nutzlast verschlüsselt werden, wobei sie in erstem Fall aus der Ethernet-Nutzlast und im zweiten Fall aus dem Originalframe besteht.



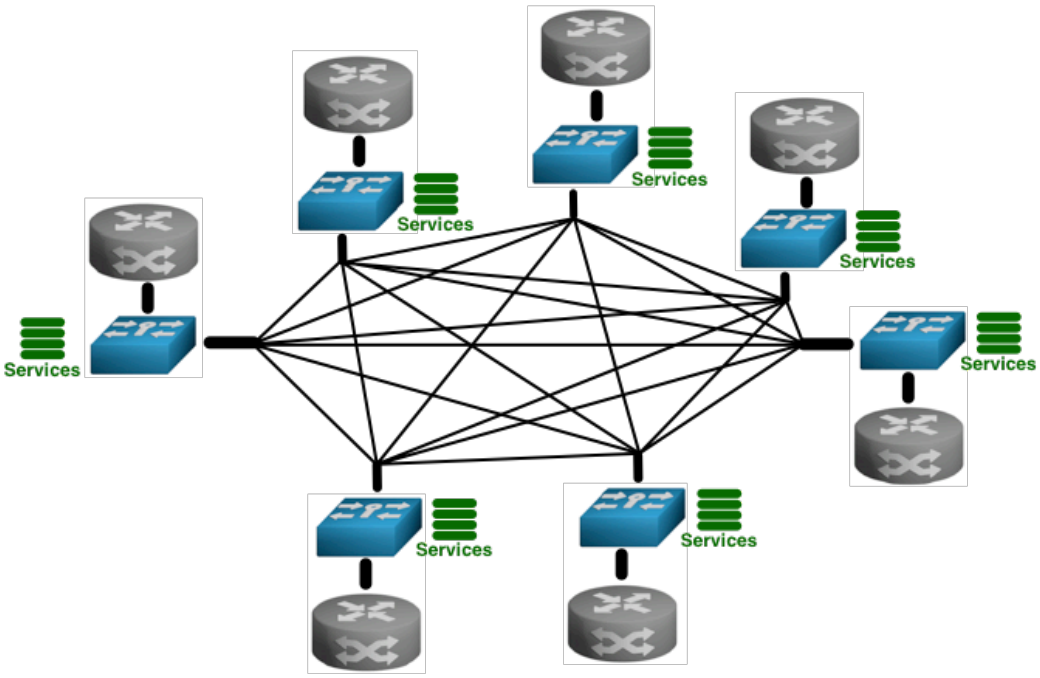
2.5.3. Zwischen MPLS-Clouds

Bei der Verschlüsselung einer Verbindung von lokalen MPLS-Wolken über eine Carrier-MPLS-Wolke darf der Verschlüssler nur die Nutzlast verschlüsseln, die aus dem enkapsulierten Originalframe besteht. Dazu muss er erkennen, dass es ich um MPLS handelt und wo sich die Nutzlast befindet.

Die nachstehenden beiden Diagramme zeigen MPLS-basierte Multipunkt-Netzwerke: Einmal auf der Basis von Ethernet Privat LAN und einmal auf der Basis von Ethernet Virtual Private LAN. Nur wenn es sich um ein in sich geschlossenes Ethernet-Netzwerk ohne externe Anbindung an IP-Netzwerke handelt, kommt ein Ethernet Private LAN in Frage. Bei einem Ethernet Virtual Private LAN gibt es diese und viele andere Einschränkungen nicht.



Verbindung von lokalen MPLS-Wolken über Ethernet Private LAN



Verbindung von lokalen MPLS-Wolken über Ethernet Virtual Private LAN

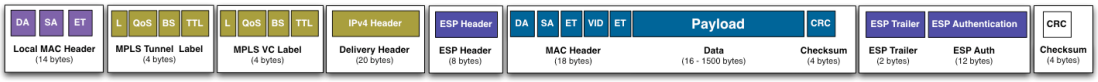
Das Ethernet Virtual Private LAN erlaubt es, das MPLS-Netzwerk als eines von mehreren Netzwerken zu unterstützen.

Die Anforderungen an den Verschlüssler sind je nach Einsatzszenario und Topologie unterschiedlich. Dies betrifft sowohl die Verschlüsselungsmodi wie auch die Netzwerkunterstützung. Nur die wenigsten Verschlüssler lassen sich optimal auf alle Multipunkt-Topologien und –Einsatzszenarien parametrisieren.

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

2.5.4. Das Verwenden von IPSec für die Verschlüsselung von MPLS

MPLS-Netzwerke kommen in unterschiedlichen Varianten. Die Absicherung passt sich diesen Varianten an. MPLS over IP, MPLS over GRE und MPLS over L2TPv3. Für alle drei gilt: Da es sich bei MPLS selbst um einen Tunnel handelt, wird IPSec im Transport Modus verwendet. Die Absicherung mit IPSec macht nur dann Sinn, wenn es sich um ein reines IP-Netzwerk handelt. In einer Carrier-Ethernet-Umgebung bietet es weder die nötige Sicherheit noch die gewünschte Effizienz. In Bezug auf die Sicherheit fehlt die Verschlüsselung und Authentisierung der Daten unterhalb von Layer 3 und in Bezug auf die Effizienz liegen Overhead und Verarbeitungsgeschwindigkeit deutlich unter den Möglichkeiten eines guten Ethernet-Verschlüsslers.



MPLS über Ethernet, getunnelt über IP und geschützt mit 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

Große Entscheidungen erfordern besondere Sicherheit.

Regierungen und ihre Mitarbeiter sind darauf angewiesen, kritische Daten geschützt und zuverlässig austauschen zu können – denn wo wichtige Entscheidungen getroffen werden, hat Datensicherheit höchste Priorität. Dafür sind Giesecke & Devrient und secunet Ihre verlässlichen Partner. Zusammen sorgen wir dafür, dass Geheimnisse auch geheim bleiben.

www.cybersecurity-madeingermany.com

secunet

Giesecke & Devrient

3. Verschlüsselung: Sicherheit, Effizienz und operationelle Aspekte

Unterschiedliche Vorgehensweisen haben Auswirkungen auf Sicherheit, Netzwerkkompatibilität, Effizienz, Einsatzbereich, Betrieb und Kosten. Nah- und Weitverkehrsnetze bilden in der Regel eigene Sicherheitszonen. Es macht Sinn, diese so gut wie möglich abzusichern, weil so wichtiger Datenverkehr verhältnismässig günstig abgesichert werden kann. So frei werdende Ressourcen stehen dann für komplexere und schwieriger abzusichernde Bereiche zur Verfügung.

3.1. Sicherheit

Die Sicherheit umfasst eine Vielzahl an unterschiedlichen Aspekten und es gibt unterschiedliche Lösungswege für die jeweiligen Problemkreise. Entscheidend für die Sicherheit ist das jeweilige Gesamtsystem inklusive dessen Implementierung, nicht einzelne, aus dem Kontext gerissene Teilbereiche[13].
Die beste Lösung für das Absichern von Layer 2-Netzwerken bieten heute spezialisierte, autonome Layer 2-Verschlüssler. Es handelt sich dabei um komplette Lösungen, die sich messerscharf auf ihre Aufgabe fokussieren. Nur deshalb können sie ihren Dienst dermassen effizient und sicher leisten. Die Abläufe und das Management sind vollständig auf die eine Aufgabe optimiert. Dies erhöht nicht nur Leistung und Sicherheit, sondert wirkt sich kurz-, mittel- und längerfristig auch positiv auf die Flexibilität und die Kosten aus. Es gibt zwar unterschiedliche Ansätze, um Layer 2-Verschlüsselung in andere Appliances zu integrieren und sie als Nebenaufgabe auszuführen, doch bietet bisher keine dieser Lösungen die Sicherheit und Effizienz eines dedizierten Verschlüsslers.

Die benötigte Sicherheit wird durch zwei Hauptfaktoren bestimmt. Einerseits ist das der Schutzbedarf der über das Netzwerk übermittelten Daten: Für Daten, die „nur“ sensitiv sind, geltend aufgrund des geringeren möglichen Schadens weniger strenge Sicherheitsvorgaben als für vertrauliche oder gar geheime Daten. Es hängt also davon ab, wie wichtig und vertraulich die Daten sind. Andererseits ist das der Schutzbedarf des Netzwerks in Bezug auf Sicherheit und Kontinuität. Ist eine Organisation vom reibungslosen Betrieb des Netzwerks abhängig, so kann eine Beeinträchtigung negative Folgen auf den Betrieb haben. Ein möglichst guter und effizienter Schutz des Netzwerks vor Angriffen ist deshalb essentiell. Besteht keine solche Abhängigkeit, dann kann auch ein geringerer Schutz genügen.

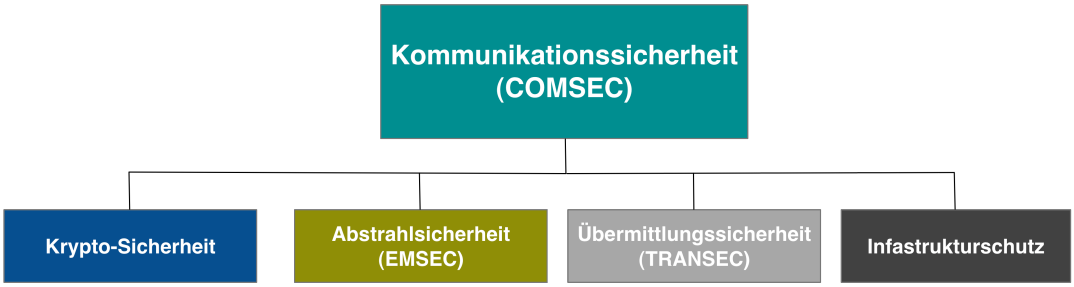
Grundsätzlich lassen sich Netzwerkverschlüssler in drei Sicherheitskategorien aufteilen:

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

- High Assurance für klassifizierte und sensitive Daten[14]
- Standard Assurance für sensitive Daten
- Low Assurance für wenig sensitive und unsensitive Daten

Für die Einstufung ist die gewährte Sicherheit entscheidend. Im Bereich High Assurance findet man spezialisierte Appliances, die auf einer Sicherheitsplattform basieren, die für die Übermittlung klassifizierter Daten zertifiziert sind und sowohl Netzwerk wie auch Daten eigenständig verlässlich schützen. Da solche Geräte bei Zertifizierung für hohe Geheimhaltungsstufen unter Verkaufs- und Exportrestriktionen fallen können, gibt es Anbieter, die ihre Geräte nur für die unteren Geheimhaltungsstufen von klassifizierten Daten zertifizieren lassen, obwohl sie Sicherheitsanforderungen von höheren Geheimhaltungsstufen erfüllen. Nur so können die Geräte sowohl im Regierungs- und Behördenmarkt als auch im zivilen Geschäftsmarkt angeboten werden.
Standard Assurance wird ebenfalls von Appliances gewährt, doch sind diese nur für die Übermittlung sensitiver Daten zertifiziert. Solche Geräte verfügen über alle essentiellen Sicherheitsmerkmale und gewähren eigenständig sowohl Schutz für die Daten als auch für das Netzwerk.
Im Bereich Low Assurance finden sich vorwiegend integrierte Lösungen, bei denen zwar zeitgemässe Verschlüsselungsalgorithmen zum Einsatz kommen, aber nicht alle essentiellen Sicherheitsmerkmale vorhanden sind. Selbst solche Lösungen lassen sich zertifizieren, sind aber nur für weniger sensitive Daten und Netzwerke mit geringerem Schutzbedarf geeignet. In diese Kategorie fallen beispielsweise integrierte MACSec-Lösungen und virtuelle Appliances ohne zusätzliche Hardwareunterstützung.

Das ultimative Ziel ist die Kommunikationssicherheit. Diese fängt bei der Krypto-Sicherheit an and setzt sich über Abstrahlsicherheit (EMSEC) die Übermittlungssicherheit und den Infrastrukturschutz fort.



Die Krypto-Sicherheit umfasst Netzwerksicherheit, sichere Schlüssel und ein sicheres Verschlüsselungsgerät.

[14] https://de.wikipedia.org/wiki/Geheimhaltungsstufe

3.1.1. Netzwerksicherheit

Die Devise beim Absichern von Netzwerken lautet: So viel wie möglich und so einfach wie möglich verschlüsseln und authentisieren. Dabei gibt es Kompromisse zwischen absoluter Netzwerksicherheit und Netzwerkkompatibilität, denn am sichersten ist es, wenn alles verschlüsselt ist. Da dies sämtliche enthaltene Adressinformationen verdeckt, geht die Netzwerkompatibilität auf dem nativen Layer verloren, da zwischengeschaltete Netzwerkgeräte solche Frames wegen den unzugänglichen Adressinformationen nicht mehr verarbeiten können.
Netzwerksicherheit für den Datentransport setzt mehrere Funktionalitäten voraus, die sich aus dem Zusammenspiel von Endpunktfunktionalität und übermittelten Daten ergeben: Die Vertraulichkeit der übermittelten Daten, das Sicherstellen der Integrität der übermittelten Daten, die Authentisierung der übermittelten Daten und die Resistenz gegen Angriffe. Grundsätzlich sind native Lösungen für eine Netzwerkschicht sowohl am kompatibelsten, am sichersten und am effizientesten. Bei Carrier Ethernet ist das eine Layer 2-Verschlüsselung.
Mit Layer 3-Verschlüsselung kann man die IP-Schicht und was darüber liegt verschlüsseln, nicht aber das zugrundeliegende Ethernet-Netzwerk mit sämtlichen Protokollen, die sich darauf tummeln. Der Schutz des gesamten Ethernet-Netzwerkverkehrs lässt sich nur mit Layer 2-Verschlüsselung ohne ressourcenhungrige Einkapselung und zusätzliches Tunneln bewerkstelligen. Layer 3-Verschlüsselung ist dazu nicht in der Lage, da es nur die IP-Pakete auf dem Network Layer verschlüsseln kann; der gesamte Rest bleibt aber unverschlüsselt. Effizienten Schutz für Layer 2-Nutzlast gibt es nur auf Layer 2. Das Gleiche gilt für den Vollschutz sämtlichen Layer 2-Verkehrs (ARP, STP, CDP, etc.).
Um Layer 3 zu schützen, muss IPSec den Original-Header tunneln und um Layer 2 zu schützen muss der ganze Layer 2-Frame eingekapselt werden. Beide Mechanismen führen zu einer wahrnehmbaren Leistungseinbusse. Bei Standortverbindungen über Carrier Ethernet bietet die Verschlüsselung direkt auf Layer 2 mittels AES-GCM unter Verwendung von 256 Bit-Schlüsseln für die vorhersehbare Zukunft eine optimale Lösung.
Bei der Netzwerksicherheit spielen die verwendeten Standards und Algorithmen und deren Implementierung eine wichtige Rolle, sind aber in Bezug auf die gewährte Sicherheit zusätzlich abhängig von sicheren Schlüsseln und einem sicheren Verschlüsselungsgerät.

3.1.2. Sicheres Verschlüsselungsgerät

Ist der Netzwerkverkehr gut abgesichert, so ist der nächste Angriffspunkt in den Endgeräten zu finden. Ein dediziertes Gerät lässt sich dabei einfacher absichern als der Teilbereich eines Geräts. Auch bei einem dedizierten Gerät müs-

sen alle Zugänge abgesichert sein, doch gibt es deutlich weniger Zugänge als bei einer integrierten Appliance oder einer virtuellen Appliance. Insbesondere fallen sämtliche systeminternen Zugänge weg. Geringere Komplexität führt zu mehr Sicherheit.
Die meisten spezialisierten Appliances bauen auf einer Sicherheitsplattform auf, sind auf Sicherheit optimiert und genügen höchsten Anforderungen. Es sind in sich geschlossene und geprüfte Systeme. Sie weisen auch nur die notwendigen Schnittstellen auf. Ohne vollumfassende Absicherung gegen Angriffe von aussen leidet die Sicherheit des Verschlüsselungsgeräts selbst. Bei integrierten und virtuellen Appliances ist es schwierig bis unmöglich eine solche Sicherheit zu bieten. Das liegt unter anderem daran, dass der nötige Schutz aller möglichen zusätzlichen externen und internen Einfallstore fast nicht zu bewerkstelligen ist. Entsprechend häufig tauchen bei integrierten Appliances wie Switches, Router und Firewalls Schwachstellen auf, die erstens die Geräte für Angriffe anfällig machen und zweitens mittels Patch geflickt werden müssen [15][16][17][18][19]. Was in Bezug auf Schwachstellen bekannt wird, ist nur die Spitze des Eisbergs. Zu den bekannten Schwachstellen kommen noch die bisher nicht öffentlich bekannten Schwachstellen hinzu. Diese stellen ein unkontrollierbares Risiko dar. Zudem führt das Einspielen eine Patches zu Betriebskosten und Netzwerkausfallzeit.

3.1.3. Sichere Schlüssel

Unsichere Schlüssel kompromittieren jede Verschlüsselung. Die Sicherheit fängt bei der Erstellung an und erstreckt sich über Austausch und Lagerung. Auch hier spielt Hardware eine übergeordnete Rolle. Für das Erstellen eines sicheren Schlüssels braucht es Zufallszahlen. Die benötigte Zufälligkeit liefert wegen der Qualität und Quantität der benötigten Entropie nur ein hardwarebasierter echter Zufallszahlengenerator. Reine Softwarelösungen beschränken sich auf berechnete Pseudozufallszahlen. Es ist oft die eingeschränkte Zufälligkeit der Zufallszahlen, die einen Schlüssel von vornherein unsicher macht[20].

Bei spezialisierten Appliances sind Gehäuse und Schlüsselspeicher komplett abgesichert, meist auch gegen Abstrahlungen. Bei Manipulationsversuchen wird der Schlüsselspeicher geleert und angezeigt, dass ein Manipulationsversuch stattgefunden hat. Die Gehäuse sind gegen Manipulationsversuche resistent. Diese Sicherheit ist bei integrierten Appliances wie Switches, Firewalls und Router fast nicht und bei virtuellen Appliances gar nicht erreichbar.
Für die Verschlüsselung wird immer der Schlüssel im Klartext verwendet. Die Sicherheit der Umgebung, in welcher der Schlüssel eingesetzt wird, ist deshalb

[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

ein entscheidendes Kriterium. Erfolgt die Verschlüsselung direkt auf der Netzwerkschnittstelle, so gewährt das mehr Angriffspunkte und weniger Sicherheit als wenn die Verschlüsselung in einem geschützten und nicht gegen aussen exponierten Bereich erfolgt.

3.1.4. Übermittlungssicherheit (TRANSEC)

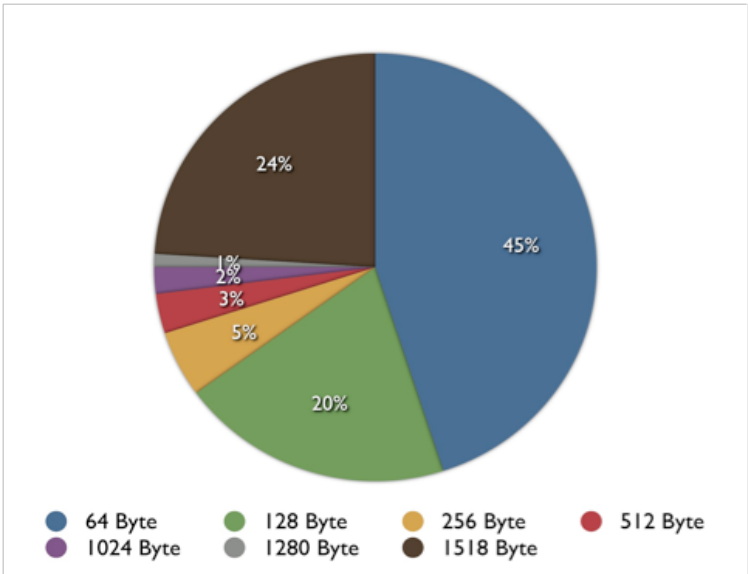
Authentisierte Verschlüsselung stellt die Vertraulichkeit der übermittelten Daten und die Integrität des Netzwerks sicher, der Netzwerkwerkverkehr bleibt aber sichtbar. Damit sich nicht mittels Traffic Analysis herausfinden lässt, was sich auf dem Netzwerk abspielt, gibt es Traffic Flow Security. Diese vernebelt den Netzwerkverkehr. Traffic Flow Security kann unterschiedlich implementiert werden. Ein Ansatz besteht darin, grössenmässig gleichförmige Frames zu verwenden. Es wird eine allgemeine Framegrösse festgelegt, die immer eingehalten wird. Die effektiven Netzwerk-Frames werden in diese Frames gepackt und damit getunnelt. Passen zwei oder mehrere Frames in den Tunnel-Frame, so werden sie zusammen in den Tunnel-Frame gepackt und der verbleibende Platz mit zufällig generiertem Netzwerkverkehr aufgefüllt. Passt ein Netzwerk-Frame aufgrund der Grösse nicht in ein Tunnel-Frame, so wird es fragmentiert und über mehre Tunnel-Frames gesplittet. In Bezug auf Overhead und Latenz bringt dieser frame-orientierte Ansatz Nachteile mit sich. Er ist in der Regel auf Punkt-zu-Punkt-Betrieb beschränkt.
Ein anderer Ansatz orientiert sich nicht an der Framegrösse, sondern am Verkehrsfluss. Statt Frames werden Lücken im Verkehrsfluss aufgefüllt und es entsteht ein ununterbrochener Datenstrom. Die neusten Entwicklungen erlauben die Vernebelung des Netzwerkverkehrs in drei unterschiedlichen Verschlüsselungsmodi – Frame, Transport und Tunnel – und in allen Topologien: Punkt-zu-Punkt, Punkt-zu-Multipunkt und Multipunkt-zu-Multipunkt. Während im Frame-Modus sämtliche Adress- und Netzwerksverkehrsinformationen vernebelt sind, bleiben im Tranport-Modus die Netzwerkadressen sichtbar. Im Tunnel-Modus bleiben nur die Netzwerkadressen der Verschlüssler sichtbar. Mittels einer Kombination von Gruppierung von Frames und nichtssagendem Zusatzverkehr wird eine erfolgreiche Traffic Analysis verhindert, ohne dass die Netzwerkkompatibilität darunter leidet. Die variable Gruppierung von Frames hat zudem positive Auswirkungen auf die Netzwerkeffizienz, da gruppierte Frames nur einmal authentisiert werden müssen und auch der Interframe Gap zwischen den gruppierten Frames wegfällt.

