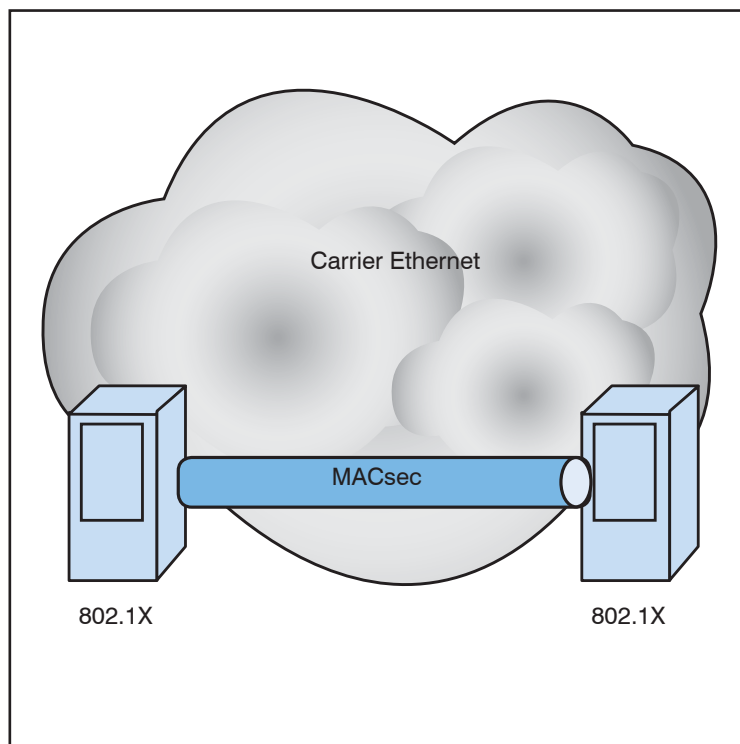


Neue Verfahren für mandantenfähige Netze

von Dr. Simon Hoff, Dr. Behrooz Moayeri



Dieser Beitrag befasst sich mit neuen Verfahren für mandantenfähige Netze. Einerseits hat sich Carrier Ethernet mittlerweile neben Multi-Protocol Label Switching (MPLS) als Technologie in den Service-Provider-Netzen etabliert, und andererseits wurde IEEE 802.1X, der Standard für Port-basierende Authentisierung, der u. a. für eine dynamische Zuordnung eines Endgeräts zu

einer Benutzergruppe genutzt wird, in 2010 wesentlich erweitert.

Im ersten Teil des Beitrags wird auf Carrier Ethernet eingegangen. Danach folgt eine Zusammenfassung der in 2010 hinzugekommenen Erneuerungen in IEEE 802.1X, die diesen Standard noch wichtiger für mandantenfähige Netze machen.

1. MPLS bekommt Konkurrenz

In den letzten zehn Jahren hat sich Multi-Protocol Label Switching (MPLS) zum De-facto-Standard für mandantenfähige Netze entwickelt. Die wesentlichen Erfolgsfaktoren von MPLS waren die folgenden:

weiter auf nächster Seite

Schwerpunktthema

Neue Verfahren für mandanten- fähige Netze

Fortsetzung von Seite 1



Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück



Dr. Behrooz Moayeri ist in der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er ist zudem Leiter des Competence Centers Netze.

- Dank der zugrundeliegenden Routing-Protokolle kann MPLS auf jede Backbone-Topologie (Ring, Stern, vermascht) abgebildet werden.
- MPLS bietet eine Reihe von Mechanismen für Verkehrslenkung und Traffic Engineering (TE).
- MPLS hat sich trotz der Komplexität des Verfahrens in der Praxis als sehr robust erwiesen.
- MPLS ist sehr skalierbar, weil das Verfahren mit jeder neuen physikalischen Übertragungstechnik kombiniert werden kann. Es war zum Beispiel überhaupt kein Problem, MPLS mit 10Gigabit Ethernet zu kombinieren. Hier lag zum Beispiel ein ganz entscheidender Vorteil von MPLS gegenüber Asynchronous Transfer Mode (ATM), einer Technologie, die bei 622 Mbit/s stehen blieb.
- Anders als herkömmliches IP Routing unterstützte MPLS von Anfang an Virtual Private Networks (VPNs) und damit auch Mandantenfähigkeit.
- MPLS unterstützt anders als zum Beispiel Synchronous Digital Hierarchy (SDH) Any-to-any-Kommunikation innerhalb eines Mandantennetzes.
- Automatismen in einem MPLS-Netz ermöglichen ein sogenanntes Edge Provisioning, d. h. das Hinzufügen eines Standorts zu einem Mandantennetz be-

schränkt sich auf die Zuordnung des Edge Devices am Standort zum betreffenden VPN.

Der Siegeszug von Ethernet in lokalen Netzen brachte schon vor ca. zehn Jahren Hersteller und Netzbetreiber auf die Idee, innerhalb des für die Ethernet-Standardisierung zuständigen Institute of Electrical and Electronic Engineers (IEEE) an zusätzlichen Ethernet Standards für Carrier-Netze zu arbeiten. Diese Arbeit trägt viele Früchte, u. a. die beiden verabschiedeten Standards für Provider Bridging (IEEE 802.1ad) sowie Provider Backbone Bridging (IEEE 802.1ah) und den kurz vor der Verabschiedung stehenden Standard Shortest Path Bridging (IEEE 802.1aq). Zusammen bilden vor allem diese drei Standards die Basis für das sogenannte Carrier Ethernet, das MPLS hinsichtlich der o. g. Vorzüge in fast nichts nachsteht und daher eine Technologie darstellt, die das Potenzial hat, MPLS in vielen Bereichen zu verdrängen.

2. Ethernet: Technologie für mandantenfähige Backbones

Die wichtigsten Standards des IEEE für den Einsatz von Ethernet in mandantenfähigen Backbones sind:

- IEEE 802.1ad: Provider Bridged Networks
- IEEE 802.1ag: Ethernet Operations, Administration and Maintenance (OAM)

- IEEE 802.1ah: Provider Backbone Bridged Networks

- IEEE 802.1aq: Virtual Bridged Local Area Networks - Amendment 8: Shortest Path Bridging

Diese Standards befassen sich vor allem mit Ethernet im Backbone, während sich die Spezifikation IEEE 802.3ah-2004 mit dem Titel „Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks“ den Einsatz von Ethernet als Zugangsplattform zu Provider Backbones regelt. Im Standard IEEE 802.3ah geht es eher um die physikalischen Schnittstellen und Übertragungsverfahren, so dass wir uns im Folgenden eher auf die Standards aus der Reihe IEEE 802.1 konzentrieren. Diese Standards befassen sich mit den Mechanismen auf der Ebene der Schicht 2.