3.2. Effizienz, Leistung und Erweiterbarkeit

Die Effizienz wird durch die Grösse des Sicherheitsoverheads, das Schlüsselsystem, die Verarbeitungsgeschwindigkeit und die Skalierbarkeit bestimmt.

3.2.1. Sicherheitsoverhead

Der Sicherheitsoverhead wird durch die verwendeten Verschlüsselungsstandards und Verschlüsselungsmodi generiert. Dabei gilt festzuhalten, dass es ohne Sicherheitsoverhead auch nur eine massiv eingeschränkte Sicherheit gibt. Ein Vergleich des gesamten Verschlüsselungsoverheads bei Verwendung des gleichen Verschlüsselungsstandards (AES-GCM) zeigt auf, dass bei IPSec ein Paketoverhead von mindestens 58–73 Bytes[21] entsteht, während bei der Verschlüsselung eines Ethernet-Frames im Transport-Modus nur ein Verschlüsselungsoverhead von 24-32 Bytes anfällt. Der Overhead auf Layer 2 ist also signifikant tiefer und die Layer 2-Lösung entsprechend effizienter.



Je kleiner die Paketgrösse, desto grösser ist in relativer Hinsicht der von IPSec generierte Overhead. Gemäss IMIX, dem standardisierten durchschnittlichen Paketgrössenmix für IP-Verkehr betragen die Pakete mit einer Grösse von 64 Bytes rund 45% aller IP-Pakete auf einem Netzwerk. Die IP-Pakete von einer Grösse von 64 Bytes und 128 Bytes machen zusammen gar knapp zwei Drittel aller Pakete aus.

Die Fähigkeit und Flexibilität des Schlüsselsystems hat Auswirkungen auf den Netzwerkoverhead, da nur Gruppenschlüsselsysteme Multicast- und Broadcast-Frames effizient zuweisen können, so dass ein Fluten von Multicast- und Broadcast-Frames über alle Verbindungen vermieden wird. IKE, das Schlüsselsystem von IPSec, hat in diesem Bereich deutliche Schwächen. Diese haben mehrere Anbieter dazu gebracht eigene proprietäre Schlüsselsysteme für IPSec zu entwickeln und zu vermarkten. Die meisten Layer 2-Verschlüssler verfügen

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

über eingebaute leistungsfähige Gruppenschlüsselsysteme mit integriertem Failover-Mechanismus.

3.2.2. Leistung

Die spezialisierten Appliances sind auf Leistung optimiert. Es besteht kein Wettbewerb der unterschiedlichen Funktionalitäten um die vorhandenen Ressourcen.
Integrierte Appliances sind auf spezifische Leistungsmerkmale optimiert, die aber selten parallel ausgenutzt werden können. Oft werden aus Kostengründen ASICs (Application Specific Integrated Circuit) statt FPGAs (Field Programmable Gate Array) eingesetzt, auf denen aber nur spezifische Funktionen implementiert sind. Werden Funktionen benutzt, die nicht hardwaremässig implementiert sind, so erfolgt deren Abarbeitung über Software und führt zu entsprechenden Leistungseinbussen. Erfolgt die ganze Verarbeitung auf einer CPU, so ist von vornherein die Leistung auf tiefe bis mittlere Bandbreiten beschränkt und Latenz und Jitter erhöht. Ist die CPU für den Verschlüssler dediziert, so ist die Leistungscharakteristik einschätzbar und konstant. Bei einer CPU, die verschiedenen Applikationen dienen muss – wie das regelmässig bei einer integrierten Appliance oder einer virtualisierten Umgebung der Fall ist – ist die jeweilige Leistungscharakteristik von der Auslastung durch andere Applikationen abhängig und somit variabel und unberechenbar.
Es ist aber auch möglich, dass es künftig integrierte Appliances geben wird, welche für die Verschlüsselung einen ASIC oder ein Subsystem mit eigenem FPGA verwenden. ASICs gibt es so z.B. für MACSec, doch sind die meist direkt auf der Netzwerkschnittstelle verbaut oder gar in den Netzwerkchip integriert. Zudem ist der interne Systemdurchsatz oft ungenügend, was das Ausnutzen der maximalen Netzbandbreite verunmöglicht. So ist der IMIX-Durchsatz einer ASIC-basierten Lösung eines führenden Netzwerkgeräteherstellers von vornherein auf 90% beschränkt.

FPGAs machen die Verschlüssler schnell, da alles in Hardware abgearbeitet wird: Die Latenz für Layer 2-Verschlüssler mit Hardwareunterstützung wird in Mikrosekunden ausgedrückt, während die software-basierte Verschlüsselung mit IPSec in Millisekunden gemessen wird. Zwischen Mikrosekunden und Millisekunden besteht ein Faktor von 1’000.

3.2.3. Erweiterbarkeit

Spezialisierte Layer 2-Verschlüssler sind in der Regel so dimensioniert, dass die Funktionalität zu einem späteren Zeitpunkt erweitert werden kann. So kann das Gerät dem aktuellen Stand der Technik angepasst werden. Für diesen Zweck muss der verwendete FPGA grosszügig dimensioniert sein, was wiederum die Kosten erhöht. Unterdimensionierte FPGAs sind hingegen schnell voll

und verursachen dadurch einen hohen Stromverbrauch, der auch zu hoher Wärmeentwicklung und Stabilitätsproblemen führt. Eine Anpassung an den aktuellen Stand der Technik ist bei solch unterdimensionierten FPGAs auch nur beschränkt möglich.
Erweiterbarkeit ist ein Kostentreiber und deshalb auf der Prioritätsliste der Entwickler von integrierten Appliances weit unten zu finden. Die Entwickler konzentrieren sich eher auf die initiale Kostenbegrenzung als auf die mittel- und langfristige Kosteneffizienz für den Kunden. Software-basierte reale und virtuelle Appliances sind ebenfalls problemlos erweiterbar, sind aber deutlich leistungsschwächer. Erweiterungen der Software-Funktionalität können diese Leistungsschwäche noch akzentuieren.

3.2.4. Kosten

Während integrierte Appliances wie Switches/Routers mit zusätzlicher Verschlüsselungshardware aufgrund der wegfallenden Kosten für Gehäuse, redundantes Netzteil, etc. günstiger in der Anschaffung sind, wird aus diesem Preisvorteil über die Zeit ein Preisnachteil. Die Lebensdauer einer integrierten Appliance liegt bei etwa 4-5 Jahren, während die spezialisierten Appliances regelmässig 7-8 Jahre eingesetzt werden. Die kürzere Lebensdauer hebt den initialen Kostenvorteil mehr als auf.
Ein anderer Aspekt, der oft vernachlässigt wird, ist die Herstellergebundenheit: Aufgrund der unterschiedlichen Schlüsselsysteme und des unterschiedlichen Leistungsumfangs sind Ethernet-Verschlüssler verschiedener Hersteller nicht untereinander kompatibel. Bei einer integrierten Lösung wirkt sich das zusätzlich auf die Switches/Routers aus. Wechselt man an einem Standort den Lieferanten der integrierten Appliance, so ist dieser Standort in Bezug auf die Verschlüsselung nicht mehr Teil des MANs/WANs. Der gleiche Hersteller muss an allen Standorten verwendet werden, was zu einer doppelten Herstellerbindung führt: Sowohl für die Verschlüsselung als auch für den Switch/Router. Auch die unterschiedlichen Varianten von MACSec sind untereinander nicht kompatibel. Ein Wechsel, z.B. von Cisco auf Juniper, HP, Avaya, Arista oder Huawei, ist dann verunmöglicht. Kosteneinsparungen durch Lieferantenwechsel fallen aus. Bei Verwendung spezialisierter Appliances fällt die Herstellerbindung in Bezug auf vorgeschaltete Switches und Router weg.

3.3. Operationelle Aspekte

3.3.1. Einfaches Installieren und Konfigurieren

Ethernet-Verschlüssler sind Höcker im Draht (bump-in-the-wire). Sie fügen sich problemlos in bestehende Netzwerke ein und werden einfach eingeschlauft. Eine Rekonfiguration des Netzwerks ist unnötig. Die Konfiguration ist je nach Anbieter einfach und schnell. Fehler sind dabei praktisch ausgeschlossen. Die Netzausfallzeit für die Installation ist auf ein Minimum reduziert. Bei IPSec ist das alles deutlich komplizierter, zeitaufwändiger und fehleranfälliger.
Integrierte MACSec-Lösungen sind zwar auch einfach zu konfigurieren, doch bieten sie nur einen Schutz der Kategorie Low Assurance.

3.3.2. Betriebsaufwand und Betriebskosten

Spezialisierte Ethernet-Verschlüssler brauchen kaum Unterhalt und haben deshalb den Ruf, in die Kategorie “Installieren & Vergessen” (deploy & forget) zu fallen. Sie führen ihre Arbeit im Hintergrund aus, ohne dabei die Leistungsfähigkeit des Netzwerks zu beeinträchtigen. Geringer Unterhalt ist gleichbedeutend mit geringerem Personalaufwand und geringeren Betriebskosten. Da sie alles von Layer 2 an aufwärts ohne eingebaute Leistungsbremsen schützen können ist es sinnvoller, Ethernet-basierte Site-to-Site- und Multi-Site-Netzwerke mit Ethernet-Verschlüsslern und nicht mit IPSec zu schützen. Das gleiche gilt für Layer 2.5 VPNs (MPLS), die auf Layer 2 verschlüsselt werden können, ohne dass dabei – im Gegensatz zur Verschlüsselung auf Layer 3 - ein Tunneln nötig ist.

Von Layer 2 aus besteht direkter Zugriff auf alle relevanten Netzwerkschichten (2-7). Das richtige Produkt erlaubt das Verschlüsseln aller Netzwerke, die über ein Ethernet MAN oder WAN betrieben werden: Ethernet, MPLS und IP. Und das Ganze ohne Tunneln und Einkapseln. Das Verschlüsseln von Ethernet-Netzwerken auf Layer 2 ist einfacher, sicherer und leistungsfähiger. Bei direkten Glasfaserverbindungen steht alternativ eine Verschlüsselung von OTN direkt auf Layer 1 zur Verfügung.

Auch für IP-Netzwerke steht die Verschlüsselung von IP-basierten Standortvernetzungen mittels eines Layer 2-Verschlüsslers unter Verwendung von Ethernet over IP (EoIP) zur Verfügung. In Kombination mit einem integriertem Gruppenschlüsselsystem und Verkehrsflussoptimierung besteht so eine sicherere und effizientere Alternative für GETVPN.

3.3.3. Kosteneinsparungspotential

Bei korrekter Strukturierung des Netzwerks und Verwendung eines guten Telekomanbieters können dank Linienkonsolidierung im Access-Bereich laufende Kosten eingespart werden. Da kaum ein Gebäude über mehr als zwei komplett redundante Netzwerkanbindungen verfügt, macht es aus operationeller und finanzieller Hinsicht nur in den seltensten Fällen Sinn, für mehr als zwei Anschlüsse zu bezahlen.

3.4. Sicherheitszertifikate: Schein oder Sein?

Sicherheitszertifikate gaukeln oft eine falsche Sicherheit vor. Die Hauptsünder sind dabei FIPS und Common Criteria. Es ist kein Zufall, dass ausgerechnet FIPS- und Common Criteria-zertifizierte Produkte von gewissen Organisationen ausgehebelt wurden und sich auch US-Behörden regelmässig über erfolgreiche Angriffe auf US-Regierungsnetzwerke beschweren. Für die FIPS-Zertifizierung gibt es unterschiedliche Klassen und unterschiedliche Prüfungsbereiche. Nur in den wenigsten Fällen handelt es sich um eine vollumfängliche Prüfung des ganzen Systems, sondern nur um die Prüfung des kryptographischen Moduls im Rahmen des Cryptographic Module Validation Program[22]. Ist ein solches Modul erst einmal zugelassen, dann muss das Produkt erst dann erneut validiert werden, wenn Änderungen vorgenommen werden oder es seit fünf Jahren unverändert auf dem Markt ist. Hingegen kommt es regelmässig vor, dass eine Zertifizierung bestehen bleibt, selbst wenn Schwachstellen bekannt sind, bekannt werden oder bekannt sein müssten[23]. Bei FIPS geht es weniger um Sicherheit, sondern vorwiegend um das Einhalten von Vorgaben. FIPS ist eine nationale Vorgabe für den Schutz von sensitiven Daten und Zugangsvoraussetzung für den amerikanischen und kanadischen Regierungsmarkt. Es handelt sich aber nicht um einen internationalen Sicherheitsstandard. Eine FIPS-Zertifizierung selbst ist noch kein vertrauenswürdiger Beleg für das Erfüllen aktueller Sicherheitsanforderungen. Das sehen nur die Anbieter von FIPS-zertifizierten Lösungen anders. Selbst im amerikanischen Regierungsmarkt gelten für den Schutz klassifizierter Daten strengere Anforderungen. Das Betreiben von Produkten im FIPS-Modus ist ein latentes Sicherheitsrisiko.

Bei Common Criteria wird die Einhaltung der Sicherheitsziele überprüft. Der Hersteller legt dabei die Sicherheitsziele selbst fest. Es scheint naheliegend, dass ein Hersteller die Sicherheitsziele so festlegt, dass er sie auch erfüllt. In einigen Bereichen gibt es vordefinierte Sicherheitsziele, aber nicht für Ethernet-Verschlüssler. Entsprechend gibt es auch keine offizielle Common Criteria-Zertifizierung für Ethernet-Verschlüssler auf internationaler Ebene. Die Her-

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

steller, die mit einer Common Criteria-Zertifizierung werben, haben nur ihre selbstdefinierten Ziele erfüllt. Es gibt mittlerweile ein Profil für MACSec-Ethernet-Verschlüsselung für Punkt-zu-Punkt-Verbindungen, das von der NIAP (National Information Assurance Program) im Auftrag der NSA erstellt wurde[24]. Es beschränkt sich aber auf MACSec, basiert vollumfänglich auf US-Standards und beinhaltet Vorgaben, welche mit grosser Wahrscheinlichkeit die Sicherheit beeinträchtigen. In Bezug auf US-Standards ist unter anderem sowohl die Verwendung von spezifischen NIST-Kurven als auch die Verwendung des für eine FIPS-Zulassung erforderlichen Zufallszahlengenerators nach NIST-Vorgaben vorgeschrieben. In Bezug auf Sicherheit sind mehrere essentielle Sicherheitsfunktionen nur optional. Und damit die Evaluation möglichst einfach ist, wird die Security Boundary mit der Device Boundary gleichgesetzt, die Sicherheit des Netzwerkgeräts als gegeben angenommen und auf eine eingehende Prüfung verzichtet. Nur so ist den wirtschaftlichen Interessen amerikanischer Hersteller Genüge getan.

Es gibt aber durchaus Zertifikate, die halten, was sie versprechen: Geprüfte Sicherheit. Dazu gehört die Zulassung eines Produktes durch das deutsche Bundesamt für Sicherheit in der Informationstechnologie (BSI) für den Schutz von klassifizierten Daten. Die Prüfung umfasst das ganze System mit sämtlichen Implementierungsdetails, inklusive Source Code der Software und der Hardware. Nicht evaluierbare ASIC-Lösungen erhalten deshalb keine Zulassung. Jede Änderung erfordert eine neue Evaluierung. Erfolgt nach längstens fünf Jahren keine Änderung am Produkt, so wird die Zulassung widerrufen. Das BSI beschränkt die Gültigkeit einer Zulassung auf weniger auf fünf Jahre, wenn das Produkt Algorithmen und Schlüssellängen verwendet, die das BSI nur noch für den gewährten Zeitraum als genügend einstuft oder wenn das Produkt sonstige potentielle Schwachstellen (beispielsweise in der Benutzerschnittstelle) enthält, die in naher Zukunft ausgenutzt werden könnten.

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

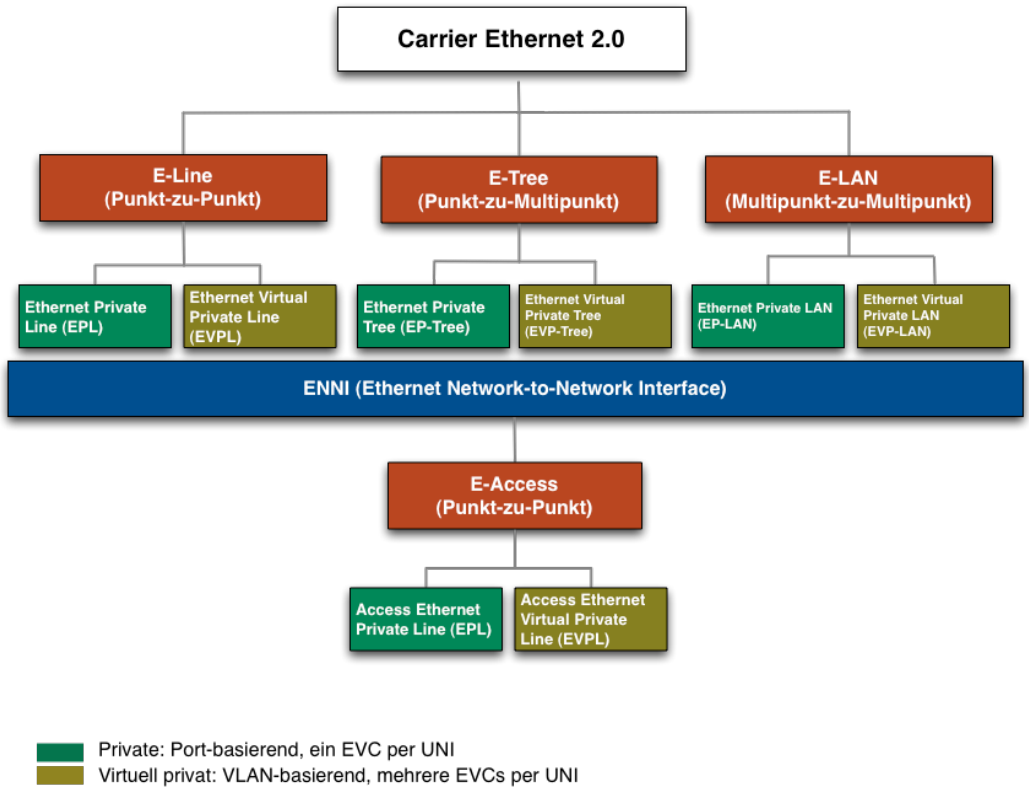
High Assurance Network Encryption

4. Ethernet für regionale und Weitverkehrsnetze: Carrier Ethernet 2.0

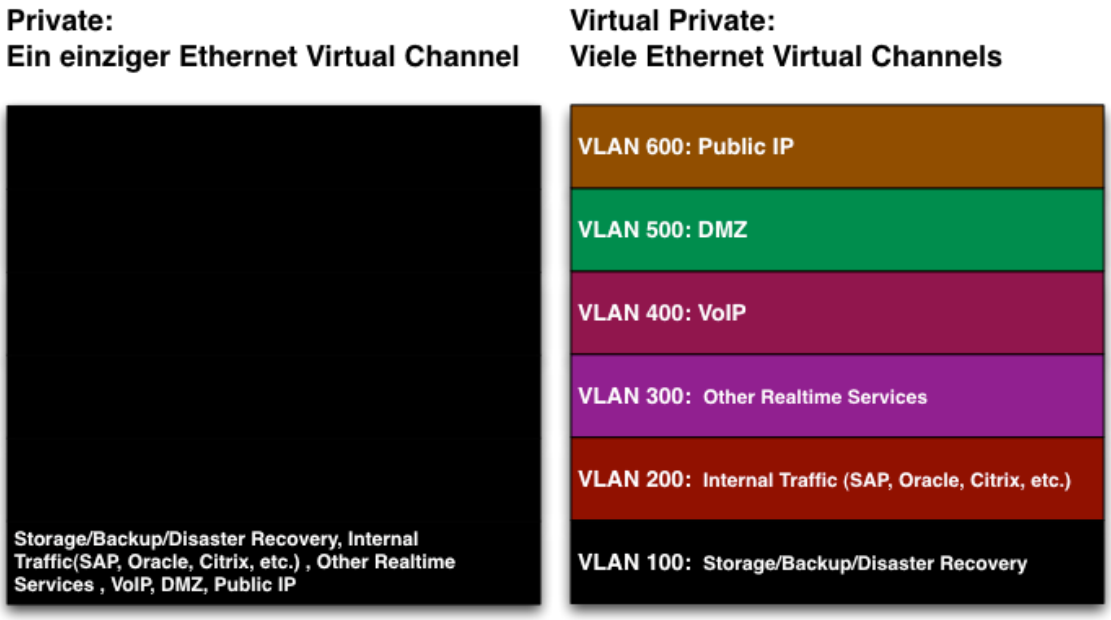
Ethernet ist ursprünglich ein Standard für lokale Netzwerke, der von der IEEE definiert und weiterentwickelt wird. Carrier Ethernet baut zwar darauf auf, ist aber auf die Erfordernisse von regionalen Netzwerken (MAN) und Weiterverkehrsnetzwerken (WAN) ausgelegt. Verantwortlich für die relevanten Standards ist das Metro Ethernet Forum (MEF). Regionale und Weitverkehrsnetzwerke unterscheiden sich deutlich von lokalen Netzwerken und hat entsprechende Auswirkungen auf die Anforderungen an Verschlüssler. Was innerhalb eines lokalen Netzwerkes oder für eine reine Punkt-zu-Punkt-Verbindung noch relativ einfach ist, wird nun relativ komplex, da die unterschiedlichsten Szenarien unterstützt werden müssen.

4.1. Carrier Ethernet: Zugang und Topologien

Das Metro Ethernet Forum (MEF) hat drei unterschiedliche Topologien für regionale und Weitverkehrnetze definiert und standardisiert. Das ursprüngliche Szenario war auf einen einzelnen Telekomanbieter beschränkt, der dem Kunden sämtliche Zugänge und Netzwerkdienstleistungen anbot. Das erwies sich vor allem bei Weitverkehrsnetzwerken als wenig praxistauglich. Deshalb wurde eine standardisierte Schnittstelle zwischen den Ethernet-Services verschiedener Telekomanbieter definiert. Das Ethernet-Network-to-Network-Interface (ENNI) standardisiert die Interkonnektivität zwischen Carrier Ethernet-Netzwerken.

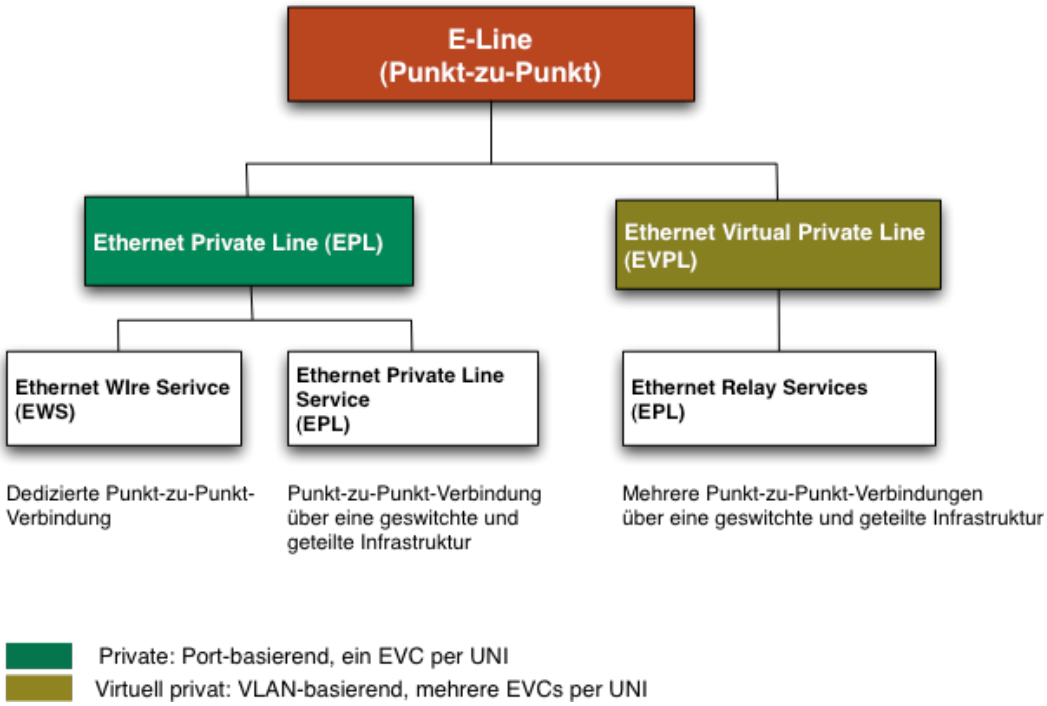


Carrier Ethernet unterscheidet zwischen „privaten“ und „virtuell privaten“ Topologien. Die port-basierten Varianten – sie stützen sich auf die Sender- und Empfängeradressen der beteiligten Geräte – sind auf einen einzigen Ethernet Virtual Channel (EVC) beschränkt. Sämtliche Frames, ob mit oder ohne Tag werden einer VLAN-ID zugewiesen und auf einen einzigen Ethernet Virtual Channel (EVC) abgebildet. Die VLAN-basierten virtuell privaten Varianten unterstützen hingegen eine Vielzahl von VLANs und EVCs. Jeder EVC kann mehrere VLANs beinhalten solange diese die gleiche Dienstgüte (Class of Service(CoS) verwenden. Dies gewährt deutlich mehr Flexibilität und erlaubt – im Zusammenspiel mit ausgeklügelten Gruppenschlüsselsystemen – die kryptographische Trennung von Subnetzwerken. Die erhöhte Flexibilität einer solchen Kombination erweitert die Einsatzszenarien bei gleichzeitiger Senkung der Betriebskosten.



4.2. E-Line (Punkt-zu-Punkt)

Bei der E-Line stehen drei unterschiedliche Varianten zur Verfügung:



Die Hauptunterscheidung ist zwischen port-basierten und VLAN-basierten Verbindungen (Privat Line vs. Virtual Line). Die port-basierten Verbindungen sind zusätzlich differenziert in dedizierte und geteilte Linien.

Auf einem Netzwerkdiagramm präsentieren sich die Topologien wie folgt:

4.2.1. Ethernet Private Line Service

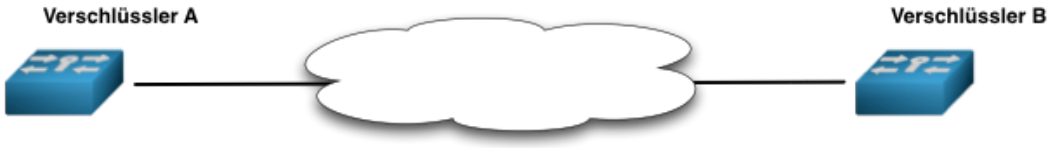
Ethernet Private Line Service bietet eine direkte Linie zwischen den beiden Verschlüsslern. Diese basiert entweder auf einer eigenen Glasfaser oder auf xWDM.

Da sich zwischen den beiden Verschlüsslern keine aktiven Netzwerkkomponenten befinden, bildet der Ethernet Private Line Service ein Hop-to-Hop-Szenario. Obwohl in diesem sämtliche Verschlüsselungsmodi (Frame, Transport, Tunnel) funktionieren, ist aus Sicherheitsüberlegungen der bevorzugte

Verschlüsselungsmodus für dieses Szenario der authentisierte Frame-Modus. Kombiniert mit Traffic Flow Security bietet er eine robuste Grundlage für die Verbindungen, bei welchen die Priorität auf dem Vermeiden von Frame-Overhead liegt und diese Anforderung höher gewichtet wird als der Verlust der Authentisierung. Auch im Frame-Modus steht in der Regel eine authentisierte Verschlüsselung zur Verfügung, die Replay- und Integritätsschutz zur Verfügung stellt.
Alternativ steht hier auch die authentisierte OTN-Verschlüsselung auf Layer 1 als effiziente Möglichkeit zur Verfügung.

4.2.2. Ethernet Wire Service

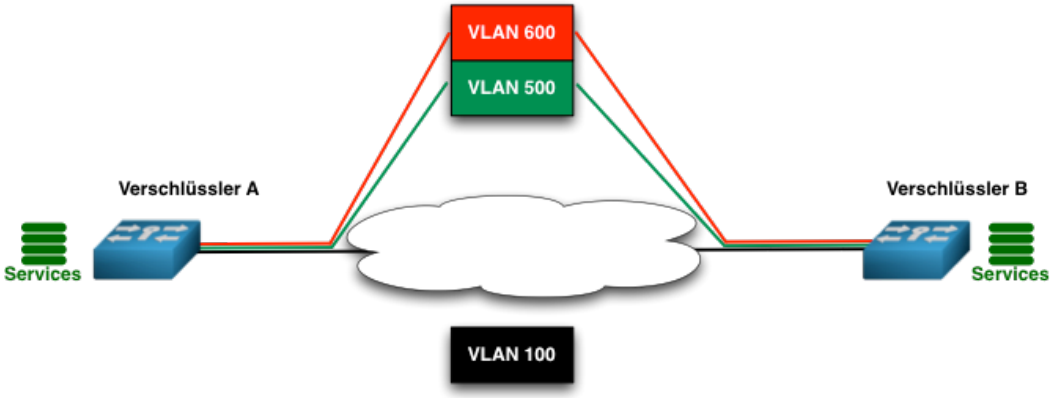
Im Gegensatz zum Ethernet Private Line Service benutzt der Ethernet Wire Service eine geteilte Infrastruktur. Diese Infrastruktur kann aus unterschiedlichen Elementen bestehen: Von einer reinen Layer 2-Netzwerk-Cloud bis zu einer Mischung aus Layer 2- und Layer 3-Netzwerk-Cloud. Ethernet Wire Service ist auf einen einzigen Service beschränkt. Der gesamte Datenverkehr wird gleich behandelt und verschlüsselt. Eine Differenzierung basierend auf VLAN-IDs ist nicht möglich.



Da sich bei dieser Topologie aktive Elemente zwischen den beiden Verschlüsslern befinden, ist die Auswahl an Verschlüsselungsmodi auf Transport und Tunnel beschränkt.

4.2.3. Ethernet Virtual Private Service

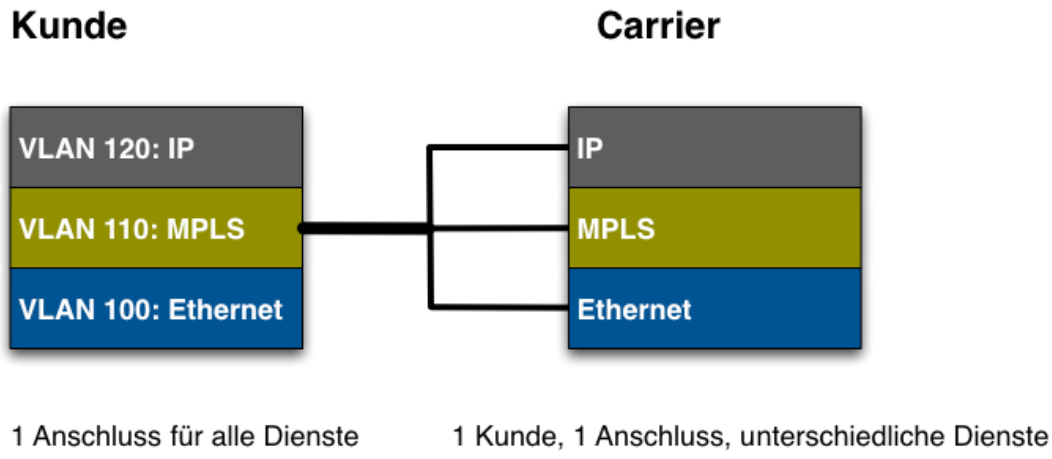
Der VLAN-basierte Ethernet Virtual Private Service stellt mehrere Dienste pro Leitung zur Verfügung. Unterschiedliche Dienste können unterschiedlichen VLANs zugewiesen werden. Dies bringt mehrere Vorteile mit sich. So kann beispielsweise die Verschlüsselung einer Ethernet-Verbindung zwischen zwei Standorten, während andere VLANs Verbindungen zum privaten IP-Netzwerk und dem öffentlichen Internet bringen.



Auch bei dieser Topologie sind aktive Netzwerkkomponenten zwischen den beiden Verschlüsslern vorhanden. Dies beschränkt die verfügbaren Verschlüsselungsmodi auf Transport und Tunnel. Um einen Ethernet Private Line Service abzusichern, muss der Verschlüssler selektive Verschlüsselung basierend auf VLAN-IDs unterstützen.

4.3. E-Access

Der Zugang zu einem Datennetzwerk über einen Ethernet-Anschluss über einen lokalen Anbieter wird als E-Access bezeichnet. Die Schnittstelle zum Ethernet-Netzwerk des Telekomanbieters, die auch als „User Network Interface (UNI)“ bezeichnet wird, muss so nicht zwangsläufig vom Telekomanbieter zur Verfügung gestellt werden, der das regionale oder Weitverkehrnetzwerk betreibt. Es erlaubt das Verwenden eines lokalen Anbieters, der dann die Verbindung zum regionalen oder Weitverkehrsnetzwerk herstellt. E-Access ist die lokale Auffahrrampe für eine Vielzahl von möglichen Services (Ethernet, MPLS, IP, etc.). Stellt der Anbieter des regionalen und Weitverkehrsnetzwerkes gleichzeitig auch den lokalen Anschluss, so wird die ganze Dienstleistung von einem einzigen Anbieter erbracht. Dies ist aber oft nur für den lokalen oder nationalen Bereich möglich. Die lokale Auffahrrampe bringt mehrere Vorteile mit sich. Einer davon ist die Konsolidierung von Anschlusslinien bei gleichzeitigem Beibehalten sämtlicher Dienste. Da Gebäude fast nie über mehr als zwei komplett redundante Anschlüsse an redundante Telekomnetzwerke verfügen bringt eine Vielzahl von physischen Anschlüssen an das Telekomnetzwerk nicht viel. Ein Anschluss mit 10G ist in diesem Fall letztlich genauso redundant wie zehn separate Anschlüsse mit je 1G.



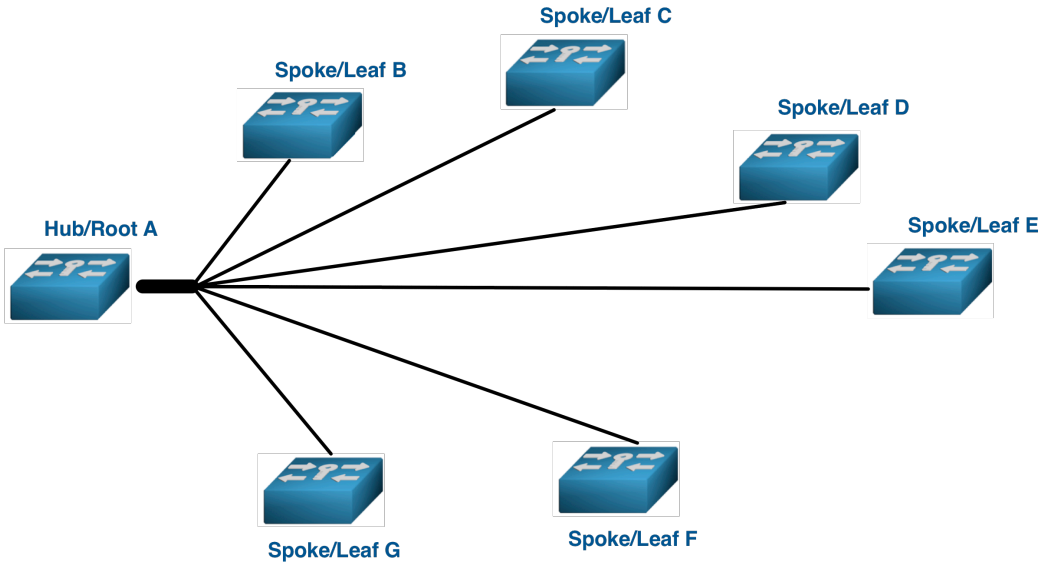
Die Konsolidierung von Anschlusslinien kann zu merkbaren Kosteneinsparungen führen. Nicht nur bei den Leitungskosten, sondern auch bei den Verschlüsslern. Für hohe Bandbreiten sind in der Regel die Kosten pro Megabit deutlich günstiger als für tiefe Bandbreiten. Voraussetzung ist aber ein Telekomanbieter, der bei sich die unterschiedlichen Zuweisungen von VLAN-ID auf Netzwerktypen machen kann.

4.4. E-Tree (Punkt-zu-Multipunkt)

Punkt-zu-Multipunkt-Topologien werden häufig auch als „Hub & Spoke“ oder als „Rooted Multipoint“ bezeichnet. E-Tree kommt in zwei Varianten: „Private“ ist port-basierend, während „virtual private“ auf VLAN-IDs aufbaut. Auch hier erlaubt die virtuell private Variante mehrere Ethernet Virtual Channels (EVC) auf einem einzelnen Port.
Für den privaten E-Tree gibt es technisch auch die Lösung, den Port des Hubs zu virtualisieren und so innerhalb eines einzelnen Ethernet Virtual Channels mehrere separate Punkt-zu-Punkt-Verbindungen aufzubauen. Aufgrund mangelnder Skalierbarkeit und Flexibilität ist dieser Ansatz aber suboptimal und vorzugsweise auf kleine Netzwerke beschränkt.
Für beide Varianten gilt: Ein Hub/Root darf nur mit anderen Hub/Root und mit jedem der Spoke/Leaf getrennt kommunizieren, während die Spoke/Leaf nur mit Hub/Root, aber nicht mit anderen Spoke/Leaf direkt kommunizieren dürfen.

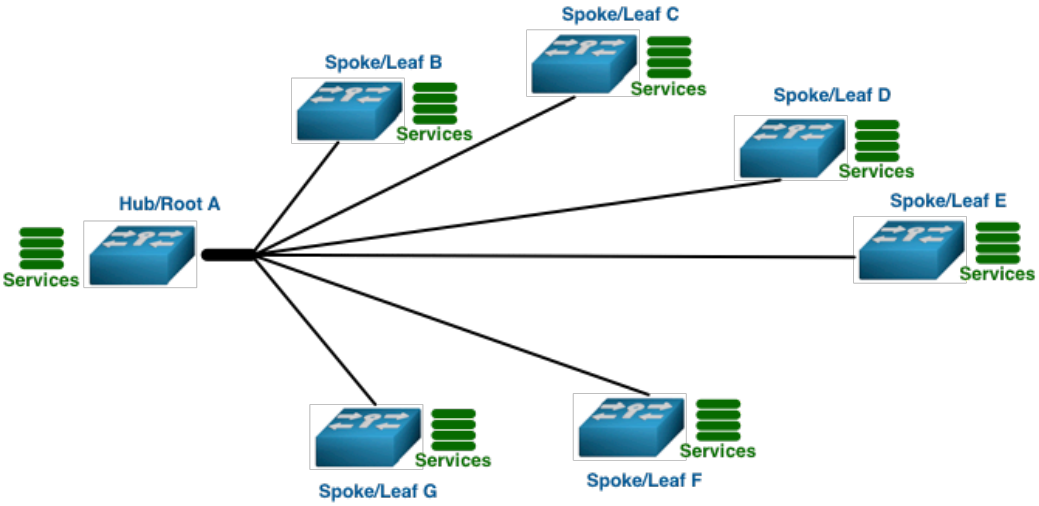
4.4.1. Ethernet Private Tree (EP-Tree)

Für den EP-Tree gilt: Ein Ethernet Private Tree kann sowohl über dedizierte wie auch über geteilte Linien betrieben werden. Dedizierte Linien sind vorwiegend in regionalen Netzwerken anzutreffen, da sich die Kosten in der Regel nach Distanz und Bandbreite berechnen. Das Metro Ethernet Forum hat keine Topologie speziell für die Verwendung von E-Tree über dedizierte Linien definiert.

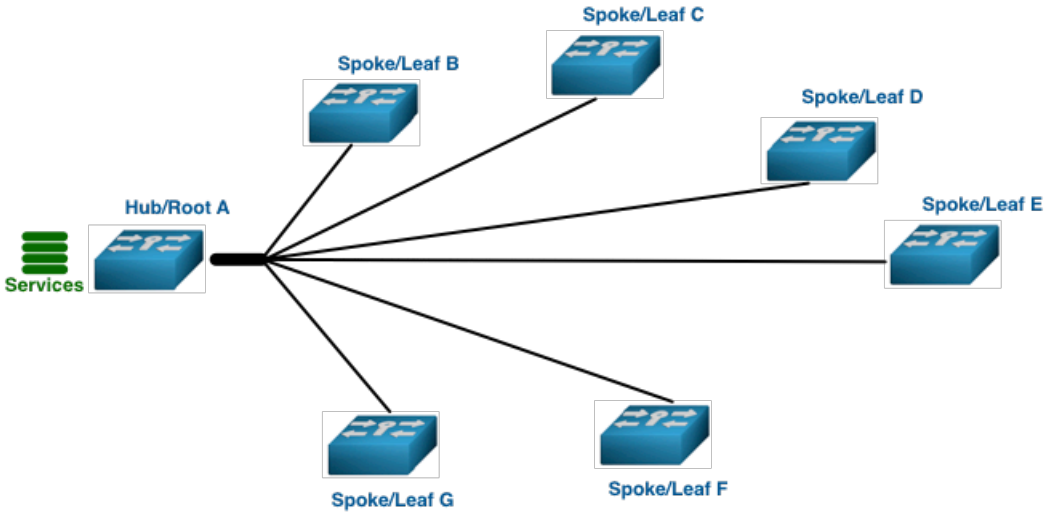


4.4.2. Ethernet Virtual Private Tree (EVP-Tree)

Der EVP-Tree ist deutlich flexibler als der EP-Tree. Die logische Trennung nach VLAN-ID gekoppelt mit der Unterstützung mehrerer Services pro Anschluss erlaubt die Linienkonsolidierung an allen Anschlüssen.



Eine weitere Möglichkeit ist, nur Hub/Root mit mehreren EVCs auszustatten, so dass nur Hub/Root mit anderen Hub/Root und direkt mit der Aussenwelt kommunizieren können.



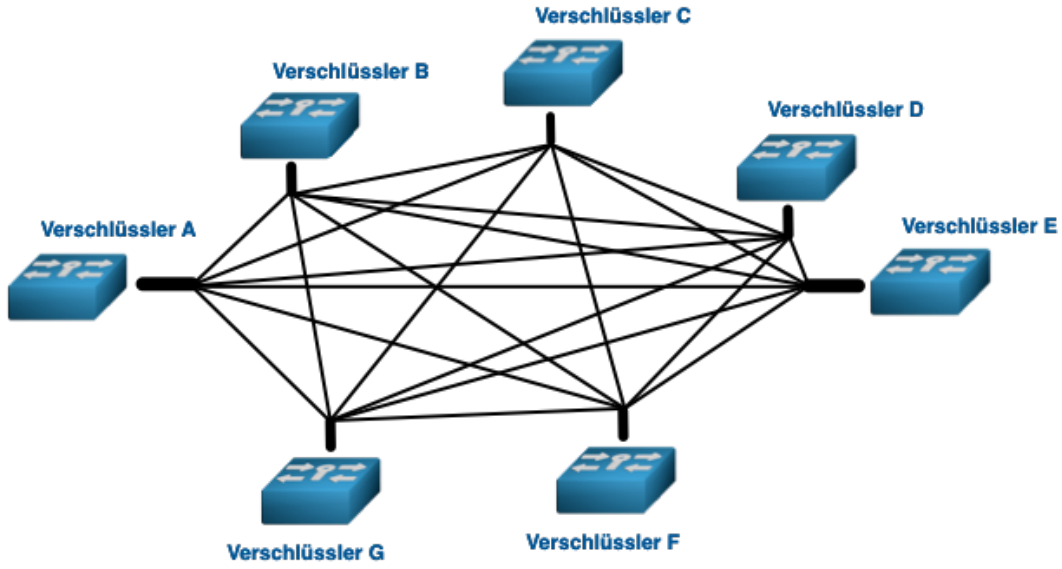
Auf den Diagrammen ist zwar jeweils nur ein einzelner Hub/Root abgebildet, doch ist es durchaus auch möglich mehrere Hub/Root zu verwenden.