Der Standard IEEE 802.1ad sieht vor, dass beim Übergang vom LAN zum WAN ein Service Provider Tag als Bestandteil des Headers hinzugefügt wird. Dieser VLAN-Tag wird als Service Virtual Local Area Network (S-VLAN) Tag bezeichnet und unterscheidet sich vom Customer Virtual Local Area Network (C-VLAN) Tag. C-VLAN-Tags werden von Kunden und S-VLAN-Tags vom Provider vergeben und verwaltet. So entsteht ein „Stapel“ von Tags im Frame Header, weshalb das Verfahren auch als „Q-in-Q Tagging“ bekannt ist (Q steht dabei für den Standard IEEE 802.1Q, der erstmalig die Verwendung von VLAN-Tags regelte).

Neue Verfahren für mandantenfähige Netze

IEEE 802.1ah erweitert den Ansatz von IEEE 802.1ad in dem Sinne, dass eine vollständige Einkapselung eines Ethernet-Rahmens des Kunden im vollständigen Ethernet-Rahmen des Providers inkl. eigener Adressen vorgesehen wird. Provider und Kunden nutzen jeweils einen eigenen Medium Access Control (MAC) Header. Das Verfahren ist daher als MAC-in-MAC bzw. MAC Address Stacking bekannt.

Provider Bridging (PB) bzw. Provider Backbone Bridging (PBB) bilden zusammen die Grundlage eines neuen Anwendungsgebiets von Ethernet, das manchmal als „Carrier Ethernet“ bezeichnet wird. Damit ist die Nutzung von Ethernet als Transporttechnologie im WAN gemeint (siehe Abbildung 1).

3. Neue Redundanzmechanismen

Ein Problem im Zusammenhang mit Carrier Ethernet stellen die bisher in Ethernet-Netzen üblichen Redundanzmechanismen dar. Der in Ethernet-Netzen dominierende Layer-2-Redundanzmechanismus ist Spanning Tree. Spanning Tree in der bisherigen Form ist aber für große Backbones nicht geeignet. Das Protokoll ist nicht skalierbar und der Algorithmus nicht robust genug. Hinzu kommt, dass der Netzbetreiber mit Spanning Tree nur wenige Möglichkeiten für die gezielte Lenkung des Verkehrs hat. Ein weiterer Nachteil besteht darin, dass bei Anwendung von Spanning Tree Leitungen nicht effizient genutzt werden. Per definitionem macht Spanning Tree aus einem vermaschten Netz eine Topologie, in der es zwischen zwei beliebigen Punkten im Netz nur einen aktiven Pfad geben darf. Somit werden alle anderen Pfade vom Algorithmus blockiert, wie in der Abbildung 2 dargestellt.

Aber vielleicht der gravierendste Nachteil von Spanning Tree für Backbone-Betreiber besteht darin, dass die Redundanzmechanismen des Backbones und der Kundennetze nicht sauber voneinander getrennt sind. Das Spanning-Tree-Verfahren bietet keinerlei Schutzmechanismus, welcher die Auswirkung von Fehlern und Änderungen auf einen Netzbereich begrenzen würde. Die Neukonfiguration von Spanning Tree kann das ganze Netz in Mitleidenschaft ziehen. Es reicht, dass aufgrund eines Fehlerzustandes die Neukonfiguration des Netzes sich ständig wiederholt, oder dass die Prozessoren der Netzkomponenten durch die ständige Berechnung des Spanning Tree in den Hochlastbereich geraten, und schon sind das ganze Netz und die darüber abgewickelten Dienste betroffen. Solche Szenarien sind in der Praxis häufig eingetreten. Mit Spanning Tree kann somit ein Kundennetz andere beeinflussen, was aus der

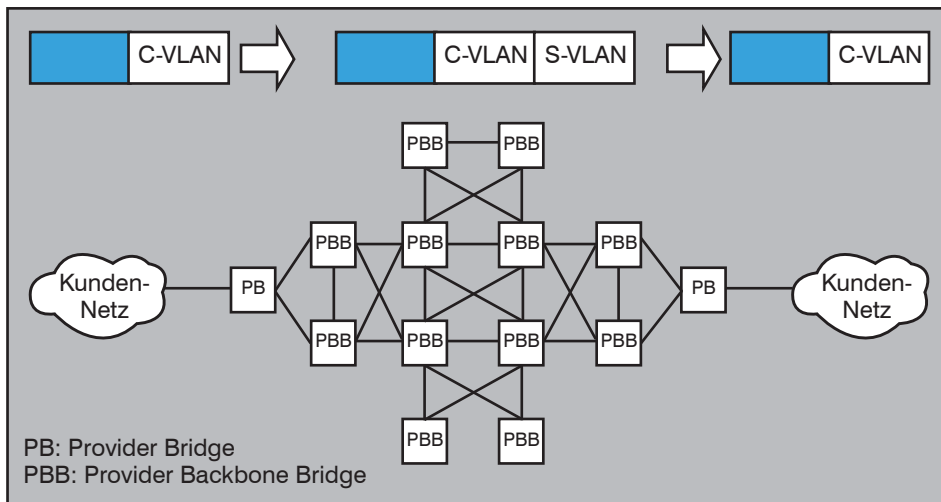


Abbildung 1: Provider Bridges fügen den Rahmen S-VLAN-Tags hinzu

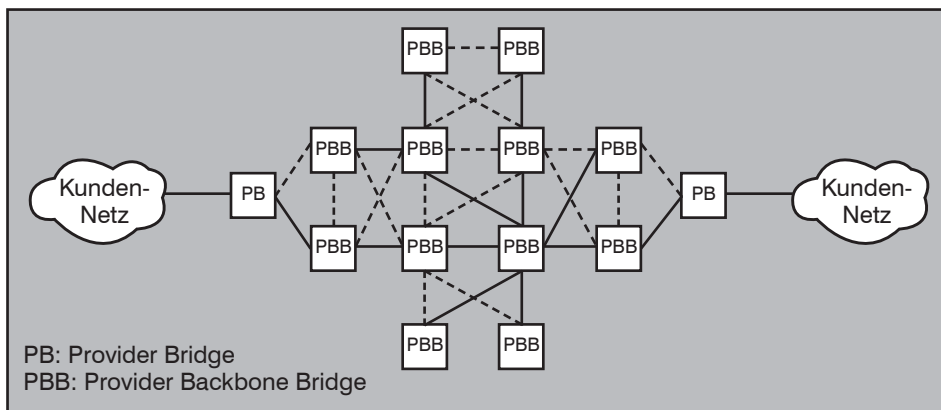


Abbildung 2: Blockierungen von Links durch Spanning Tree

Sicht des Backbone-Betreibers nicht akzeptabel ist.