4.5. E-LAN (Multipunkt-zu-Multipunkt, Mesh)

E- LAN erlaubt die Kommunikation von jedem innerhalb des Netzwerks mit jedem anderen innerhalb des Netzwerks. Deshalb wird eine solche Topologie oft auch als „Mesh“ bezeichnet.

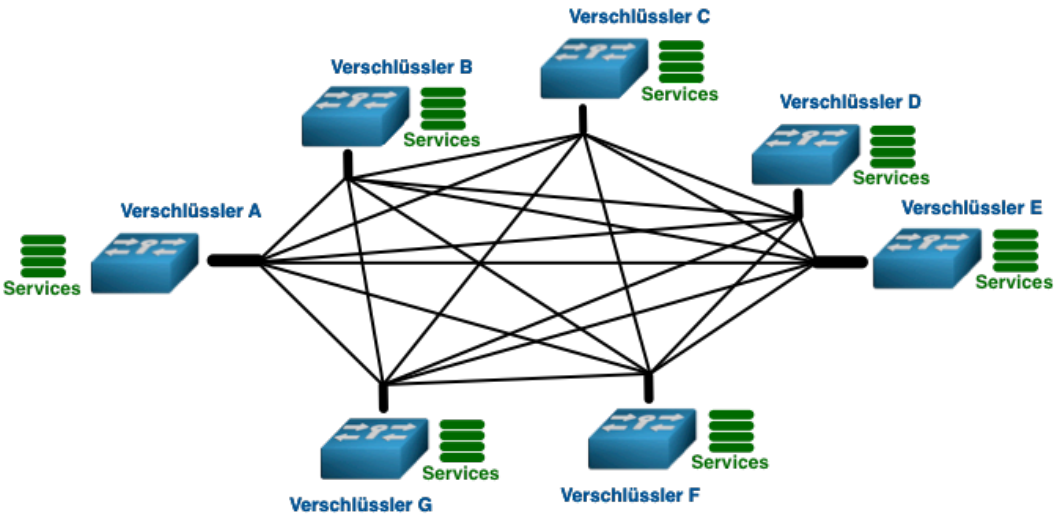
4.5.1. Ethernet Private LAN (EP-LAN)

Ein Ethernet Private LAN lässt sich sowohl über dedizierte Linien wie auch über eine geteilte Infrastruktur betreiben. Vor allem bei Weitverkehrsnetzen sind die Kosten für dedizierte Linien prohibitiv, da die gesamte nötige Redundanz des Netzwerks auf Kosten des Kunden geht und die Zahl der nötigen Verbindungen mit jedem zusätzlichen Standort überproportional steigt. Das Metro Ethernet Forum hat auch keine spezielle Topologie für E-LAN über dedizierte Linien definiert.



4.5.2. Ethernet Virtual Private LAN (EVP-LAN)

Das Ethernet Virtual Private LAN unterstützt am User Network Interface (UNI) mehrere, durch VLAN-IDs getrennte Services. Multipunkt-zu-Multipunkt ist nur einer dieser Services. Er erlaubt die Kommunikation jedes Standorts mit jedem anderen Standort. Abhängig vom verwendeten Schlüsselsystem und der Schlüsselzuweisung erlaubt es eine EVP-LAN-Topologie, alle unterschiedlichen LAN-Topologien Punkt-zu-Punkt, Punkt-zu-Multipunkt, Multipunkt-zu-Multipunkt) parallel abzubilden.



Virtual Private E-LAN bietet mit Abstand die grösste Flexibilität in Bezug auf Einsatzszenarien und Konfigurationsmöglichkeiten. Die volle Nutzung der gebotenen Möglichkeiten setzt ein geeignetes Gruppenschlüsselsystem voraus, das die selektive Verschlüsselung nach VLAN-ID und die kryptographische

die selektive Verschlüsselung nach VLAN-ID und die kryptographische Trennung nach VLAN-ID beherrscht.

Layer 2-Verschlüssler sichern Standortverbindungen ab und machen das vorzugsweise transparent. Bei der Verbindung von Standorten über Carrier Ethernet lassen sich sowohl Layer 3-Netzwerke als auch Layer 2-Netzwerke absichern. Speziell bei Layer 2-Netzwerken muss darauf geachtet werden, dass ein Problem an einem Standort andere Standorte nicht in Mitleidenschaft zieht. VLANs, die sich über mehrere Standorte erstrecken können zum Problemfall werden. Kritisch ist vor allem das Auftreten eines Bridging Loops, der zu einer Flutung führt, die sich dann über alle beteiligten Standorte propagiert. Dazu kommen noch Problematiken, die sich aus einer hohen Anzahl an MAC- und IP-Adressen innerhalb eines überdimensionierten VLANs ergeben können[252627].
Ein Layer 2-Verschlüssler für Carrier Ethernet schützt die Verbindung zwischen Standorten. Solche Verbindungen lassen sich sowohl mittels Router (Layer 3) als auch mittels Switch (Layer 2) terminieren. Eine interne Terminierung auf Layer 3 ist in der Regel die bessere Lösung[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**

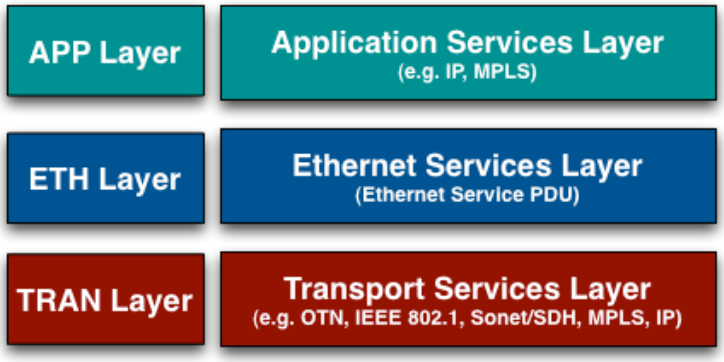
gemalto
security to be free

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

5. Carrier Ethernet: Dreischichtenmodell und Transportnetzwerke

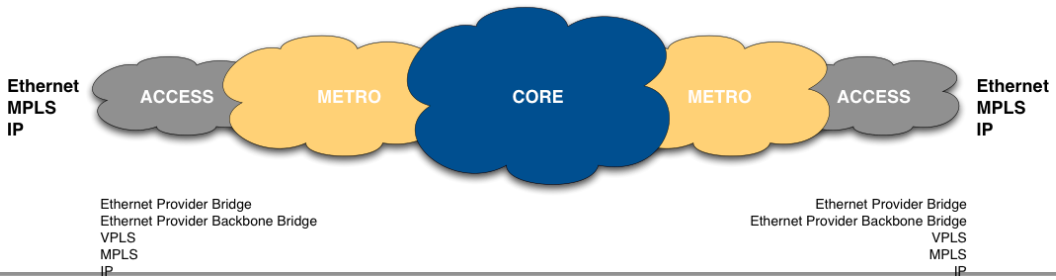
5.1. Das Dreischichtenmodell

Carrier Ethernet verwendet ein dreischichtiges Modell, wobei sich die standard-definierende Organisation, das Metro Ethernet Forum (MEF), auf die mittlere Schicht – den Ethernet Services Layer – konzentriert.



Das Dreischichtenmodell zeigt die Umgebung, in welcher ein Verschlüssler seine Arbeit verrichten können sollte. IEEE 802.1 (Ethernet) ist nur eine von vielen möglichen Transportmöglichkeiten und die Netzwerkprotokolle aus dem Application Services Layer können wiederum auch als Transportschicht dienen. Die volle Unterstützung und Absicherung von Carrier Ethernet-basierten Netzwerken ist komplex.

Jede der Metro und Carrier-Ethernet-Topologien benötigt ein Transportnetzwerk, das die jeweiligen Voraussetzungen erfüllt. Native Ethernet-Transportnetzwerke finden sich vorwiegend im Access- und Metro-Bereich, doch wird oft auch bereits da ein anderes Transportnetzwerk verwendet. Verbreitet sind OTN, MPLS, IP und teilweise noch Sonet/SDH. Der Begriff „Carrier Ethernet“ umfasst jedes Transportnetzwerk, das für den Transport von Ethernet-Frames benutzt wird. Die verwendeten Transportnetzwerke innerhalb eines MANs oder WANs sind meistens nicht homogen. Abhängig von der Platzierung des Verschlüsslers und des verwendeten Transportnetzwerks wird der originale Ethernet-Frame enkapsuliert oder getunnelt. Der ausgelieferte Ethernet-Frame ist aber identisch mit dem gesendeten Ethernet-Framet.



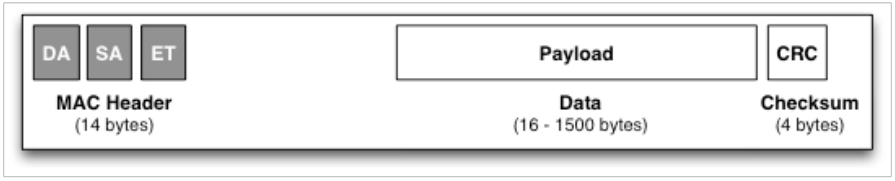
5.2. Natives Ethernet und Pseudowires

Native Ethernet-Netzwerke sind durch die IEEE 802.3 Standards definiert. Sie sind eigentlich das, was man gemeinhin als Ethernet-Netzwerke bezeichnet. Je nach verwendetem IEEE 802.3 Standard ist der Ethernet-Frame mehr oder weniger informationshaltig. Je grösser und je öffentlicher das Netzwerk, desto informationshaltiger sind in der Regel die Frames.
Im Gegensatz zu nativen Netzwerken sind die Pseudowires keine physischen Netzwerkverbindungen, sondern nur logische. Die Ethernet-Frames werden als Nutzlast auf dem Transportnetzwerk übermittelt, das die physische Netzwerkverbindung zur Verfügung stellt. Die gebräuchlichsten Formate auf dem Transport Services Layer sind MPLS (oft in der MPLS-TP-Variante), OTN und IP.

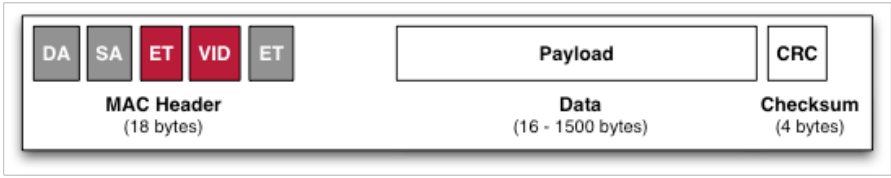
5.2.1. Native Ethernet-Formate

Native Ethernet Frame-Formate hängen vom jeweiligen Netzwerk und der Position im Netzwerk ab. Auf der Kundenseite (Customer Edge) sieht das anders aus als auf der Carrier-Seite (Provider Edge).

Auf der Kundenseite findet man vorwiegend „normale“ Ethernet II-Frames und Ethernet II-Frames mit VLAN-Tag. Bei einem Ethernet-Transportnetzwerk sehen die Frames – ohne Verschlüsselung - bei der Übergabe an das MAN/WAN folgendermassen aus:



Ethernet II Frame

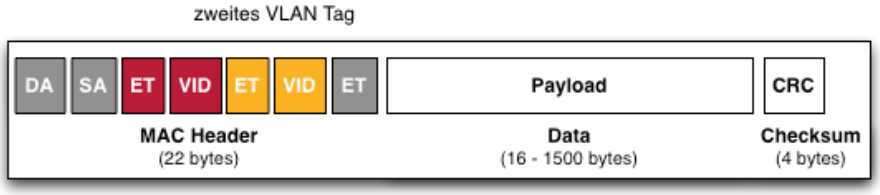


Ethernet II Frame mit VLAN –Tag

Dies sind die beiden häufigsten Frame-Formate auf der Kundenseite. Es kommt aber durchaus aus vor, dass bereits auf Kundenseite zur besseren Strukturierung des Netzwerks mit zwei VLAN-Tags versehen sind.

Auf der Carrier-Seite wird der Frame um Zusatzinformationen erweitert, so dass unter anderem die nötige Skalierbarkeit in Bezug auf die Adressen gewährt

ist.



QinQ: Ethernet II Frame mit hierarchischen VLAN-Tags (IEEE 802.1Q)

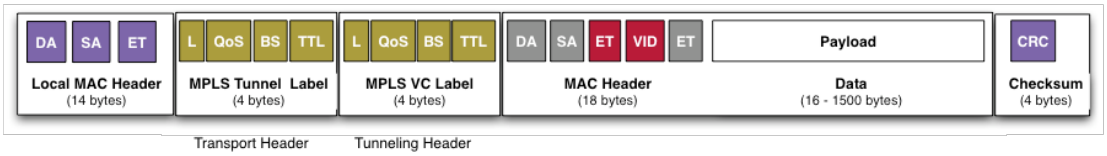
Mac-in-Mac: Ethernet II-Frame über Ethernet getunnelt (IEEE 802.1ah)

Bei QinQ (auch als PB – Provider Bridge bezeichnet) wird auf der Carrier-Seite ein zusätzliches VLAN-Tag hinzugefügt, während bei Mac-in-Mac (auch als Provider Backbone Bridge bezeichnet) der Original-Frame über Ethernet getunnelt wird. Dies kann durchaus auch sequentiell erfolgen. Diese Frame-Erweiterungen auf Carrier-Seite sind nur temporär während des Transports über das Carrier-Netzwerk. Der Kunde sieht und merkt davon nichts.

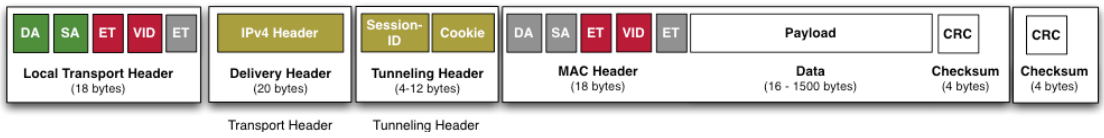
http://en.wikipedia.org/wiki/Ethernet
http://en.wikipedia.org/wiki/IEEE_802.1Q
http://en.wikipedia.org/wiki/IEEE_802.1ah (Mac-in-Mac)

5.2.2. Pseudowires

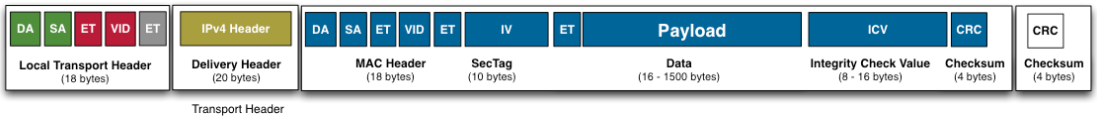
Ein Pseudowire ist die Emulation eines verbindungsorientierten Layer 2-Dienstes über ein paketorientiertes Netzwerk. Der Originalframe ist auf dem Pseudowire nur Nutzlast, benutzt also ein anderes Transportnetzwerk als sein eigenes. Oft handelt es sich dabei um eine Kombination von Ethernet, OTN, Sonet/SDH, IP und MPLS. Für den Kunden ist dieser Teil des Carrier Ethernets voll transparent: Er bekommt vom Carrier einen Ethernet-Anschluss mit garantierten Leistungseigenschaften und sieht nichts als sein Ethernet.
Es gibt allerdings Szenarien, in denen der Verschlüssler selbst einen Pseudowire erstellen muss. Am häufigsten betrifft das einzelne Verbindungen innerhalb eines Ethernet-MANs oder -WANs, die nur über ein IP-Netzwerk transportiert werden können. In solchen Fällen verschlüsselt der Verschlüssler den Ethernet-Frame und versieht ihn mit einem IP-Header. So kann die Verschlüsselung effizient auf Layer 2 erfolgen.
Die beiden gebräuchlichsten Formate sind Ethernet über MPLS (EoMPLS) und Ethernet über IP (EoIP).



Frame Ethernet über MPLS (EoMPLS)



Frame Ethernet über IP (L2TPv3)



Frame verschlüsseltes Ethernet über IP

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

Auch Pseudowires sind Angriffen ausgesetzt:

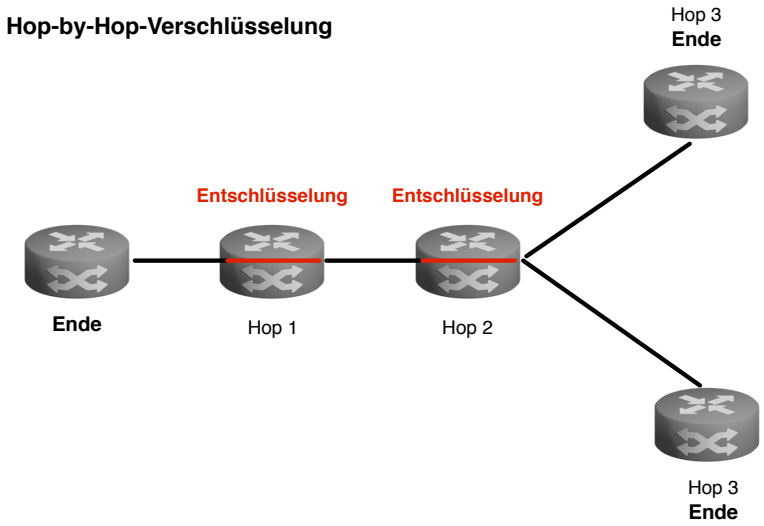
https://www.ernw.de/download/ERNW_MPLS-Carrier-Ethernet.pdf
https://www.blackhat.com/presentations/bh-europe-09/Rey_Mende/BlackHat-Europe-2009-Mende-Rey-All-Your-Packets-wp.pdf
http://www.blackhat.com/presentations/bh-europe-09/Rey_Mende/BlackHat-Europe-2009-Mende-Rey-All-Your-Packets-slides.pdf

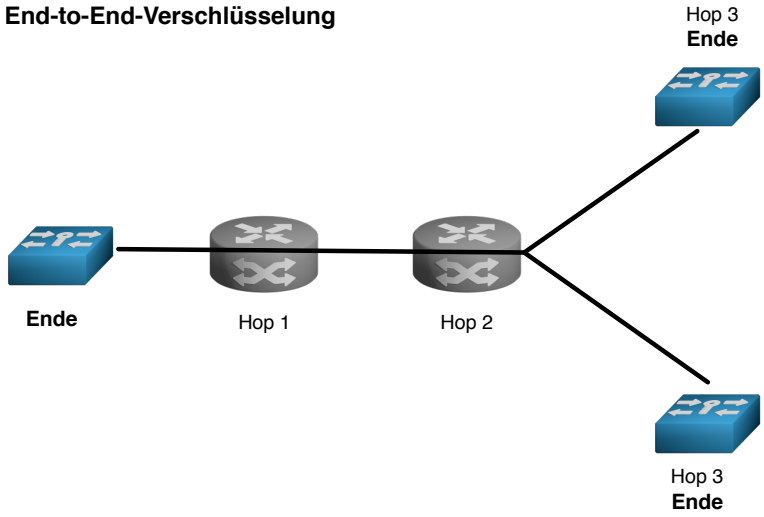
6. Positionierungsvarianten für Verschlüssler

Ethernet-Verschlüssler sichern Verbindungen zwischen Standorten ab. Als Standort gilt ein Datencenter, eine Firmenzentrale, ein Fabrikationsbetrieb, eine Filiale und jede andere Art von Standort, der mit den anderen Standorten über ein MAN oder ein WAN verbunden und integriert werden soll. Ein solches Netzwerk kann auch Private und Community Clouds beinhalten. Die Verschlüssler werden häufig direkt an der Schnittstelle zwischen dem lokalen Netzwerk und dem Telekomanbieternetzwerk positioniert. Die gezeigten Positionen sind logischer Natur und haben Auswirkung auf die Anforderungen an den Verschlüssler.

6.1. Hop-by-Hop vs. End-to-End

Die Flexibilität bei der Positionierung wird massgeblich durch das verwendete Grundprinzip und durch die Funktionalität des Verschlüsslers in Bezug auf konditionelle Verschlüsselung und konditionelles Verschlüsselungsoffset bestimmt. Bei einer Hop-by-Hop-Verschlüsselung werden die Daten bei jedem Hop entschlüsselt, in unverschlüsselter Form verarbeitet und dann wiederum verschlüsselt zum nächsten Hop weitergesendet. Anders sieht es bei einer End-to-End-Verschlüsselung aus, bei der die Daten während der gesamten Übertragung zwischen Absender und Ziel gesichert bleiben auch wenn sich dazwischen Hops befinden.

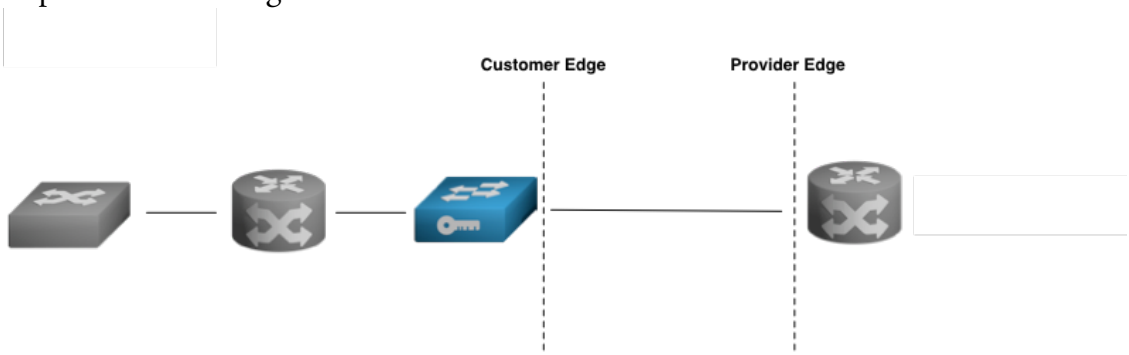




Während in einem lokalen Netzwerk eine Hop-by-Hop-Verschlüsselung vorteilhaft sein kann, ist sie für MAN- und WAN-Umgebungen nur dann einsetzbar, wenn der nächste effektive Hop gleichzeitig auch das andere Verbindungsende ist. Der Einsatzbereich und die Flexibilität von Hop-by-Hop-Verschlüsselungslösungen sind deshalb stark eingeschränkt. Mittels Tunneln kann lässt sich zwar eine Angrenzung herstellen, doch ist das zwangsweise Tunneln sowohl in Bezug auf Overhead wie auch auf Latenz keine gute Lösung. End-to-End-Verschlüsselung ist effizienter und flexibler.

6.2. Zwischen Customer Edge (CE) und Provider Edge (PE)

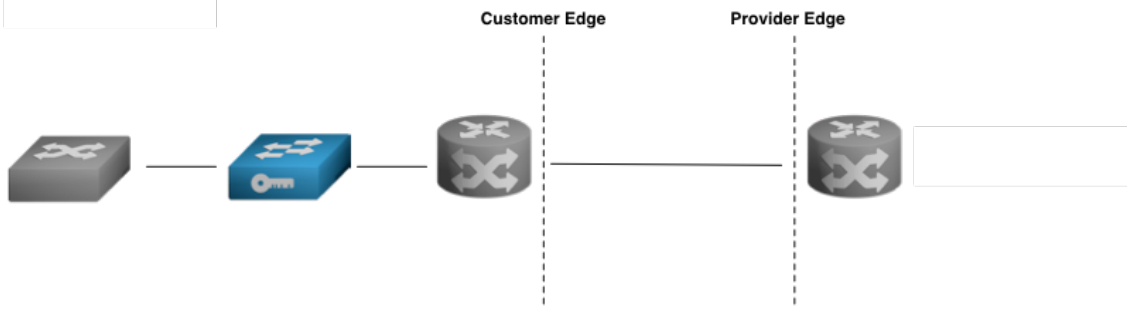
Dies ist das mit Abstand häufigste Szenario. Der Verschlüssler bildet die Grenze zwischen dem lokalen Netzwerk und dem Netzwerk des Telekomanbieters. Schon bei diesem einfachen Szenario zeigt sich die Problematik von Hop-by-Hop-Verschlüsselung:



Der erste Hop, d.h. die erste aktive Netzwerkkomponente nach dem Verschlüssler, ist ein Gerät des Telekomanbieters und dieses möchte man nicht unbedingt in das eigene Netzwerk miteinbeziehen. Ebenfalls nicht in Frage kommt, dass die gesamten Daten auf diesem Gerät in unverschlüsselter Form vorliegen.

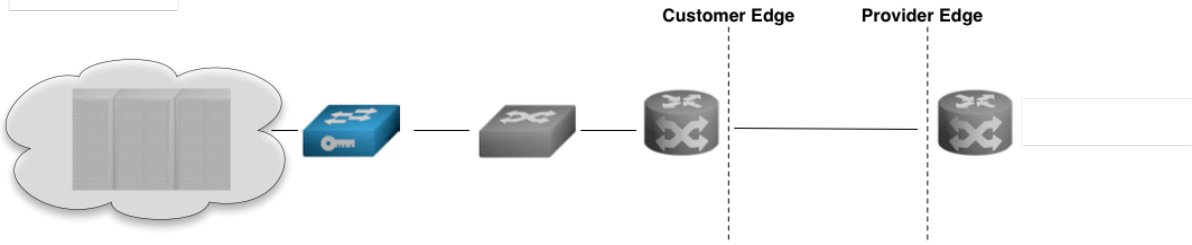
6.3. Zwischen Customer (C) und Customer Edge (CE)

Die Absicherung lässt sich auch weiter in das lokale Netzwerk schieben.

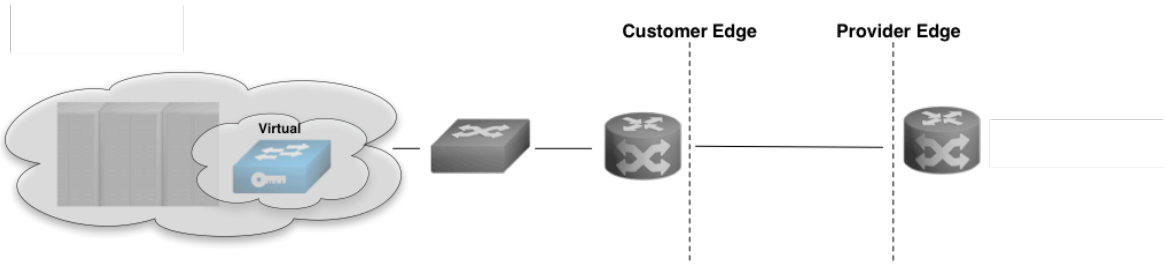


6.4. Zwischen Cloud Customer und Customer Edge (CE)

Die Absicherung der Verbindung mit einer Private oder Community Cloud lassen sich Verschlüssler auch direkt vor der Cloud positionieren.



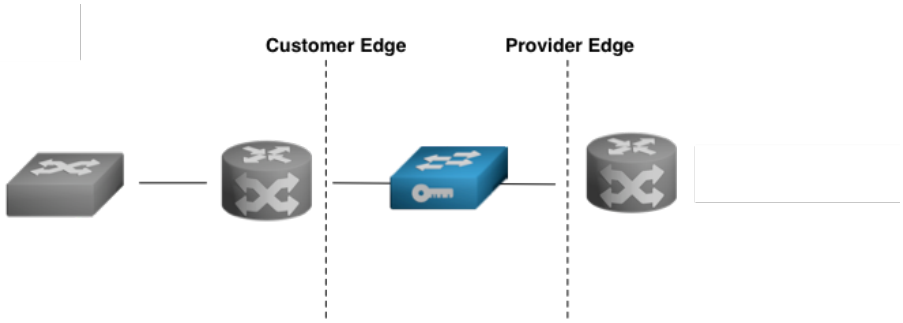
6.5. Innerhalb einer Cloud



Das Absichern mittels einer virtuellen Appliance innerhalb einer Cloud wird nur in ganz speziellen Szenarien verwendet. In einer virtualisierten Umgebung ist die Sicherheit der Schlüssel nur in beschränktem Umfang vorhanden. Ohne zusätzlichen Schutz liegen sämtliche Schlüssel in der virtuellen Appliance zugriffsbereit vor. Einigermassen Abhilfe schaffen zwei Möglichkeiten: (1) Das Ausstatten der Cloud-Hardware mit einer lokalen sicheren Aufbewahrungsmöglichkeit wie einer Smartcard, und (2) das Mitverwenden eines echten Verschlüsslers als Hardware Security Module (HSM) für virtuelle Appliances. Die Problematik der Verwendung eines Schlüssels im Klartext zum Verschlüs-

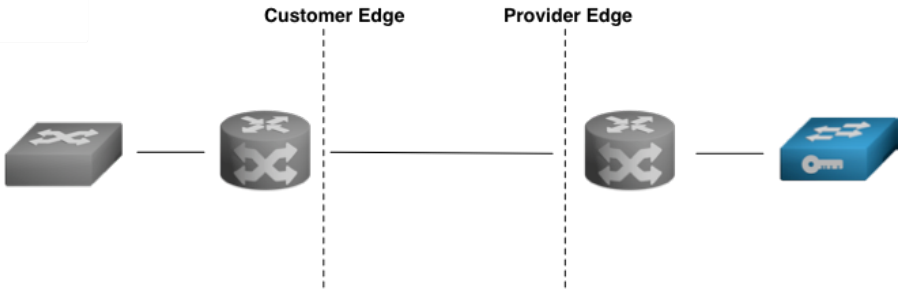
seln in einer unsicheren Umgebung bleibt aber auch in diesem Fall vorhanden.

6.6. Zwischen Provider Egde (PE) und Customer Edge (CE)



Dieses Szenario kommt vorwiegend in zwei unterschiedlichen Anwendungen vor: Einerseits beim Verschlüsseln von MPLS-Netzwerken auf Layer 2, wenn der Kunde seine eigenen Routing-Tabellen verwendet und andererseits wenn die Verschlüsselung als Managed Service vom Telekomanbieter bezogen wird.

6.7. Zwischen Provider Edge (PE) und Provider (P)

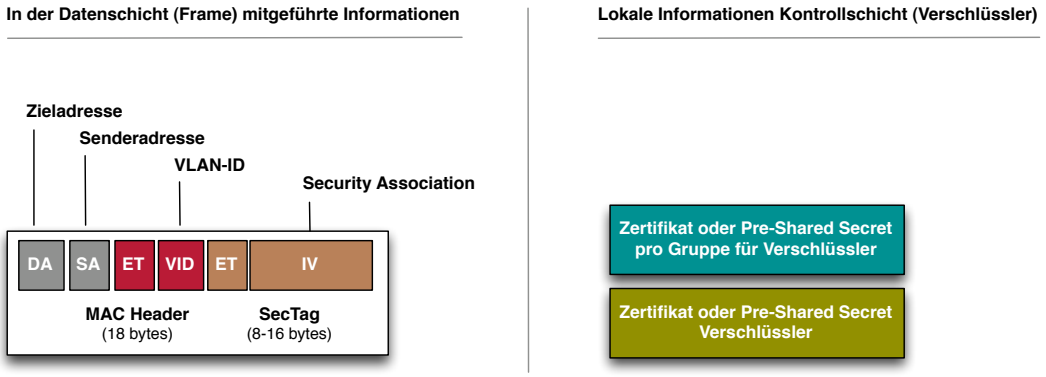


Dieses Szenario kann ebenfalls auftreten, wenn die Verschlüsselung als Managed Service vom Telekomanbieter bezogen werden. Da die Daten bis zum Verschlüssler komplett ungeschützt sind, macht ein solches Szenario nur selten Sinn.

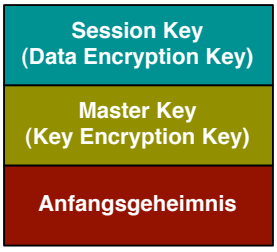
7. Schlüsselverwaltung, Schlüsselsysteme, Schlüsselzuweisung und Netzwerktopologien

7.1. Schlüsselverwaltung

Die Schlüsselverwaltung kümmert sich um die Erstellung, Austausch, Lagerung und Zuweisung der Schlüssel. Sie ist mehrschichtig und setzt voraus, dass auf den Verschlüsslern ein Anfangsgeheimnis vorhanden ist. Das vorverteilte Anfangsgeheimnis ist Basis für die Authentisierung und den Schlüsselaufbau.

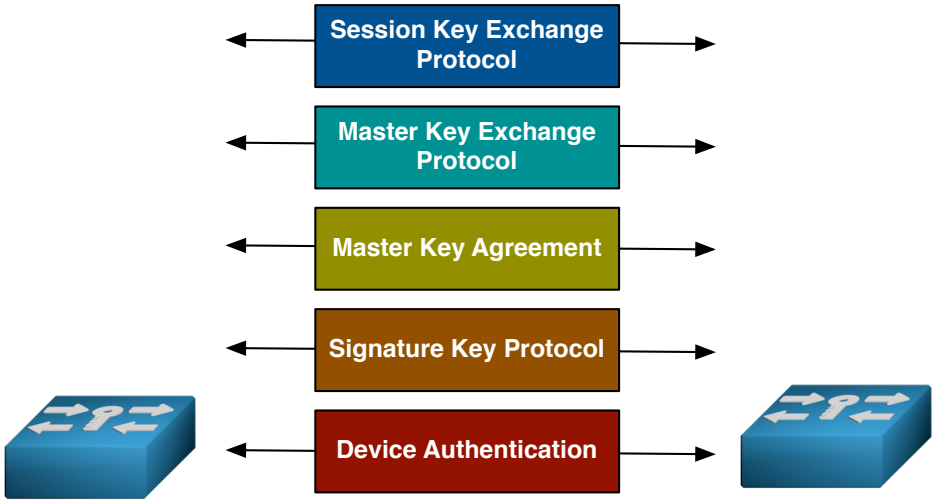


Vereinfacht dargestellt braucht es für Verschlüsselung ein Anfangsgeheimnis zur Authentifizierung und Signatur, einen Master Key (Key Encryption Key) zum Verschlüsseln des Session Key (Data Encryption Key) und einen Session Key zum Verschlüsseln der Daten.

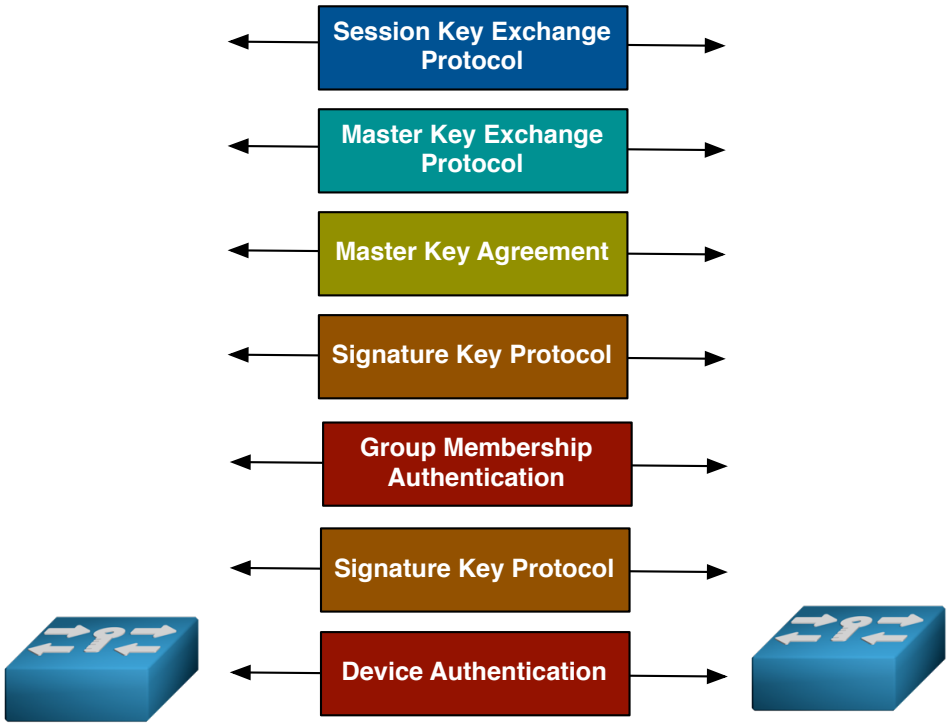


Zuerst muss etabliert werden, wer mit wem kommunizieren darf. Ist die Connectivity Association erstellt, so braucht es zusätzlich eine Security Association, die festlegt, wie die beiden Beteiligten sicher miteinander kommunizieren. Dafür wird ein Anfangsgeheimnis benötigt. Dabei kann es sich um einen Pre-Shared-Key oder ein Zertifikat handeln. Bei Verwendung von elliptischen Kurven gehört auch die Kurven-Domain dazu.

Vom Anfangsgeheimnis bis zum Session Key laufen mehrere komplexe Prozesse ab, die sowohl in sich selber wie auch in der Abfolge sicher sein müssen.



Noch eine Stufe komplexer ist es bei der Verwendung von Gruppenschlüsselsystemen, da nicht nur das Gerät sondern auch die Gruppenmitgliedschaft authentifiziert werden muss. Dafür braucht es ein zusätzliches gruppenspezifisches Anfangsgeheimnis.



Bei Gruppenschlüsselsystemen ist darauf zu achten, dass nebst der Geräteauthentifizierung und der entsprechenden Connectivity und Security Association zusätzlich pro Gruppe eine zusätzliche Connectivity und Security Association besteht.

Die erste Schwierigkeit besteht darin, das Anfangsgeheimnis sicher auf die si-

chere Hardware zu bekommen.

7.2. Anfangsgeheimnis, Authentifizierung und Signaturprotokoll

Für eine Kommunikation braucht es mehr als eine Partei. Die beteiligten Verschlüssler müssen sich deshalb gegenseitig finden, erkennen und authentifizieren. Als Basis dienen Zertifikate (asymmetrisches Verfahren) oder Pre-Shared Secrets (symmetrisches Verfahren).

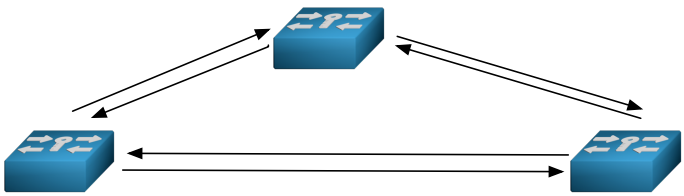
http://en.wikipedia.org/wiki/Shared_secret
http://en.wikipedia.org/wiki/X.509

Bei Pre-Shared Secrets kann die Authentifizierung entweder per Verschlüsslerpaar, per Netzwerk oder per Gruppe aufgesetzt werden.

Für die Authentifizierung stehen unterschiedliche Möglichkeiten zur Verfügung. So wird oft eine port-basierte Netzwerkzugriffkontrolle auf Basis von IEEE 802.1x verwendet. Sie setzt allerdings einen zusätzlichen externen Authentisierungsserver voraus, der Protokolle wie RADIUS und EAP unterstützt. Dies ist die gebräuchliche Vorgehensweise bei zertifikatsbasierten Systemen. Man sollte dabei beachten, dass die Sicherheitsstufe dieser Infrastruktur zumindest demjenigen des Verschlüsslers entsprechen sollte.
Als verbreitete Alternative gibt es die integrierte Netzwerkzugriffskontrolle, die ohne zusätzliche externe Dienste und Server auskommt und auf einer Kombination von Access Control Lists, vorverteilten Geheimnissen und zusätzlichen Authentifizierungsmechanismen beruht.

Ist dies erfolgt, so besteht zwischen den beteiligten Verschlüsslern jeweils eine Connectivity Association. Sie dürfen und können miteinander kommunizieren.

Connectivity Association



Geräte dürfen miteinander kommunizieren

Authentisierung via Certificate oder Pre-shared Secret/Pre-shared Key

Ist die Connectivity Association erstellt, so braucht es zusätzlich eine Security Association, die festlegt, wie die beiden Beteiligten sicher miteinander kommu-

nizieren.

Pre-Shared Secret respektive Zertifikat dienen auch zur Signatur, mit welcher der Absender verifiziert werden kann. Mit ihnen unterschreiben die Schlüsselaustauschverfahren die ausgetauschten Schlüssel oder Teilschlüssel um sicherzustellen, dass sie auch von der richtigen Gegenstelle stammen.

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

Die Signatur in Kombination mit dem entsprechenden Signaturprotokoll ist Basis für den Schlüsselaustausch.

7.3. Schlüsselaustausch

Für den Schlüsselaustausch kommen sowohl symmetrische wie auch asymmetrische Verfahren in Frage.

7.3.1. Symmetrischer Schlüsselaustausch

Bei einer symmetrischen Vorgehensweise sind alle Schlüssel direkt voneinander abgeleitet. Zuerst wird beim Verschlüssler ein Pre-Shared-Secret eingegeben. Der Master Key wird intern im Verschlüssler erzeugt und mit dem Shared Secret verschlüsselt. Der Session Key wird ebenfalls vom Verschlüssler erstellt und mit dem Master Key verschlüsselt. Master- und Session Key werden jeweils in der verschlüsselten Form über die Leitung zum anderen Verschlüssler übertragen. Das grosse Problem bei dieser Vorgehensweise liegt darin, dass wenn das Shared Secret irgendwann bekannt wird, jede früher aufgezeichnete Kommunikation entschlüsselt werden kann. Der Vorteil liegt in der geringen Komplexität und der damit verbundenen hohen Sicherheit gegen Angriffe und Analysen.

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

7.3.2. Asymmetrischer Schlüsselaustausch

Bei einer asymmetrischen Vorgehensweise werden die Teilschlüssel vollständig im Verschlüssler generiert, ohne dass der Benutzer einen Zugriff darauf hätte. Aus den jeweils ausgetauschten Teilschlüsseln berechnen beide Seiten jeweils das gleiche Shared Secret. Im Gegensatz zu einem symmetrischen Verfahren

kennt hier niemand das Shared Secret. Der Verschlüssler erzeugt anschliessend intern den Master Key und verschlüsselt ihn mit dem Shared Secret. Auch der Session Key wird vom Verschlüssler erstellt. Als Schlüssel für den Schlüsselaustausch dient der Master Key. Die Übertragung der Master- und der Session-Keys von einem Verschlüssler zum andern erfolgt immer in verschlüsselter Form.

Als asymmetrische Verfahren werden primär Diffie-Hellman und RSA eingesetzt. Diffie-Hellman verwendet in der Standardvariante das so genannte „diskrete Logarithmus Problem". Dieses Verfahren benötigt aber bei entsprechender Sicherheit sehr lange Teilschlüssel. Gleiches gilt auch für RSA. Moderne Systeme verwenden deshalb Diffie-Hellman mit Elliptic Curve Crypto System (ECC). Dies bietet bei wesentlich kürzeren Teilschlüsseln eine höhere Sicherheit bietet und gilt heute als Standard. Doch gelten nicht alle elliptischen Kurven als gleich sicher. Insbesondere die Sicherheit der NIST-Kurven wird in Fachkreisen als zweifelhaft eingestuft. Trotzdem beschränken sich US-Standards und die meisten Anbieter auf die Unterstützung der NIST-Kurven. Sicherheitsorientierte Lösungen lassen dem Kunden die Wahl zwischen NIST-Kurven, Brainpool-Kurven und anderen Kurven wie Safecurves und eigenen Kurven. Das Erstellen elliptischer Kurven ist hochkomplex, vor allem, wenn sie sicher sein müssen. Zwischen den verschiedenen Kurven bestehen Geschwindigkeitsunterschiede, doch sind diese bei Standortvernetzungen vernachlässigbar.

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

Asymmetrische Verfahren unterschreiben die ausgetauschten Teilschlüssel um sicherzustellen, dass sie auch von der richtigen Gegenstelle stammen. Dies kann entweder durch Zertifikate (X.509) kombiniert mit entsprechenden Verfahren (RSA, DSA oder ECDSA) oder durch Verschlüsselung des Teilschlüssels mit einem Pre-Shared Secret erfolgen.