Somit ermöglicht die Kombination aus den LAN-Standards IEEE 802.3 (Ethernet), IEEE 802.1D (Bridging mit Spanning Tree), IEEE 802.1Q (VLAN), IEEE 802.1ad (Provider Bridging) und IEEE 802.1ah (Provider Backbone Bridging) zwar eine Differenzierung zwischen verschiedenen Kunden in einem mandantenfähigen Netz, aber Erweiterungen dieser Standards sind erforderlich, um Ethernet „Provider-tauglich“ zu machen.

4. Shortest Path Bridging

In einem Carrier Ethernet ist ein neues Bridging-Verfahren notwendig, das einerseits dem Provider mehr Kontrolle über das Netz gibt und andererseits besser als das herkömmliche Ethernet die Kundennetze voneinander entkoppelt. Ein solches Verfahren ist in der Abbildung 3 dargestellt.

Abbildung 3 zeigt den Fluss eines Rahmens durch das Provider-Netz. Dabei wird die vom Service Provider verwaltete MAC-

Adresse (S-MAC) dafür verwendet, den Ethernet-Rahmen zu einem Ziel innerhalb des Provider-Netzes, in der Regel zu einer Provider Bridge, weiterzuleiten. Die vom Service Provider verwaltete VLAN-ID (S-VLAN-Tag) dient dazu, in der Provider Bridge (PB) den Rahmen zum betreffenden Kundennetz zu transportieren.

Das Kundennetz übergibt dem Backbone einen Rahmen mit den herkömmlichen Header- und Trailer-Informationen, nämlich die im Kundenbereich (C für Customer) verwendeten und verwalteten Felder:

- Destination Address (C-DA)
- Source Address (C-SA)
- VLAN Identifier (C-Tag)
- Nutzdaten (C payload)
- Frame Check Sequence (FCS)

Die Provider Bridge (PB) übernimmt die Q-in-Q-Enkapsulierung und fügt dem Rahmen einen vom Provider verwalteten VLAN Identifier hinzu (S-Tag). Dieser Identifier wird im Access-Netz auf der Basis von IEEE 802.1ad für die Unterscheidung zwischen verschiedenen Kundennetzen verwendet.

Neue Verfahren für mandantenfähige Netze

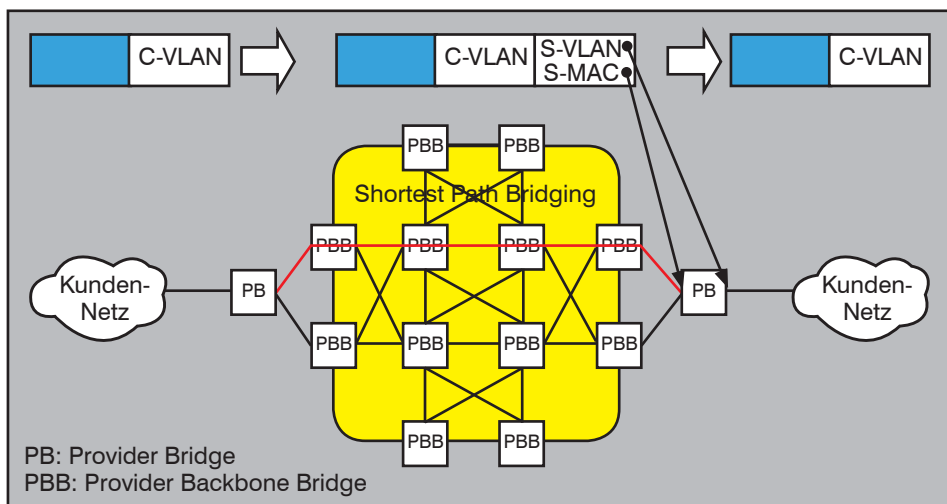


Abbildung 3: Neues Bridging-Verfahren

Über das Access-Netz gelangt der Rahmen zu einem Aggregierungs- oder Distributionsnetz auf der Basis von IEEE 802.1ah. Der Übergabepunkt zu diesem Netz ist die Provider Backbone Bridge (PBB), welche die Aufgabe der Encapsulierung gemäß 802.1ah übernimmt. Somit fügt die PBB dem Rahmen einen vollständigen MAC Header hinzu, einschließlich der im Backbone-Bereich B verwendeten und vom Service Provider verwalteten MAC-Adressen:

- Destination Address (B-DA)
- Source Address (B-SA)

Diese Header-Informationen dienen der Weiterleitung des Rahmens im Providernetz. Dabei werden die Tabellen mit den B-MAC-Adressen mittels des Routing-Protokolls IS-IS aktualisiert, und nicht wie bei IEEE 802.1D durch das „Lernen“ der MAC-Adressen. Auch das bei IEEE 802.1D vorgesehene Fluten von Paketen mit unbekannter Ziel-MAC-Adresse entfällt im Backbone.

Eine Carrier-Ethernet-Infrastruktur muss bestimmte Eigenschaften etablierter WAN-

Backbones wie SDH ebenfalls anbieten, wenn sie von einem Service Provider als Transportnetz genutzt werden soll. Zu diesen Eigenschaften gehört die schnelle Umschaltung bei Ausfällen, im SDH-Bereich Automatic Protection Switching (APS) genannt. In einem Transportnetz auf der Basis von Ethernet kann das Verfahren Spanning Tree aufgrund der o. g. Nachteile nicht genutzt werden. Geeigneter ist Link Aggregation gemäß IEEE 802.3ad. Dieses Verfahren ist jedoch in der bisher standardisierten Ausprägung nur zwischen zwei Enden einer Ethernet-Verbindung definiert, zum Beispiel zwischen zwei Switches. Erweitert man jedoch dieses Verfahren, kann es auf andere Szenarien angewandt werden. Ein solches Szenario ist in der Abbildung 4 dargestellt.