7.3.3. Austauschfrequenz

Je häufiger der verwendete Session Key geändert wird, desto geringer ist die Wahrscheinlichkeit, dass er geknackt wird oder ein Replay-Angriff Folgen haben kann. Die Sicherheit des Schlüssels hängt dabei nicht nur von der Vertraulichkeit, sondern auch von den verwendeten Verfahren und den gewählten Parametern ab. So spielen die Länge des Counters und des ICV eine Rolle. Im Counter-Modus muss z.B. der Schlüssel gewechselt werden, bevor sich der

Zählerstand wiederholet. Deshalb ist es wichtig, dass der Session Key vom System automatisch nach einer bestimmten Anzahl Minuten gewechselt wird. Der verwendete Wert wird aus der übertragenen Datenmenge, insbesondere der Anzahl Frames, abgeleitet. Das gleiche gilt für den Key Encryption Key (Master Key), der für die Verschlüsselung des Session Key verwendet wird. Da dieser weniger Daten verschlüsselt, ist die Wechselfrequenz entsprechend tiefer. Auch dieser Schlüssel sollte automatisch ausgewechselt werden können.

Schlüsseltyp	Wechselfrequenz
Session Key (Data Encryption Key)	alle 1 - 60 Minuten
Master Key (Key Encryption Key)	alle 1 -24 Stunden
Anfangsgeheimnis	alle 12 - 24 Monate

7.4. Schlüsselsysteme

Ethernet-Frames gibt es in drei Grundvarianten, welche jeweils durch die Anzahl Zielrechner bestimmt sind:

- Unicast für die Kommunikation von einer mit einer einzelnen anderen MAC-Adresse
- Multicast für die Kommunikation von einer mit mehreren MAC-Adressen
- Broadcast für die Kommunikation von einer mit allen anderen MAC-Adressen

Es stehen unterschiedliche Ansätze zur Verfügung, um sicherzustellen, dass nebst Unicast-Frames auch Multicast- und Broadcast-Frames verschlüsselt werden.

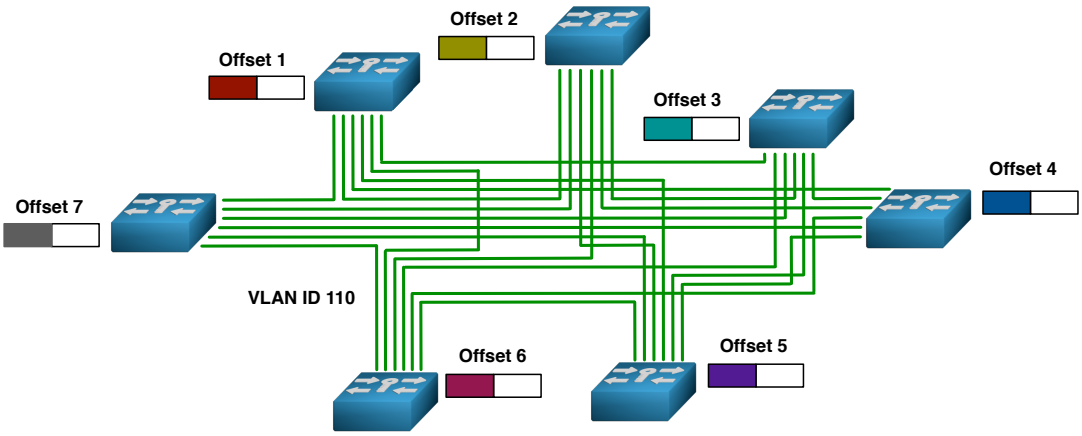
Bei der Schlüsselverwaltung kann man grob zwischen zwei unterschiedlichen Lösungsansätzen unterscheiden: Paarweise Schlüssel und Gruppenschlüssel.

Für paarweise Schlüsselsysteme besteht ein Netzwerk aus einer Mehrzahl von Punkt-zu-Punkt-Verbindungen. Jeder Verschlüssler ist mit jedem anderen Verschlüssler Punkt-zu-Punkt verbunden. Traditionelle paarweise Schlüsselsysteme verwenden jeweils den gleichen unidirektionalen Schlüssel für die Verbindung zwischen zwei Verschlüsslern.

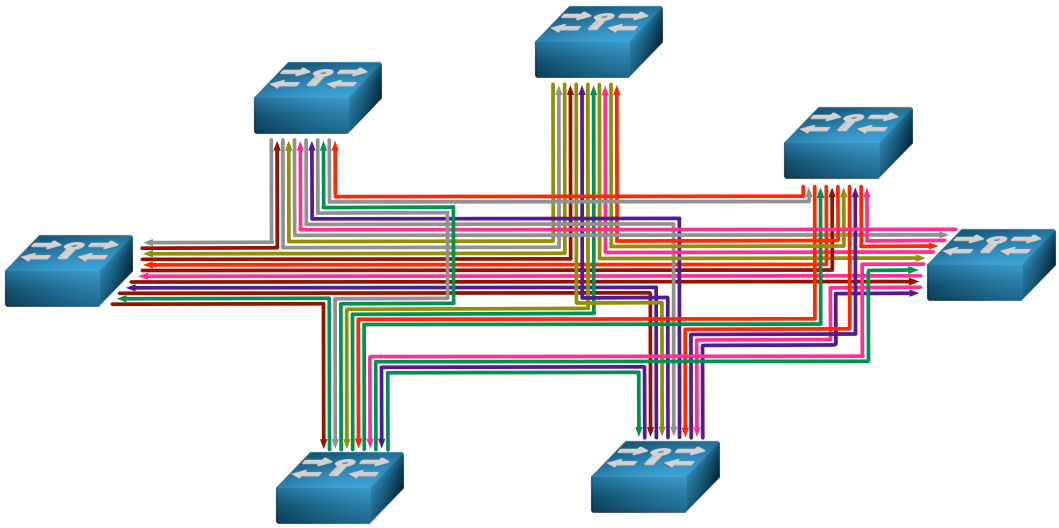
Gruppenschlüssel orientieren sich hingegen an der Zugehörigkeit zu einer Gruppe und verwenden jeweils einen unterschiedlichen Schlüssel pro Gruppe. Eine Gruppe kann beispielweise aus einem VLAN oder mehreren VLANs be-

stehen. Für die Kommunikation innerhalb einer Gruppe wird unabhängig vom Verschlüssler jeweils der gleiche Schlüssel verwendet. Ein Verschlüssler kann mehrere Gruppen unterstützen. Für jede Gruppe verwendet er einen unterschiedlichen Schlüssel. Gruppenschlüssel können bidirektional und unidirektional ausgelegt sein.

Bei bidirektionalen Gruppenschlüsseln verwenden alle Gruppenmitglieder den gleichen Schlüssel für sämtlichen Netzwerkverkehr innerhalb der Gruppe.



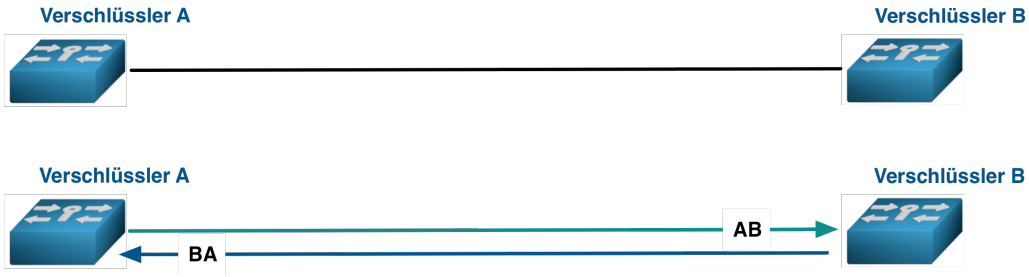
Bei unidirektionalen Gruppenschlüsseln wird hingegen ein Gruppenschlüssel nur für den ausgehenden Netzwerkverkehr von einem Verschlüssler an die anderen Gruppenmitglieder verwendet. Jedes Gruppenmitglied verwendet einen eigenen Gruppenschlüssel für den ausgehenden Netzwerkverkehr an die Gruppenmitglieder.



7.5. Paarweise Schlüssel

7.5.1. Punkt-zu-Punkt

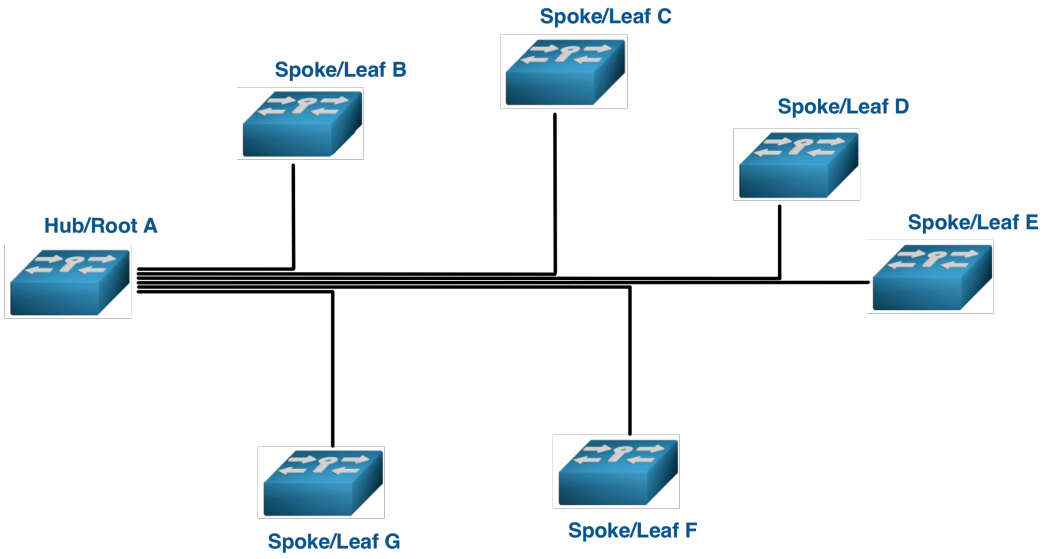
Für ein paarweises Schlüsselsystem entsprechen Punkt-zu-Punkt-Verbindungen einer Leitung, deren Endpunkte durch die beiden Verschlüssler A und B definiert sind.



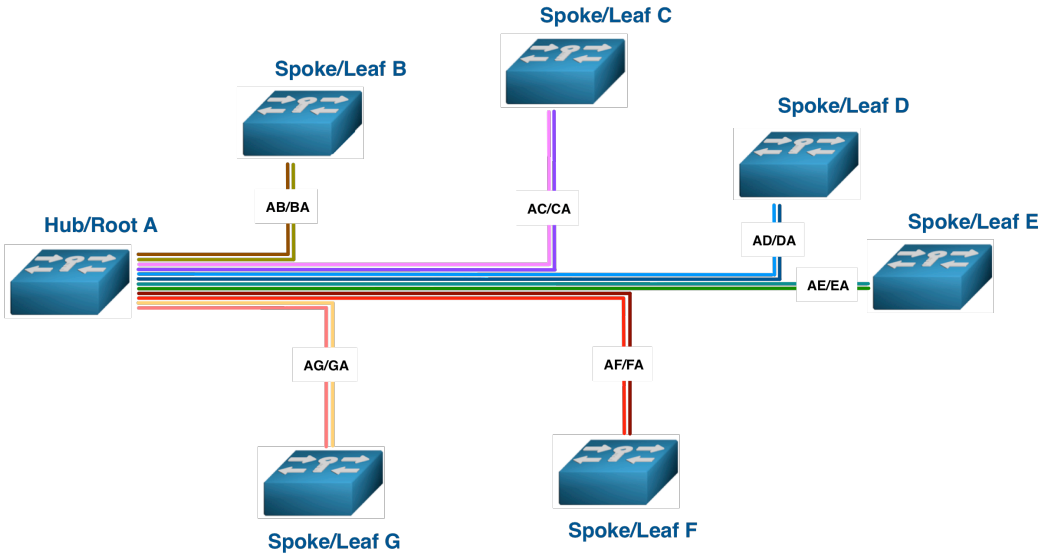
Für die Verschlüsselung der Daten von A nach B wird der Schlüssel AB verwendet. In der Gegenrichtung, von B nach A, der Schlüssel BA. Für reine Punkt-zu-Punkt-Verbindungen ist dieser Ansatz der gebräuchlichste.

7.5.2. Punkt-zu-Multipunkt

Punkt-zu-Multipunkt-Verbindungen entsprechen mehreren Punkt-zu-Punkt-Verbindungen. Sie haben einen gemeinsamen Ausgangspunkt, sind aber voneinander unabhängig. Auf der einen Seite (Hub) hat es einen Endpunkt und auf der anderen Seite (Spokes) hat es mehrere Endpunkte. Nur der Hub kann mit den Spokes kommunizieren und die Spokes nur mit dem Hub. Eine Kommunikation zwischen den Spokes ist nicht möglich.



Für jede Verbindung zwischen Hub und Spokes gibt es ein eigenes Schlüsselpaar.



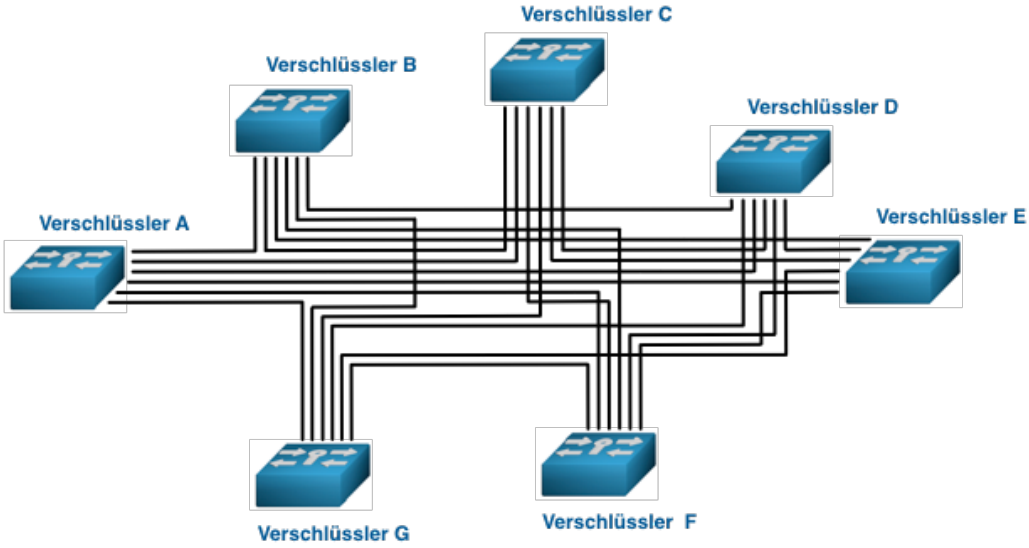
Die Zuweisung des richtigen Schlüssels auf die Frames erfolgt meistens unter Zuhilfenahme von MAC-Tabellen. In diesen sind sowohl die lokalen wie auch die entfernten MAC-Adressen des WANs gespeichert. Der Verschlüssler schaut in der Tabelle nach, hinter welchem anderen Verschlüssler sich die Ziel- oder die Senderadresse befindet und weiss so, welche Verbindung für die Schlüsselwahl relevant ist.

Paarweise Schlüsselsysteme sind für Punkt-zu-Punkt-Verbindungen ausgelegt und funktionieren deshalb ausschliesslich für Unicast-Frames. Nur diese sind über ihre MAC-Adresse eindeutig zuweisbar. Multicast- und Broadcast-Frames haben mehrere Destinationsadressen, weshalb sie für ein paarweises Schlüsselsystem nicht verschlüsselbar sind. Es gibt z.B. keinen eigenen Schlüssel, mit dem Verschlüssler A ein Multicast-Frame zu zwei Zielverschlüsslern (B und C) verschlüsseln könnte und von beiden Zielverschlüsslern entschlüsselt werden kann.
Für diese Problematik stehen vier unterschiedliche Lösungsansätze zur Verfügung: (1) Multicast- und Broadcast-Frames unverschlüsselt lassen, (2) Die Multicast- und Broadcast-Frames für jede Verbindung replizieren und sie in Unicast-Frames umwandeln, (3) ein zusätzliches, geeignetes Schlüsselsystem für Multicast- und Broadcast-Frames verwenden, und (4) von vornherein ein für Unicast, Multcast- und Broadcast-Frames geeignetes Gruppenschlüsselsystem einsetzen. Die erste Lösung – die Dispensierung der Multicast- und Broadcast-Frames von der Verschlüsselung – ist, zumindest in Bezug auf die Sicherheit von Multicast- und Broadcast-Frames, nicht akzeptabel. Die zweite Lösung - das Replizieren der Multicast- und Broadcast-Frames über alle Verbindungen – führt zu einer erheblichen Mehrbelastung des Netzwerks. Dies zieht wiederum höhere Betriebskosten oder eine schlechtere Netzwerkperformance nach sich.

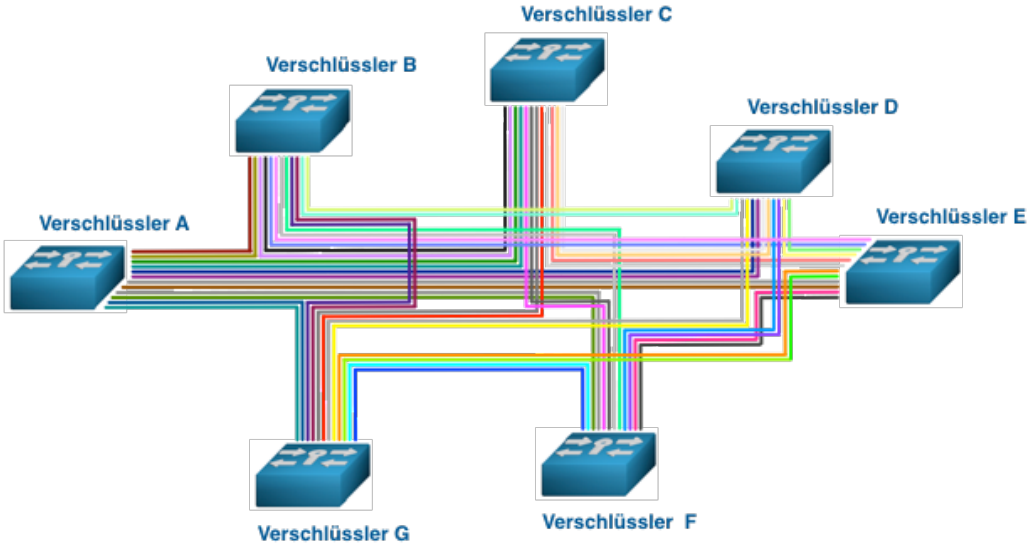
Die dritte Lösung – Verwendung eines zweiten Schlüsselsystems – führt zur Konkurrenz zweier unterschiedlicher Schlüsselsystemen, löst aber das Problem der Verschlüsselung von Multicast- und Broadcast-Frames. Je nach Frame-Typ ist dann das eine oder das andere Schlüsselsystem zuständig. Für die Multicast- und Broadcast-Frame-Verschlüsselung werden Gruppenschlüsselsysteme verwendet. Die bevorzugte Lösung ist die Verwendung eines geeigneten Gruppenschlüsselsystems.

7.5.3. Multipunkt-zu-Multipunkt

Multipunkt-zu-Multipunkt-Topologien erlauben die direkte Kommunikation aller angeschlossenen Standorte untereinander.



Paarweise Schlüsselsysteme behandeln auch Multipunkt-zu-Multipunkt-Topologien wie Punkt-zu-Punkt-Verbindungen. Für jede Verbindung zwischen zwei Verschlüsslern gibt es ein eigenes Schlüsselpaar. Die Zuweisung des richtigen Schlüssels auf die Frames erfolgt unter Zuhilfenahme von MAC-Tabellen. In diesen sind sowohl die lokalen wie auch die entfernten MAC-Adressen des WANs gespeichert. Der Verschlüssler schaut in der Tabelle nach, hinter welchem anderen Verschlüssler sich die Ziel- oder die Senderadesse befindet und weiss so, welche Verbindung für die Schlüsselwahl relevant ist. Paarweise Schlüsselsysteme vertragen sich nicht gut mit Multicast- und Broadcast-Frames. Deshalb gibt es auch hier keine Schlüssel für Frames, die an mehrere Destinationsadressen gehen.



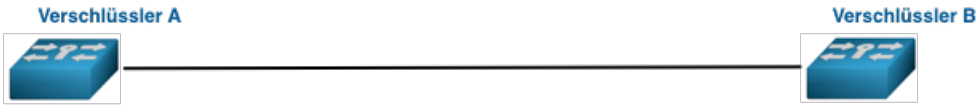
Zur Verfügung stehen wieder die vier verschiedene Lösungsansätze für diese Problematik: (1) Multicast- und Broadcast-Frames unverschlüsselt lassen, (2) Die Multicast- und Broadcast-Frames für jede Verbindung replizieren und sie in Unicast-Frames umwandeln, (3) ein zusätzliches, geeignetes Schlüsselsystem für Multicast- und Broadcast-Frames verwenden, und (4) ein für Unicast-, Multicast- und Broadcast-Frames geeignetes Gruppenschlüsselsystem zu verwenden. Bevorzugte Lösung ist auch hier die vierte Lösung.

7.6. Gruppenschlüssel

Gruppenschlüsselsysteme basieren auf dem Prinzip, dass für die Kommunikation innerhalb einer definierten Gruppe der gleiche Schlüssel verwendet wird. Die Mitgliedschaft in einer Gruppe schliesst nicht die Mitgliedschaft in weiteren Gruppen aus. Nur wird für die Kommunikation innerhalb der unterschiedlichen Gruppen jeweils ein anderer Schlüssel verwendet. Dies führt zu einer kryptographischen Trennung der Gruppen. Eine Gruppe besteht aus zwei oder mehr Mitgliedern. Für Ethernet werden Gruppen meistens nach VLAN-ID erstellt.
Multipunkt-Verbindungen entsprechen meistens Gruppen, die durch Broadcast-Domains verbunden oder getrennt sind. Innerhalb einer Gruppe wird sämtlicher Datenverkehr mit dem gleichen Schlüssel verschlüsselt. Eine Unterscheidung zwischen Unicast-, Multicast- und Broadcast-Frames ist nicht nötig.

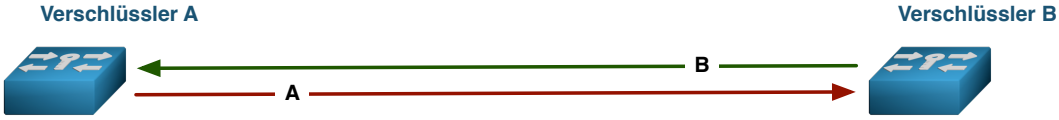
7.6.1. Punkt-zu-Punkt

Für Gruppenschlüsselsysteme wird im Punkt-zu-Punkt-Modus in der Regel eine eigene Gruppe für die Verbindung erstellt.