Die in der Abbildung 4 dargestellte Multi-Chassis Link Aggregation (MC-LAG) ist ein Verfahren, in dem analog zum sogenannten Linear APS bei SDH bei Ausfällen einer Zugangsleitung auf eine zweite Verbindung umgeschaltet wird.

MC-LAG nutzt ein Steuerungsprotokoll

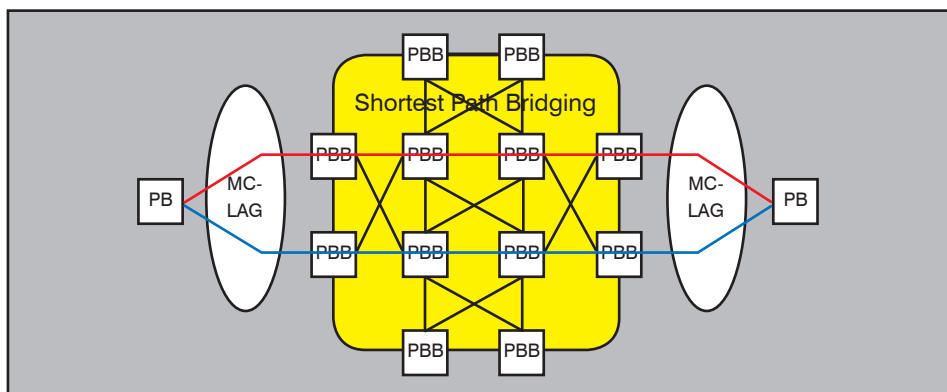


Abbildung 4: Multi-Chassis Link Aggregation

zwischen den beiden PBBs eines Paares. Das LACP (Link Aggregation Control Protocol, definiert in IEEE 802.3ad) wird zwischen PBB- und PB-Komponenten genutzt, um Ausfälle zu signalisieren.

Im Kern des Providernetzes bietet das Shortest Path Bridging (SPB) die Fail-over-Mechanismen, die auf dem Routing-Protokoll IS-IS basieren. IS-IS hat sich in Service-Provider-Netzen als robust und stabil erwiesen, so dass einer Nutzung dieses Protokolls zum „Routen“ von MAC-Adressen nichts im Wege steht.

Im Rahmen von IEEE 802.1aq wird SPB standardisiert. Die ersten Pre-Standard-Produkte sind verfügbar. Erste Interoperabilitätstests sind erfolgreich verlaufen. Mit der baldigen Verabschiedung des Standards wird gerechnet.

5. Fazit zu mandantenfähigen Ethernet-Backbones

Als Fazit dieses Abschnitts zu mandantenfähigen Ethernet-Backbones kann zusammengefasst werden:

- Ethernet kann als Technologie für mandantenfähige Backbones eingesetzt werden. Ein Ethernet-Backbone kann den Verkehr aus den angeschlossenen Kundennetzen ohne wesentliche Änderung des Rahmenformats übertragen, was die Kosten für das Netz minimieren wird.
- Zurzeit wird Ethernet in mandantenfähigen Backbones in der Regel mit anderen Verfahren wie MPLS kombiniert. Wenn man den Ethernet-Dienst so definiert, dass Ethernet-Rahmen (Frames) auf der einen Seite empfangen und auf der anderen Seite unverändert an das Zielnetz ausgeliefert werden, wird zurzeit als physikalische Schnittstelle zwischen dem Service-Provider und seinen Kunden Ethernet eingesetzt, der Transport über das Service-Provider-Netz jedoch in der Regel auf einer anderen Protokollebene mit einem anderen Verfahren wie SDH oder MPLS kombiniert.
- Die Provider und Hersteller arbeiten zugleich an Verfahren wie SPB, die das Potenzial haben, Verfahren wie MPLS und SDH langfristig auch abzulösen.

6. Elemente mandantenfähiger Netze

Für den Aufbau mandantenfähiger Netze werden grundsätzlich folgende Elemente benötigt (Abbildung 5):

- Logische Trennung der Verkehrsflüsse der Mandanten in LAN und WAN

Neue Verfahren für mandantenfähige Netze

- Kontrolle der Kommunikationsbeziehungen an Netzübergängen zwischen Mandanten, gemeinsam genutzten Ressourcen und externen Kommunikationspartnern
- Netzzugangskontrolle, die sicherstellt, dass Geräte, die an einem Netzsegment eines Mandanten angeschlossen sind, auch tatsächlich zu der entsprechenden Gruppe gehören

Logische Trennung der Verkehrsflüsse

Grundlage mandantenfähiger Netze ist zunächst die logische Trennung der Verkehrsflüsse.

Für die WAN-Übertragung sind dies, wie oben beschrieben, MPLS-VPN bzw. bei Carrier Ethernet einfach VLANs. Wenn man diese Trennung auf dem Campus im LAN fortsetzen möchte, setzt man auf Layer 2 zunächst wieder VLANs ein. Will man die VLANs nicht in der Fläche über einen kompletten Standort ausdehnen, kommt man um den Einsatz von Trennungsmechanismen oberhalb von Layer 2 nicht herum. Hier kann grundsätzlich wieder mit MPLS gearbeitet werden, was auch im LAN bei einer größeren Zahl von Mandanten oder bei einer gewissen Dynamik der Mandanten (neue Gruppen müssen öfter angelegt werden, bestehende Gruppen müssen wieder entfernt werden) durchaus in Betracht gezogen werden kann. Alternativ kann die logische Trennung auf Layer 3 durch den Einsatz von Virtual Routing and Forwarding (VRF) erfolgen. Dabei werden die VRF-Instanzen typischerweise per VLAN miteinander vernetzt, um auf einer gemeinsamen Hardware verschiedene virtuelle Layer-3-Netze zu schaffen.

Kontrolle der Kommunikationsbeziehungen an Netzübergängen

Meist ist ein Übergang zwischen den Netzen der einzelnen Mandanten bzw. von den Mandanten zu gemeinsam genutzten Diensten (z.B. DNS, Directory Services) erforderlich. Dabei müssen insbesondere die in die Netze eines Mandanten eingehenden Kommunikationsbeziehungen gefiltert werden. Typischerweise arbeitet man hier mit zentralen, entsprechend leistungsfähigen und hochverfügbaren Firewall-Systemen, die ggf. um Intrusion-Prevention-Funktionen ergänzt werden.