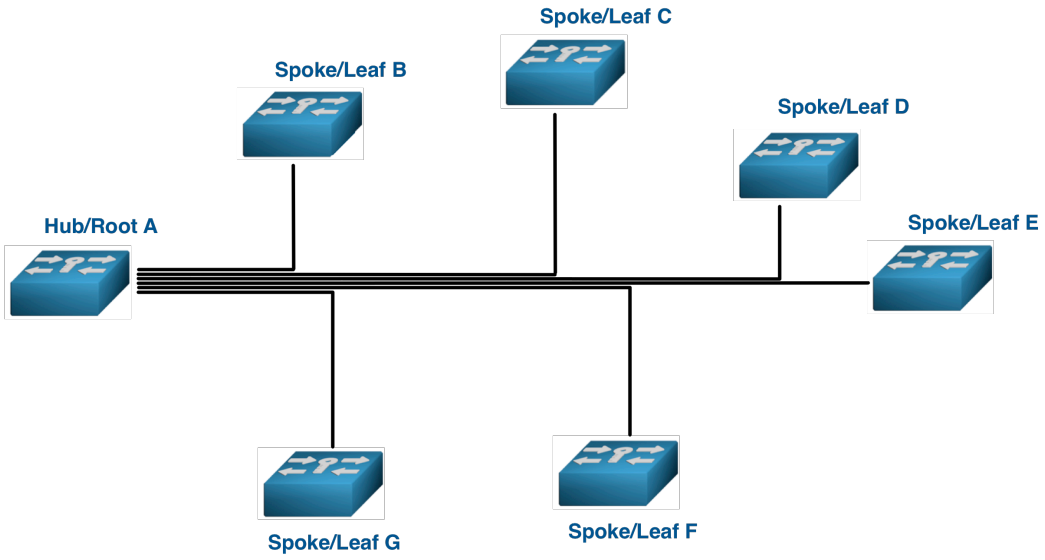
Bei einem bidirektionalen Schlüsselsystem ist das ein Schlüssel für die Verbindung.

Bei einem unidirektionalen Schlüsselsystem sind das zwei Schlüssel für die Verbindung.-



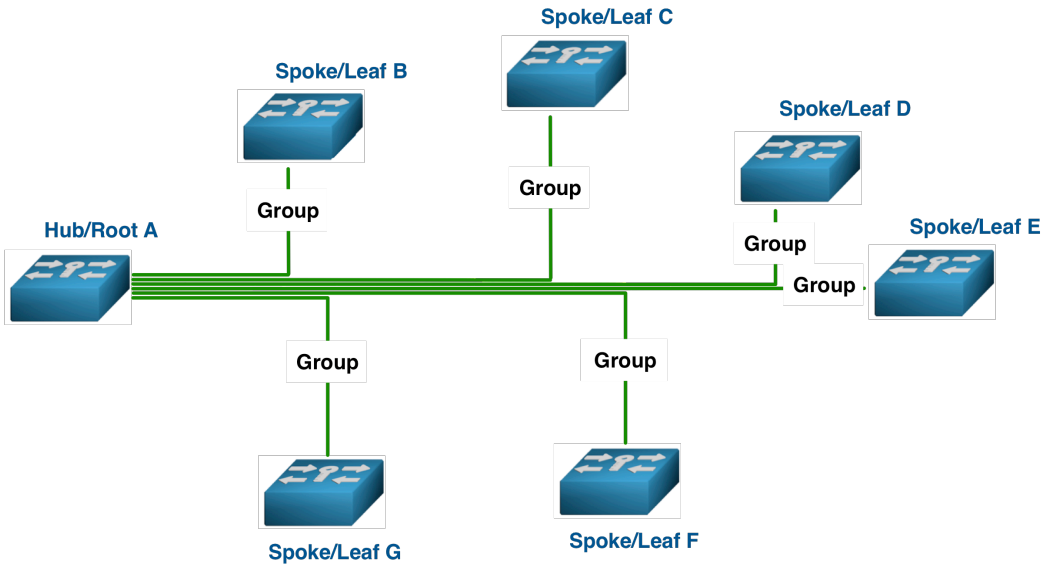
7.6.2. Punkt-zu-Multipunkt

Für Punkt-zu-Multipunkt-Szenarien stehen unterschiedliche Möglichkeiten zur Verfügung. Das Netzwerk kann als eine Gruppe betrachtet oder als mehrere Gruppen.
Je nach den Fähigkeiten des unterliegenden Transportnetzwerks ist das Schlüsselsystem alleine verantwortlich für das Getrennthalten der verschiedenen Verbindungen.

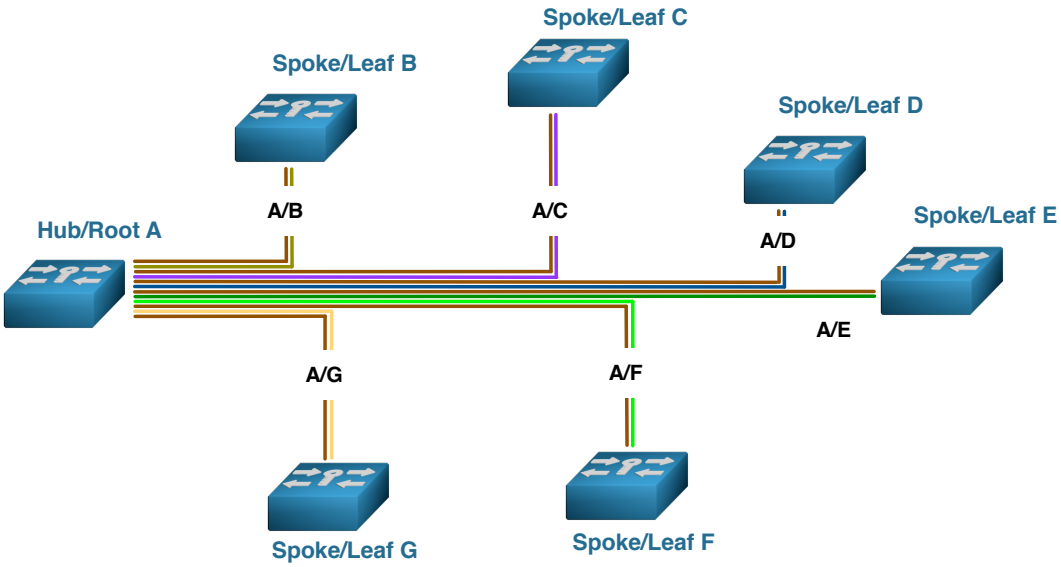


Wird bei der Verwendung von bidirektionalen Gruppenschlüsseln das ganze Netzwerk als die Gruppe betrachtet, so wird auch nur ein einziger Gruppenschlüssel für die gesamte Kommunikation innerhalb des Netzes verwendet. Alle

Verschlüssler können alle Frames entschlüsseln

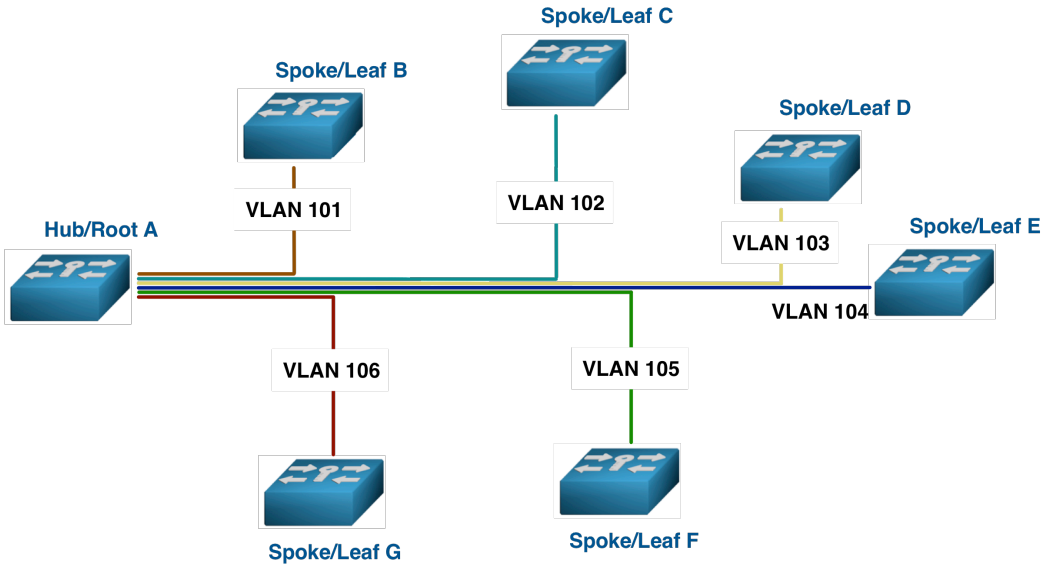


Anders sieht dies bei der Verwendung von unidirektionalen Gruppenschlüsseln aus. Alle Verschlüssler können die Frames des Hub/Root entschlüsseln, aber nur der Hub/Root die jeweiligen Frames der anderen Verschlüssler.

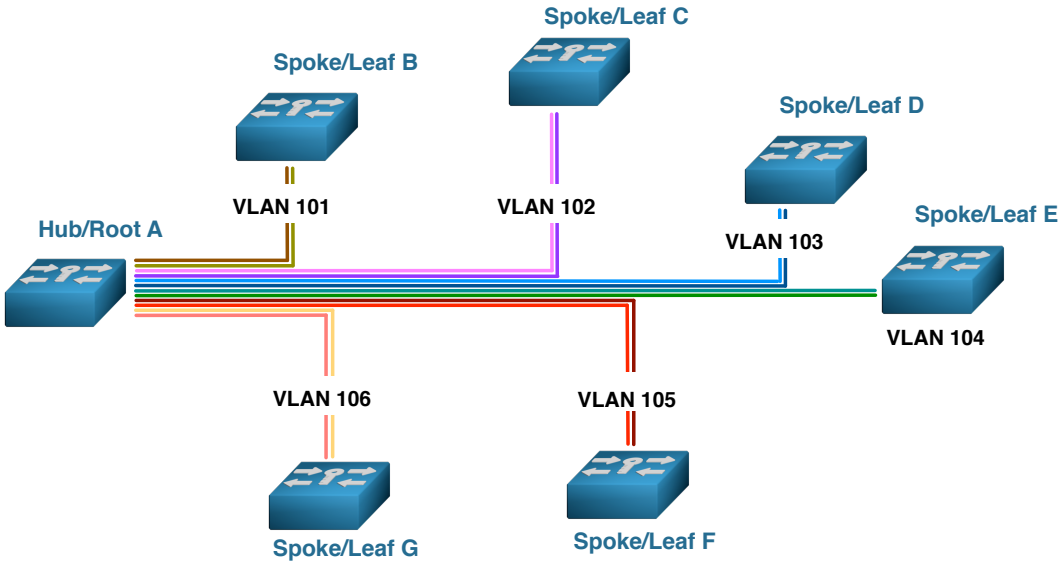


Gruppenschlüssel dienen im Kontext von MANs und WANs meist dazu, Netzwerke strukturorientiert zu verschlüsseln. Das Punkt-zu-Multipunkt-Netzwerk wird in Punkt-zu-Punkt-Verbindungen aufgebrochen, die jeweils eine eigene Gruppe konstituieren. Dadurch sind die einzelnen Verbindungen kryptographisch getrennt, eine der Voraussetzungen für Mandantenfähigkeit.

Bei einem bidirektionalen Gruppenschlüsselsystem sieht das dann so aus:

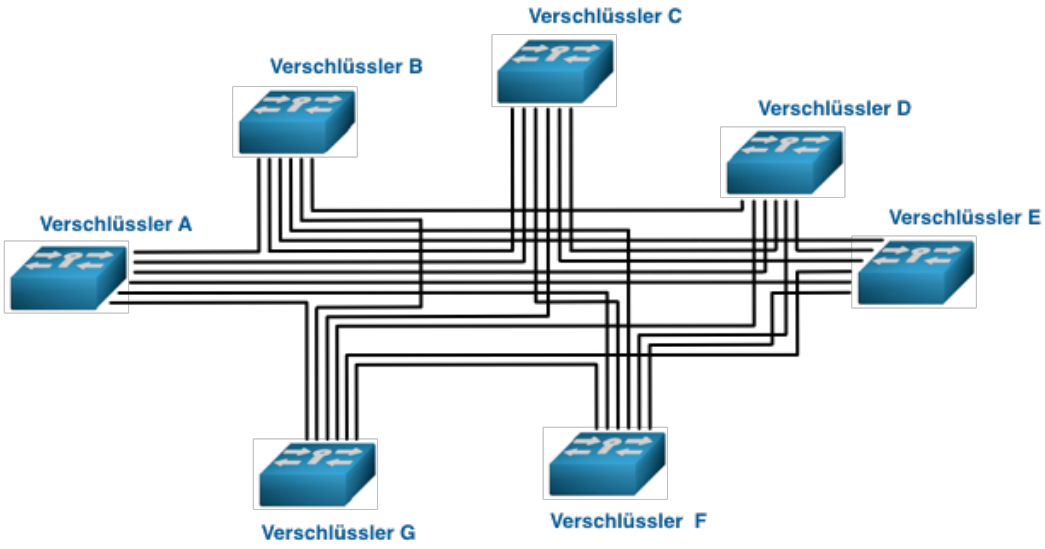


Bei einem unidirektionalen Gruppenschlüsselsystem ergibt sich ein Bild wie bei paarweisen Schlüsseln, die jedoch zusätzlich nach VLAN getrennt sind.

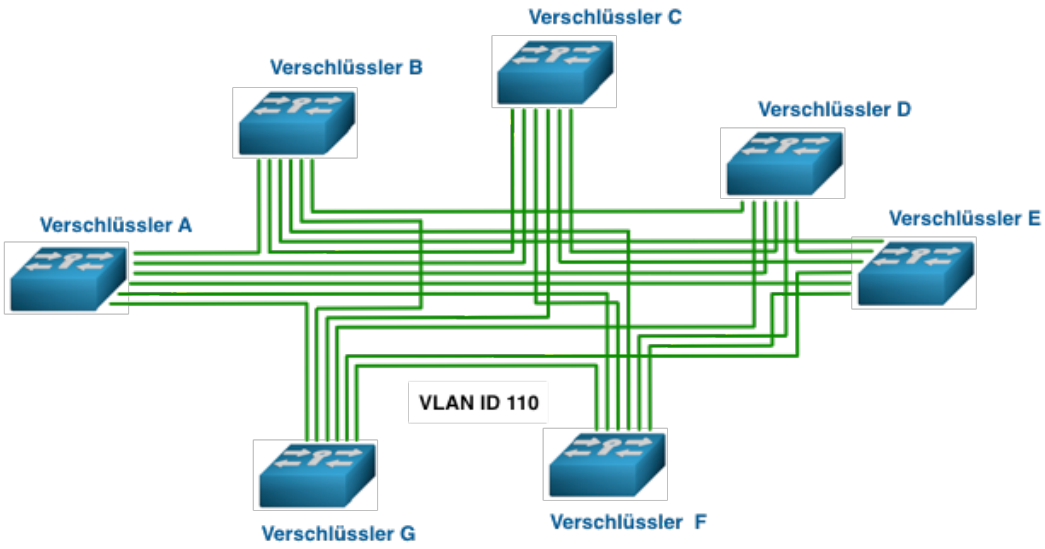


7.6.3. Multipunkt-zu-Multipunkt

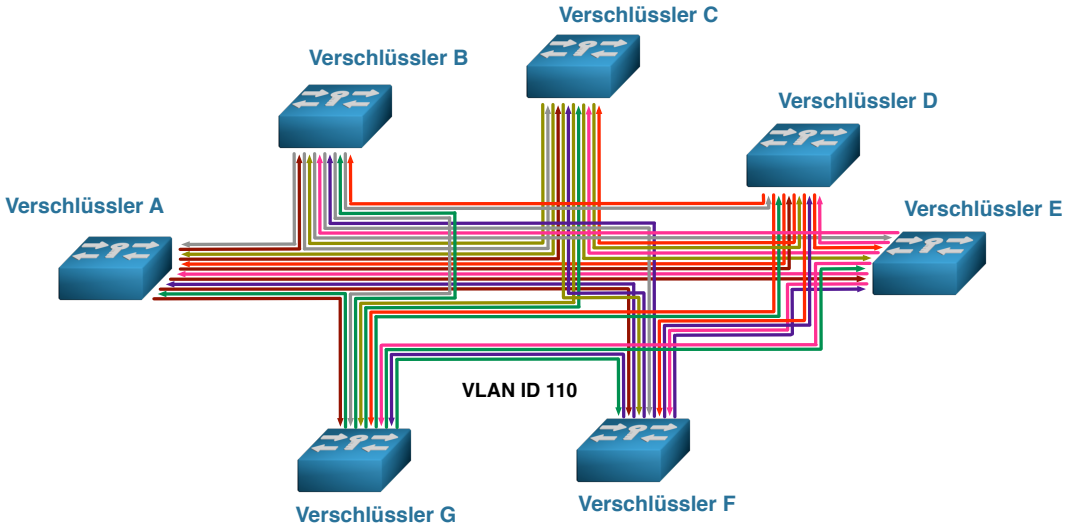
Bei Multipunkt-zu-Multipunkt-Netzwerken kann jeder mit jedem anderen kommunizieren.



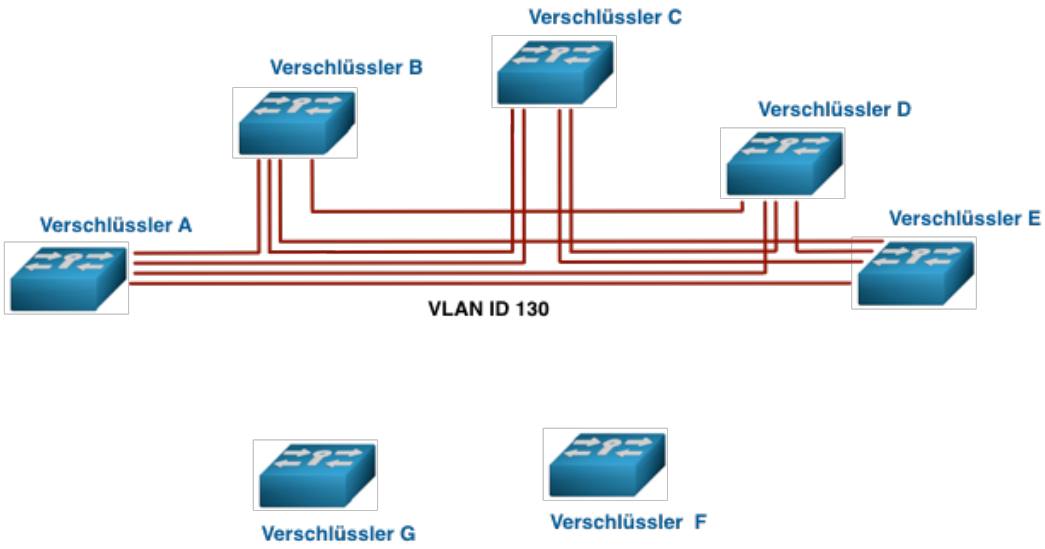
Auch hier besteht die Möglichkeit, das gesamte Netzwerk als eine Gruppe zu betrachten. Entsprechend verwendet ein bidirektionales Gruppenschlüsselsystem nur einen gemeinsamen Schlüssel:



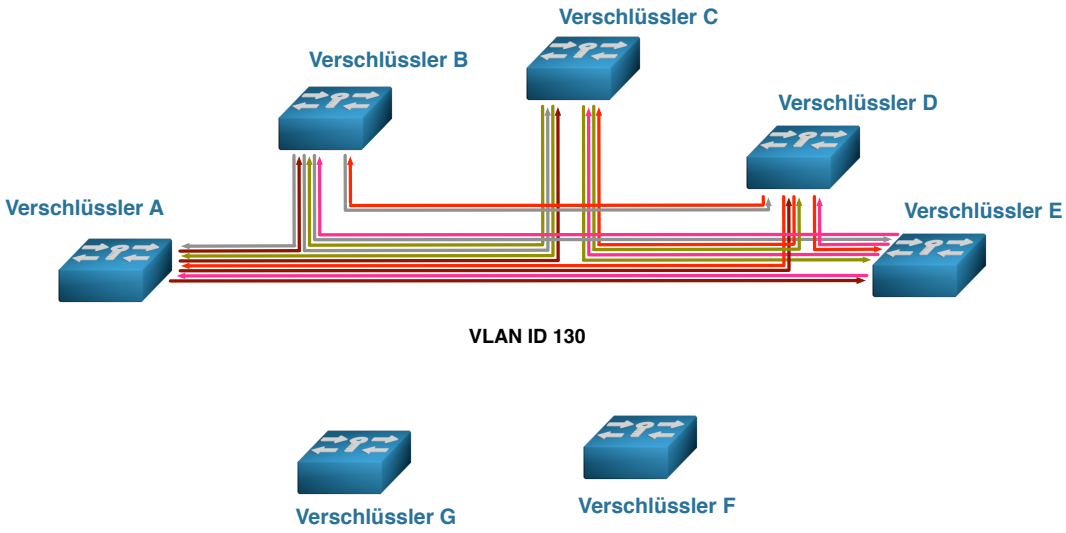
Anders sieht es bei einem unidirektionalen Gruppenschlüsselsystem aus. Jeder Verschlüssler verwendet für den ausgehenden Netzwerkverkehr seinen eigenen Gruppenschlüssel.