Die dabei zu verwaltenden Regelwerke können eine erhebliche Komplexität annehmen, da im Gegensatz zum Einsatz am Perimeter hier die Firewall internen LAN- und WAN-Verkehr filtern muss, d.h. mit dem gesamten im Intranet verwendeten Protokollapparat zurecht kommen muss. Dies beinhaltet möglicherweise ne-

ben der Filterung von Protokollen, die dynamisch Ports aushandeln (z.B. RTP und DCOM) auch die Erkennung von Sitzungen, die auf Basis von UDP aufgebaut werden (z.B. Authentisierungen via RADIUS).

Bei der Filterung der Kommunikation an den Netzübergängen ist die Verwendung verschlüsselter Protokolle zu beachten. Wenn es gewünscht ist, dass die Filterkomponenten (z.B. ein IPS) den verschlüsselten Verkehr analysieren, muss das Firewall-System um Verschlüsselungsendpunkte ergänzt werden, d.h. um entsprechende Proxies.

Insgesamt entsteht hier ein im Regelfall durchaus sehr komplexes System.

Netzzugangskontrolle zur Prüfung der Zugehörigkeit zu einem Mandanten

Nehmen wir an, ein Endgerät wird an ei-

nen aktivierten Netzwerk-Port angeschlossen, der einem Mandanten zugeordnet ist. Dann ist ein Mechanismus wünschenswert, der an dem Port prüfen kann, ob das Endgerät ebenfalls zu diesem Mandanten gehört. Nur wenn die Prüfung positiv ausfällt, wird der gewünschte Zugang zu den Ressourcen des Mandanten gewährt. Andernfalls wird der Zugang abgewiesen oder nur ein (erheblich) eingeschränkter Zugang gewährt. Diese als Authentisierung bezeichnete Prüfung der Identität des Endgeräts (bzw. des Nutzers des Endgeräts) sollte natürlich verlässlich sein, d.h. mit kryptographischen Mitteln erfolgen.

Analog könnte man fordern, dass für ein Endgerät, das an einem Netzwerk-Port angeschlossen wird, im Rahmen der Authentisierung festgestellt wird, zu welchem Mandanten das Gerät gehört, und nach erfolgreicher Authentisierung wird der Port

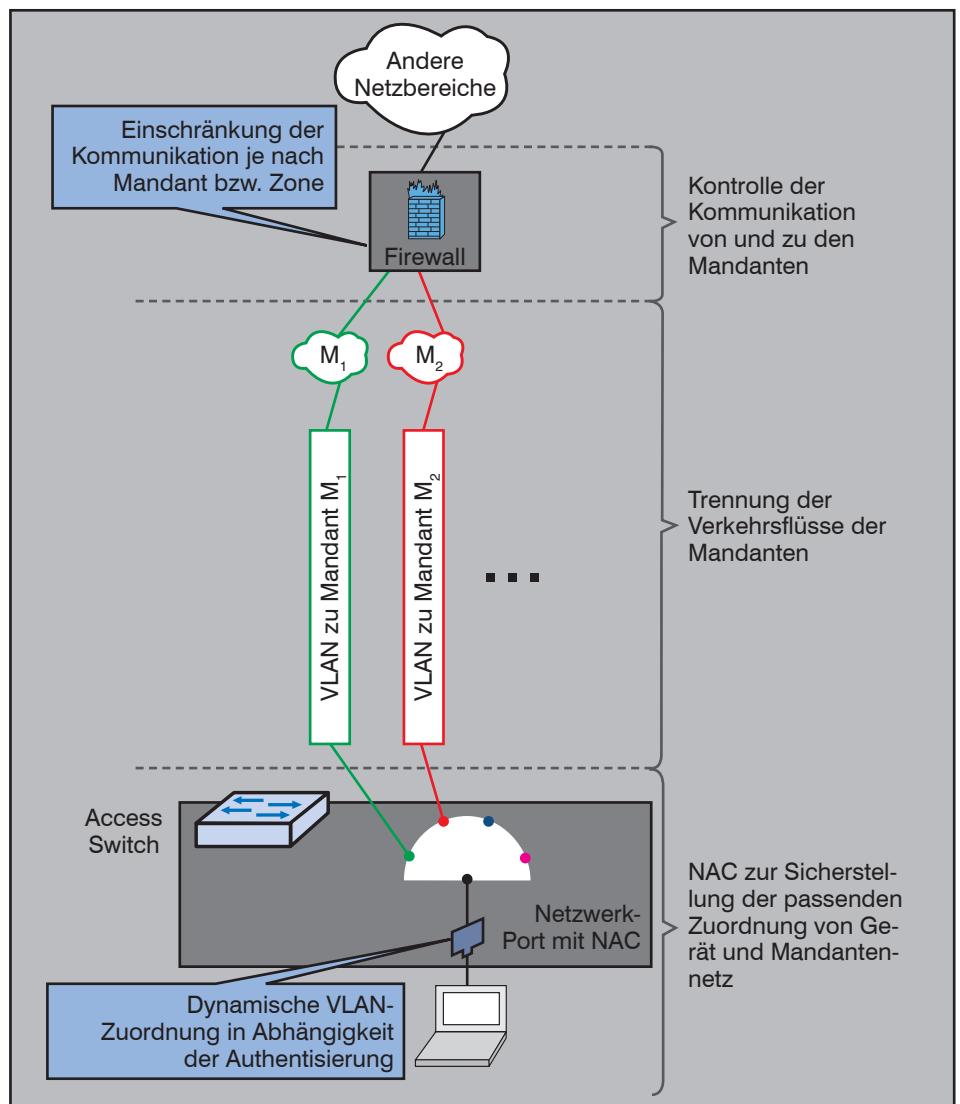


Abbildung 5: Elemente mandantenfähiger Netze

Neue Verfahren für mandantenfähige Netze

dynamisch einem VLAN zugewiesen, das in das entsprechende Mandantennetz führt.

Eine solche Netzzugangskontrolle ist dann notwendig, wenn durch andere Mechanismen (z.B. räumliche Trennung in Verbindung mit einer Zutrittskontrolle) eine passende Zuordnung von Endgerät und Mandantennetz nicht angemessen gesichert werden kann.

7. Netzzugangskontrolle mit IEEE 802.1X

Der Standard IEEE 802.1X spezifiziert eine Port-basierte Netzzugangskontrolle (Network Access Control, NAC) für Ethernet nach IEEE 802.3 und für WLAN nach IEEE 802.11.

IEEE 802.1X definiert verschiedene Rollen der beteiligten Netzelemente:

- Der **Supplicant** ist eine Software-Komponente auf dem Endgerät, die den Netzzugang anfordert und die in der Lage ist, bevor der eigentliche Netzzugang für die Übertragung von Nutzdaten bereitgestellt wird, eine Authentisierung durchzuführen.
- Der **Authenticator** bietet hierzu eine Schnittstelle, über die der Supplicant authentisiert werden kann und stellt den gewünschten Netzzugang her. Im LAN liegt diese Funktion typischerweise in demjenigen Switch, an dem das Endgerät unmittelbar angeschlossen ist. Im

WLAN wird diese Funktion vom Access Point bzw. WLAN Controller wahrgenommen.

- Der eigentliche Authentisierungsdienst wird zentral über den **Authentication Server** bereitstellt. Der Authentication Server ist typischerweise ein RADIUS-Server (siehe RFC 2865).

Für den Austausch der Authentisierungsinformationen zwischen Supplicant und Authentication Server dient das Extensible Authentication Protocol (EAP, siehe RFC 3748). Dabei erfolgt die Kommunikation über die LAN- bzw. WLAN-Schnittstelle zwischen Supplicant und Authenticator über das Layer-2-Protokoll EAP over LAN (EAPOL). Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und höheren Protokollebenen stattfindet. Die Kommunikation zwischen Authenticator und Authentication-Server geschieht meist über RADIUS, wobei eine EAP-Nachricht als RADIUS-Attribut übertragen wird (siehe RFC 2865). Für die Verwaltung der Daten der Geräte oder Nutzer, die sich mit IEEE 802.1X authentisieren, wird oft ein Verzeichnisdienst (Directory Service) wie z.B. LDAP verwendet, der vom RADIUS-Server angesprochen wird. Abbildung 6 zeigt die genutzten Protokolle im Überblick. Wichtig ist dabei, dass es keine direkte Kommunikation des Supplicant mit dem Authentication Server gibt. Der Authenticator ist der einzige für den Supplicant sichtbare Kommunikationspartner, der sich also quasi wie ein Au-

thentisierungs-Proxy verhält.

IEEE 802.1X gestattet nach einer erfolgreichen Authentisierung eine Autorisierung, die über eine simple Türöffnerfunktion hinausgeht. Der Authentication Server kann bei der Erteilung der Zugangserlaubnis zusätzlich eine Information für die Zuweisung eines VLANs oder einer Access Control List (ACL) für den Port, an dem der Supplicant angeschlossen ist, übertragen. Auf diese Weise kann dynamisch und individuell bzw. in Abhängigkeit von der Gruppenzugehörigkeit des Supplicant (der dabei ein Gerät oder einen Nutzer repräsentieren kann) eine Autorisierung der Kommunikation, d.h. insbesondere auch eine Zuordnung zu einem Mandantennetz, vorgenommen werden.

IEEE 802.1X wurde 2001 erstmalig verabschiedet, jedoch 2004 und zuletzt im Februar 2010 überarbeitet. IEEE 802.1X-2004 ist die aktuell in der Praxis noch meist verbreitete Version.

8. Problembereiche von IEEE 802.1X in der Fassung von 2004

Für WLAN hat sich IEEE 802.1X seit Jahren im Enterprise-Bereich massiv durchgesetzt. Im kabelbasierten LAN war der Einsatz jedoch lange eher die Ausnahme und erst seit 2009 ist eine steigende Tendenz sichtbar. Dies liegt daran, dass im kabelbasierten LAN technische Eigenheiten bestehen, die der Standard in den Fassungen von 2001 und 2004 nur unzu-