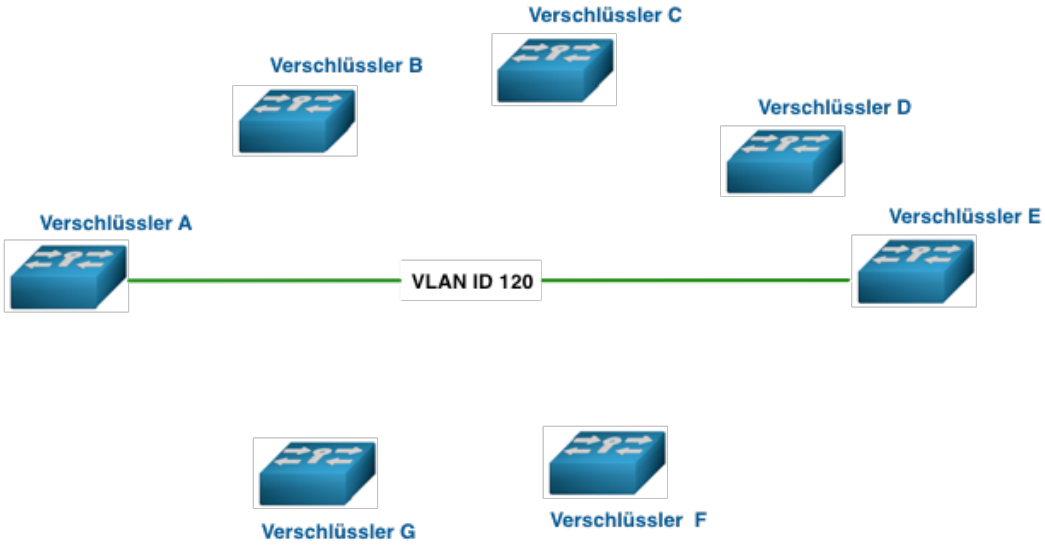
Eine Gruppe kann aber auch nur aus einem Subset des Netzwerks bestehen. Oft ist es erwünscht, dass nur die Standorte Zugriff auf Dienste haben, die sie effektiv nutzen sollten. Bei einem bidirektionalen Gruppenschlüsselsystem benutzen alle beteiligten Standorte dieser Gruppe denselben Gruppenschlüssel.



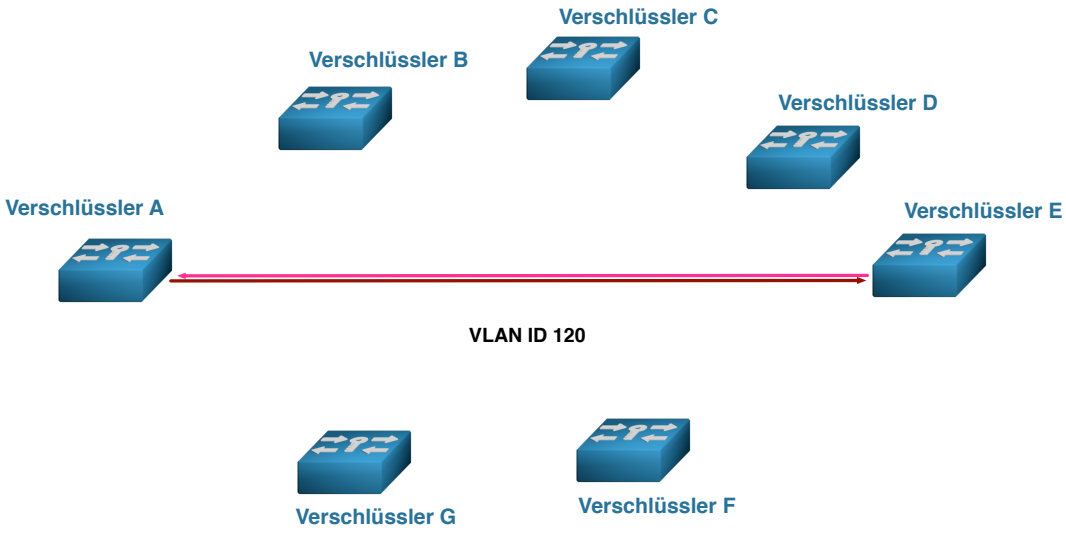
Bei Verwendung eines unidirektionalen Gruppenschlüsselsystems, verwendet jeder beteiligte Standort seinen eigenen Gruppenschlüssel für den ausgehenden Netzwerkverkehr und den jeweiligen Gruppenschlüssel der anderen Standorte für den eingehenden Netzwerkverkehr.



Das Subset kann aus einer einzigen Punkt-zu-Punkt-Verbindung innerhalb des Netzwerks bestehen. Bei einem bidirektionalen Gruppenschlüsselsystem verwenden beide beteiligten Standorte den gleichen Gruppenschlüssel.



Bei einem unidirektionalen Gruppenschlüsselsystem verwendet jeder Verschlüssler seinen Gruppenschlüssel für den ausgehenden Netzwerkverkehr und den Gruppenschlüssel des anderen Standortes für den eingehenden Netzwerkverkehr.



Leistungsfähige bidirektionale Gruppenschlüsselsysteme erlauben die Etablierung der Gruppenzugehörigkeit durch Parameter wie VLAN-IDs, MAC-Adressen, MPLS-Tags etc. Solche Gruppenschlüsselsysteme verwenden in der Regel einen Key Server, der mehrstufig redundant ausgelegt ist. Bei Ausfall eines Key Servers übernimmt automatisch der nächste. Key Server können integriert oder extern sein. Es ist auch möglich eine Kombination von externen und integrierte Key Server zu verwenden. Der Key Server sorgt dafür, dass jeder Verschlüssler die Gruppenschlüssel erhält, welche die sich hinter ihm befindlichen Geräte benötigen, um mit den anderen Gruppenmitgliedern an den anderen Standorten kommunizieren zu können. Der Key Server muss unter anderem auch sicherstellen, dass bei Änderungen der Gruppenzusammensetzung ein neuer Schlüssel erstellt wird. Mit dem neuen Schlüssel kann der alte Datenverkehr nicht entschlüsselt werden und mit dem alten Schlüssel kann der neue Datenverkehr nicht entschlüsselt werden.
Bei Ethernet drängt es sich auf, die Gruppen nach VLAN-IDs zu organisieren, da in der Regel Firmennetze die Broadcast-, Security und Failure-Domains durch VLANs eingrenzen und so auch das Netzwerk segmentieren. Bei einer Gruppenverschlüsselung, die nach VLANs organisiert ist, wird diese Segmentierung auch für die Verschlüsselung verwendet und stellt so auch eine kryptographische Trennung der VLANs her.

Bei unidirektionalen Gruppenschlüsselsystemen ist regelmässig jeder Verschlüssler sein eigener Key Server für seine Gruppenschlüssel. Der Ausfall einer Netzwerkverbindung oder eines Verschlüssler beeinträchtig deshalb die anderen Standorte nur insoweit, wie sie auf Datenaustausch mit diesem Standort angewiesen sind. Jeder Standort ist eine eigene „Failure Domain“. Auch bei Verwendung eines unidirektionalen Gruppenschlüsselsystems steht die Möglichkeit des Einsatzes von einem oder mehreren externen Key Server offen, macht aber nicht viel Sinn.

Rechenzentren und Standorte abhörsicher vernetzen

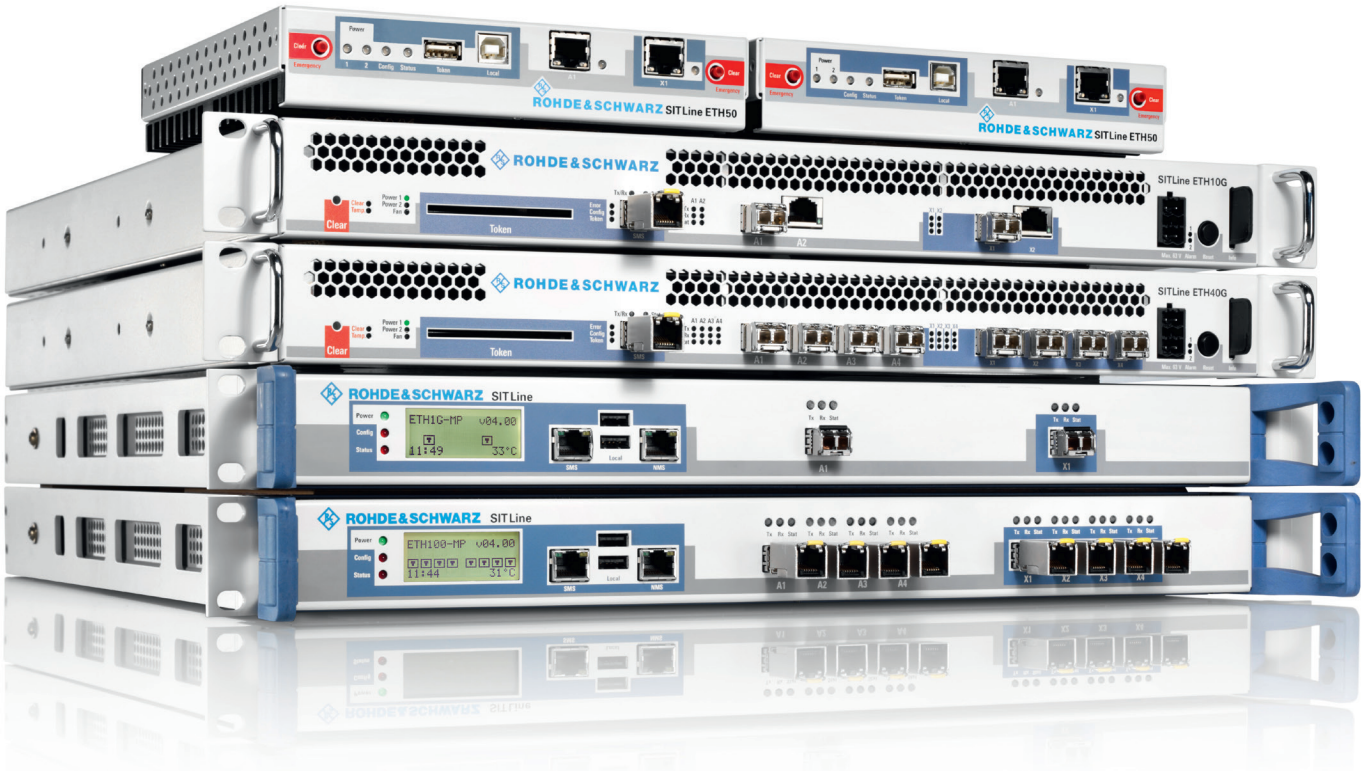
SecurITy made in Germany

Bei der Vernetzung von Standorten und Rechenzentren verlassen sensible Daten die geschützte IT-Infrastruktur. Doch optische und elektrische Leitungen können einfach abgehört werden.

R&S®SITLine ETH verschlüsselt die Daten vor der Übertragung – kostengünstig, hochverfügbar, BSI-zugelassen.

- Ethernet-Verschlüsseler für Bandbreiten bis 40 Gbit/s
- Sichere Datenübertragung über Festnetz, Richtfunk und Satellit
- BSI-zugelassen bis VS-NfD und NATO RESTRICTED

Weitere Informationen unter:
cybersecurity.rohde-schwarz.com



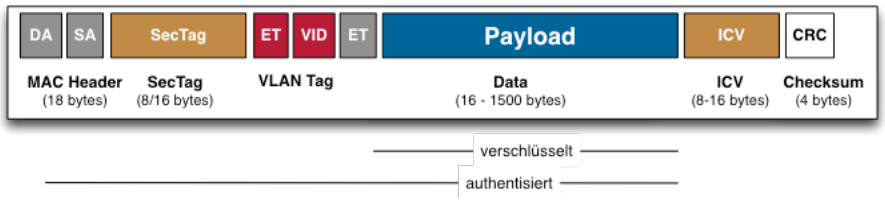
ROHDE&SCHWARZ
Cybersecurity

8. Standards

Es gibt keinen Standard für die Verschlüsselung von Carrier Ethernet-Netzwerken. Einigkeit besteht nur darin, dass authentisierte Verschlüsselung mittels AES-GCM verwendet werden soll.
Hingegen gibt es mit MACSec einen Standard für die Verschlüsselung von lokalen Ethernet-Netzwerken, dessen Anwendungsbereich bis in Nahbereichsnetzwerke (MAN) erweitert wurde. Zwischen einem lokalen Netzwerk und einem WAN gibt es massive Unterschiede, die sich sowohl auf die Funktionalitätsanforderungen wie auch auf die Sicherheitsanforderungen auswirken.

8.1. MACSec/LinkSec

MACSec/MacLink ist von der IEEE als Standard (802.1ae) für die Verschlüsselung von standortinternen LANs auf Layer 2 veröffentlicht worden Authentisierung und Schlüsselverwaltung für MACSec sind mittlerweise als Teil von IEEE 802.1X-2010 standardisiert, nachdem der erste Versuch einer eigenen Standardisierung (IEEE 802.1af) scheiterte. Beim MACSec-Frame-Format handelt sich um einen speziellen Transport-Modus, der auf die spezielle Umgebung von firmeninternen LANs ausgelegt und limitiert worden ist. Im Gegensatz zum normalen Transport-Modus setzt MACSec das SecTag direkt nach der Ziel- und Senderadresse ein. Nur Geräte, die MACSec direkt unterstützen können überhaupt das Frame-Format erkennen.



MACSec Frame-Format

Eine weitere Einschränkung findet sich in der ausschliesslichen Unterstützung von Hop-by-Hop-Szenarien. Bei jedem Gerät wird der Frame nach Empfang entschlüsselt und vor Versand verschlüsselt. Innerhalb des Geräts bleiben die Daten unverschlüsselt. Jede aktive Netzwerkkomponente auf dem Weg von der Senderadresse zur Zieladresse gilt dabei als Hop. Es ist also beispielsweise nicht möglich, Frames von der Sendeadresse via Switch/Router an die Zieladresse zu schicken, ohne dass der Switch/Router den Frame entschlüsselt, liest und dann wieder verschlüsselt. Für die Absicherung von Metro und Carrier Ethernet ist das definitiv ungünstig.
Die unterstützten Topologien sind auf Punkt-zu-Punkt und Punkt-zu-Multipunkt limitiert.

8.1.1. MACSec, der „Standard“ für lokale Netzwerke

MACSec wurde für die Verwendung innerhalb eines lokalen Firmennetzwerkes spezifiziert und findet seinen Anwendungsbereich auch vorzugsweise dort. Zur Absicherung von standortübergreifenden Netzwerken ist es in der im Standard beschriebenen Form eher ungeeignet. Ziel von MACSec war es von vornherein etwas so kostengünstig zu machen, dass die Produktkosten nur marginal tangiert werden. Die vorinstallierte Hardwareunterstützung eröffnet dann für die Produkthersteller die Möglichkeit, ohne grossen Aufwand mit Softwarelizenzen Geld zu verdienen. Auf der Strecke blieben Sicherheit, Skalierbarkeit und Funktionalität. Was in Bezug auf Funktionalität nicht passt, kann man aber versuchen passend machen. So wurden Funktionalitäten, die in spezialisierten Appliances schon lange vorhanden waren, wie zum Beispiel definierbare Verschlüsselungsoffsets und definierbare Replay-Fenster eingeführt, sind aber nicht Teil des Standards. Einzelne Anbieter haben auch am Schlüsselsystem Anpassungen vorgenommen. Bei einem führenden Hersteller von Netzwerkgeräten gibt es deshalb das eigene MACSec for LAN und das eigene MACSec for WAN. Selbstverständlich sind die beiden nicht interoperabel. Mehrere Anbieter setzen sich auch für die Unterstützung von End-to-End-Verschlüsselung ein und nehmen selbständig Verbesserungen am Standard vor. Der verwendete Ethertype bleibt aber immer noch der des Standards, der diese Verbesserungen nicht beinhaltet. Als interoperabler Standard ist MACSec gescheitert. Für Metro und Carrier Ethernet ist MACSec als integrierte Lösung sicherheitsmässig und funktionalitätsmässig beschränkt auf Szenarien mit geringen Sicherheitsanforderungen und einfachsten Umgebungen. Um die Restriktionen der Hop-by-Hop-Verschlüsselung zu umgehen, gibt es die Möglichkeit, einen MACSec-Frame zu tunneln. Das erhöht die Einsetzbarkeit genauso wie die Latenz und den Overhead, macht aber speziell im Fall von Carrier Ethernet wenig Sinn.

Eines der vielen ungelösten Grundprobleme von MACSec bleibt auch die Vorschrift der ausschliesslichen Nutzung von US-Sicherheitsstandards. Weder der zwangsweise Einsatz von NIST-Kurven noch die ausschliessliche Verwendung von NIST-Zufallszahlengeneratoren können als vertrauenserweckende Massnahmen gewertet werden. Ist die Verschlüsselung von MACSec zudem noch in ein Netzwerk-ASIC integriert, so können Implementierungsfehler und bewusst eingebaute Hintertüren direkt über die Netzwerkschnittstelle ausgenutzt werden. Bei einem LAN ist das deutlich weniger kritisch als bei einem MAN oder WAN. Aufgrund des erheblichen verbleibenden Sicherheitsrisikos sind solche Lösungen die Kategorie Low Assurance einzuordnen.

Selbst innerhalb des offiziellen Standards gibt es mittlerweile Inkompatibilitäten, weil die Unterstützung von Schlüsseln mit einer Länge von 256 Bit erst 2011 standardisiert wurde. Nur die Teile von MACSec, die von allen Netzwerkteilnehmern gleich verwendet werden sind innerhalb des Netzwerks inte-

roperabel. Für die Unterstützung von 256 Bit-Schlüsseln braucht es daher in den meisten Fällen einen Hardwaretausch. 2013 kam dann noch die Erweiterung der Paketnummerierung dazu. Jede der vielen nötigen künftigen Erweiterungen hat die gleiche Folge.

Die nachfolgenden Links zeigen auf Inhalte und Dokumente, die MACSec und dessen Nutzungszweck ausgiebig beschreiben und die obgenannten Probleme und Einschränkungen bestätigen.

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

Zwischen der IEEE und der NSA gibt es seit Jahrzehnten eine enge Zusammenarbeit. Diese führte zur Entwicklung von Spezifikationen für einen NSA Ethernet-Verschlüssler, der auf MACSec basiert, aber nicht standardkompatibel ist. Es handelt sich um einen reinen Link-Verschlüssler. Auch die IEEE arbeitet an einem Standard für MACSec-Appliances. Sowohl ESS der NSA als auch EDE (Ethernet Data Encryption) der IEEE liegen technisch und funktionalitätsmässig Jahre hinter dem, was seit längerem auf dem Markt verfügbar und sicher ist.

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

Spezialisierte Appliances zur Verschlüsselung von Carrier Ethernet-Netzwerken sind in der Regel sicherer und in mehr Szenarien einsetzbar als MACSec-Appliances. Kosten tun aber beide etwa gleich viel, ausser die MACSec-Appliance verwendet eine direkt auf der Netzwerkschnittstelle integrierte Verschlüsselungshardware. Dann ist das aber wieder eine Low Assurance-Lösung und keine Standard Assurance-Lösung. Man sollte sich immer wieder in Erinnerung rufen, dass es sich bei MACSec nicht um den Standard für Ethernet-Verschlüsselung für Carrier Ethernet handelt und es bessere und sicherere Lösungen gibt.

9. Evaluation

Dieses Dokument ist eine Einführung in die Absicherung von Metro und Carrier Ethernet-Netzwerken. Bei einer Evaluation sind viele unterschiedliche Produkteigenschaften und Leistungsmerkmale zu beachten, die in diesem Dokument nicht aufgelistet sind. Unter den auf dem Markt erhältlichen Geräten hat es solche, die über sämtliche möglichen Sicherheits- und Netzwerkfunktionalitäten verfügen, solche, welche über einen Grossteil davon verfügen und solche, die nur ein Subset abdecken. Entscheidend für die Sicherheit ist das jeweilige Gesamtsystem inklusive dessen Implementierung, nicht einzelne, aus dem Kontext gerissene Teilbereiche.
Die Kombination des SecTag-Inhalts, Schlüsselverwaltung, Schlüsselsystem und Unterstützung variabler Verschlüsselungsoffsets zeigt nur die grundlegende Funktionsweise eines Verschlüsslers auf.

Neben der Sicherheit, der Netzwerkunterstützung und der Effizienz spielt auch die Eignung für die unterschiedliche Einsatzszenarien eine Rolle.

Weitere Hilfestellungen finden sich in folgenden Dokumenten:

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

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

10. Zusätzliche Informationsquellen zu Netzwerken und Sicherheit

Netzwerkverschlüsselung bedingt Kenntnisse von Netzwerk- und Verschlüsselungstechnologien. Ein strukturiertes und segmentiertes Netzwerk ist di Grundlage jeder effizienten Absicherung. Gute, herstellerunabhängige Informationen sind leider nicht im Überfluss vorhanden. Deshalb nachstehend ein paar international von Fachkreisen anerkannte Quellen, die hervorragende Informationen bereithalten.

10.1. IPSpace

Ivan Pepelnjak veröffentlicht laufend Blog-Posts über Netzwerk- und Rechenzentrumtechnologien und deren Einsatz. Auch die Sicherheit kommt nicht zu kurz. Zu vielen Themenbereichen gibt es auch Webinare. Er ist ein weltweit gefragter Top-Experte.

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

10.2. Packet Pushers

Podcasts von Greg Ferro und Ethan Banks über Netzwerktechnologien, Netzwerkhardware und Netzwerksoftware. Sehr technisch und sehr profund.

http://packetpushers.net

10.3. Postmodernsecurity

Michele Chubirka aka Mrs. Y ist eine renommierte Infosec-Grösse und Sicherheitsarchitektin.

http://postmodernsecurity.com
http://packetpushers.net/?s=healthy+paranoia

10.4. ERNW

Enno Rey und die anderen Leute bei ERNW waren mit die ersten weltweit, welche sich mit der Sicherheit von Carrier Ethernet befasst und dabei aufgezeigt haben, wie Transportnetzwerke angegriffen werden können. ERNW ist auch Organisatorin der bekannten jährlichen Troopers-Konferenz und äusserst sich zu Sicherheitsthematiken auf ihrem Insinuator-Blog.

http://www.insinuator.net
https://www.ernw.de
https://www.troopers.de

10.5. Carrier Ethernet-Group auf LinkedIn

Vishal Sharma ist ein renommierter Telekom-Experte, hat die Carrier Ethernet-Gruppe auf LinkedIn ins Leben gerufen und ist auch deren Moderator.

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

Auf seinem Firmen-Blog finden sich interessante Beiträge zu Datennetzwerken und anderen Telekom-Themen.

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