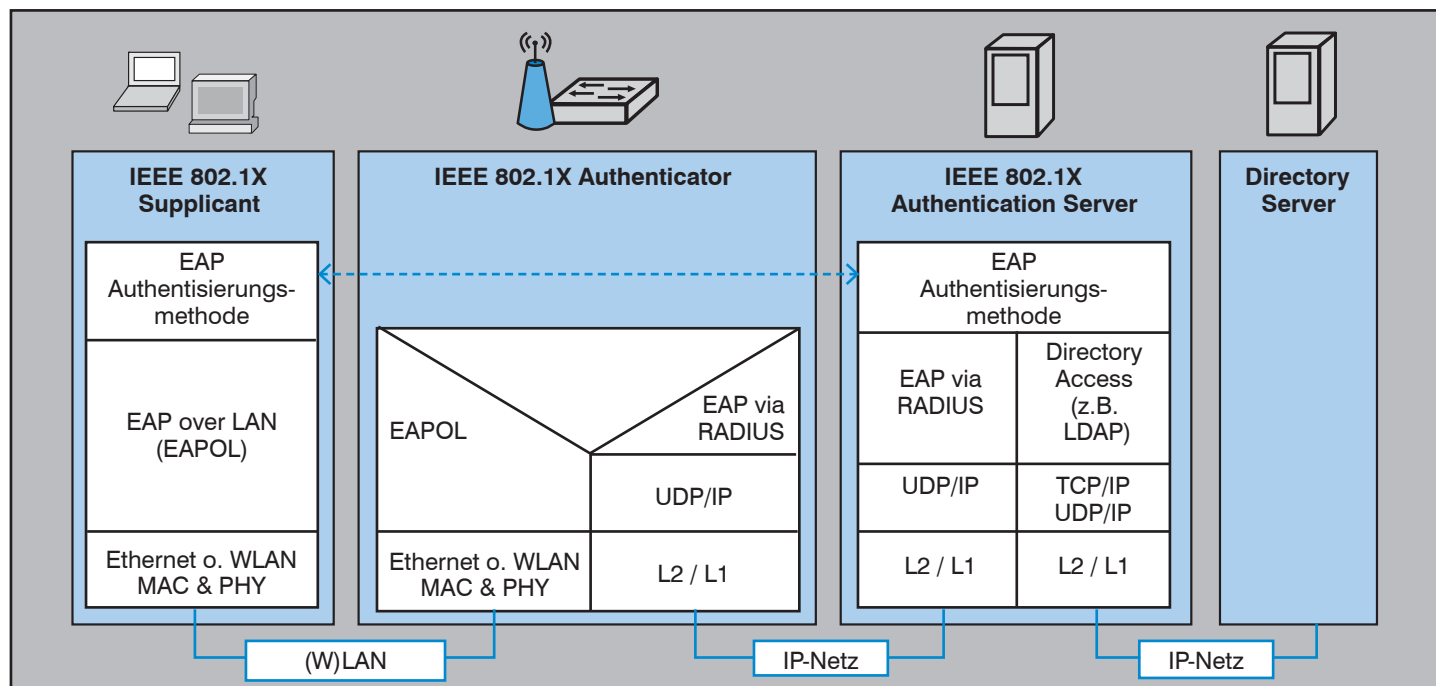


Abbildung 6: Im Rahmen der Authentisierung mit IEEE 802.1X genutzte Protokolle

Neue Verfahren für mandantenfähige Netze

reichend adressiert. Außerdem lässt IEEE 802.1X-2004 an entscheidenden Stellen empfindliche Lücken, die zu (teilweise sehr unzufriedenstellenden) herstellerspezifischen Implementierungen geführt haben, die sich an diesen Punkten so stark unterscheiden haben, dass von einem Standard eigentlich kaum noch geredet werden konnte.

Zu nennen sind unter anderem folgende Problembereiche:

- Kommunikation mit nicht authentisierten Systemen (Default Policy)
- Flexible Kombination von Authentisierungsmethoden
- Simultane Authentisierung mehrerer Endgeräte an einem Port
- Anfälligkeit gegenüber MAC-Adress-Spoofing

Kommunikation mit nicht authentisierten Systemen (Default Policy)

In der Praxis ist es notwendig, dass auch Geräten, die sich (noch) nicht erfolgreich authentisiert haben, ein eingeschränkter Netzzugang gewährt wird. Beispiele sind PXE Boot zur Softwareverteilung und der Zugriff des User Help Desk auf ein Gerät, das bedingt durch einen Fehler keine erfolgreiche Authentisierung durchführen konnte.

Hierzu muss ein Netzwerk-Port auch im nicht autorisierten Zustand im Forwarding State sein und z.B. durch eine spezielle VLAN-Zugehörigkeit in den Kommunikationsmöglichkeiten eingeschränkt werden (sogenannte Default Policy). Nach einer erfolgreichen Authentisierung erfolgt dann eine Zuweisung eines produktiven VLANs zu dem Port.

Eine solche Kommunikation mit nicht authentisierten Systemen wird zwar vom Standard IEEE 802.1X-2004 gestattet, ist aber nur in einem informellen Anhang des Standards beschrieben. Die Konsequenz ist natürlich, dass unterschiedlichste Implementierungen dieser Funktion existieren und manche Hersteller diese Funktion erst gar nicht umgesetzt haben.

Flexible Kombination von Authentisierungsmethoden

Um mit Geräten umzugehen, die kein IEEE 802.1X unterstützen, wie manche Drucker und andere Spezialgeräte, ist eine Kombination von IEEE 802.1X und einer RADIUS-basierten MAC-Adress-Authentisierung oft unerlässlich. Dabei versucht ein Port beispielsweise zunächst ein Gerät mit IEEE 802.1X zu authentisieren. Falls dies

nicht gelingt, wird die MAC-Adresse als Identitätsnachweis verwendet. Die kombinierte Authentisierung mit IEEE 802.1X und als Fallback mit MAC-Adresse ist nicht im Standard IEEE 802.1X beschrieben und als herstellerspezifisch einzustufen. Daher können sich die Implementierungen der Hersteller entsprechend deutlich unterscheiden und es ist zur Bewertung stets eine Einzelbetrachtung erforderlich.

Simultane Authentisierung mehrerer Endgeräte an einem Port

Größtes Problem in IEEE 802.1X-2004 ist die Limitierung der Spezifikationen für das kabelbasierte LAN auf eine strikte 1-zu-1-Beziehung zwischen Supplicant und Authenticator, d.h. ein Gerät pro Port.

Damit hat der Standard neben dem Anschluss eines Hubs oder eines Desktop-Switches an einen Port, der IEEE 802.1X aktiviert hat, auch den kaskadierten Anschluss von IP-Telefon und PC am PC-Port des IP-Telefons sowie die Nutzung von VMs im Bridged-Modus auf einem PC ausgeklammert.

Die Netzwerkausrüster haben daher in ihren Implementierungen den Standard durch proprietäre Funktionen ergänzt, die zwar im Grundsatz recht ähnlich sind, im Detail aber erheblich voneinander abweichen können. Das Prinzip ist dabei recht einfach: Für jede an einem Switch-Port neu gelernte MAC-Adresse erzeugt der Switch eine neue NAC-Sitzung für den Port, die per IEEE 802.1X oder per MAC-Adresse authentisiert wird (siehe Abbildung 7). Nur diejenigen MAC-Adressen, die einer authentisierten Sitzung zugeordnet werden können, erhalten einen Zugang. Auf diese Weise werden im Prinzip mehrere virtuelle Ports auf einem physischen Port geschaffen.

Anfälligkeit gegenüber MAC-Adress-Spoofing

Über IEEE 802.1X ist zwar die Authentisierung eines Systems bzw. eines Nutzers am System möglich, es erfolgt aber keine Authentisierung der über einen autorisierten Port übertragenen Pakete eines Endgeräts. Insbesondere findet keine Prüfung statt, ob die Pakete auch tatsächlich von dem Gerät stammen, auf dem der Supplicant, der sich authentisiert hat, läuft.

Ein Angreifer könnte unter der MAC-Adresse eines an einem Port authentisierten Supplicant an diesem Port einen Dialog mit der Infrastruktur führen, solange der Port autorisiert ist. Er benötigt hierzu allerdings einen Helfer, der sich erfolgreich authentisieren kann (siehe Abbildung 8).

Wenn eine NAC-Lösung basierend auf

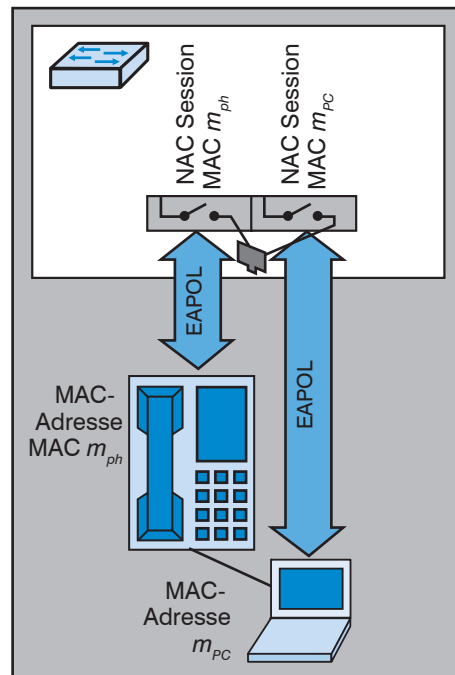


Abbildung 7: Simultane Authentisierung mehrerer Endgeräte an einem Netzwerk-Port am Beispiel von IP-Telefon und PC

der Version von 2004 des Standards IEEE 802.1X aufgebaut werden soll, muss diese Gefährdung bewertet werden. Entweder das Risiko wird eingegangen oder IEEE 802.1X-2004 macht an dieser Stelle keinen Sinn.

9. IEEE 802.1X-2010: Weiterentwicklung und Aufräumarbeit

Die Zusicherung von Vertraulichkeit und Integrität der über einen autorisierten Port übertragenen Pakete ist zunächst nicht Aufgabe eines Authentisierungsverfahrens. Hierzu muss generell die Sicherheitsarchitektur um eine Komponente für Verschlüsselung und/oder Integritätsprüfung erweitert werden. Für die verbindungslose Kommunikation in LAN/MAN werden diese Mechanismen in dem im August 2006 verabschiedeten Standard IEEE 802.1AE MAC Security (kurz: MACsec) beschrieben.

Das hierzu notwendige Schlüsselmanagement für den Aufbau von gesicherten Kommunikationsbeziehungen ist das wesentliche Element der Neuauflage von IEEE 802.1X, die Ende Februar 2010 verabschiedet worden ist. IEEE 802.1AE und IEEE 802.1X-2010 bilden dabei zusammen für das kabelbasierte LAN das konzeptionelle Pendant zur Absicherung von WLAN mit IEEE 802.11i, wie in Abbildung 9 gezeigt.

Das Grundprinzip für den Aufbau gesicherter Kommunikationsbeziehungen bei

Neue Verfahren für mandantenfähige Netze

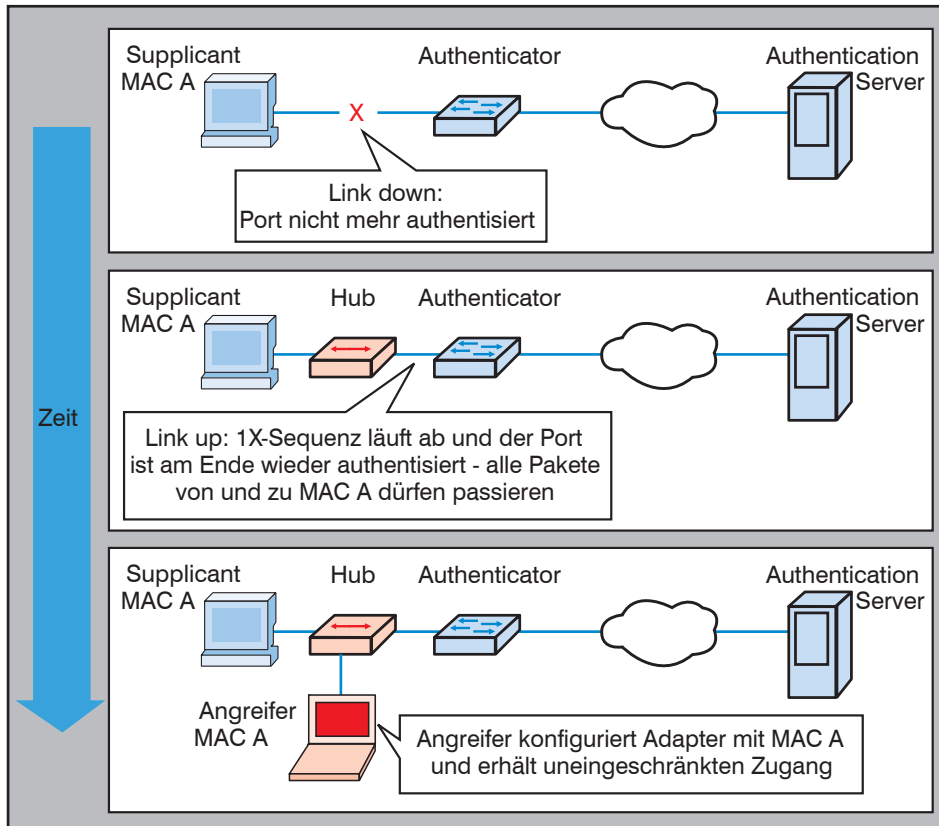


Abbildung 8: Umgehung von IEEE 802.1X-2004

IEEE 802.1X-2010 besteht darin, dass im Rahmen der Authentisierung Schlüsselmaterial in Supplicant und Authenticator bereitgestellt wird, welches dann zum Aufbau einer gesicherten Kommunikationsbeziehung mit IEEE 802.1AE verwendet werden kann (Abbildung 10). Dabei kann (analog zu WLAN gemäß IEEE 802.11i) wahlweise ein Pre-Shared Key (PSK) oder eine dynamische Schlüsselaushandlung mit EAP genutzt werden.

Die Neuauflage IEEE 802.1X-2010 beinhaltet neben der bereits angesprochenen Nutzung von IEEE 802.1AE für den Aufbau von Sicherheitszonen auf Layer 2 wei-

tere wichtige Elemente:

- Übernahme der Default Policy in den normativen Teil als erlaubte Option
- Möglichkeit der simultanen Authentisierung mehrerer Endgeräte an einem Port durch das Konzept virtueller Ports
- Absicherung von Zugang und Übertragung für Carrier Ethernet

10. IEEE 802.1AE MAC Security (MACsec)

MACsec ergänzt das MAC-Layer der Netz-

elemente eines LAN um eine Hop-by-Hop-Absicherung, die Daten-Vertraulichkeit, -Integrität, -Authentisierung für die verbindungslose Kommunikation in einem LAN schafft (Abbildung 11). Die Default Cipher Suite verwendet den Advanced Encryption Standard (AES) mit 128 Bit Schlüssel. Die Verschlüsselung ist dabei optional. Kernelement ist die Authentisierung der Daten, welche neben den Nutzdaten auch die MAC-Adressen berücksichtigt, was insbesondere die eben beschriebene Spoofing-Attacke automatisch aushebelt.

Neben Punkt-zu-Punkt LAN-Verbindungen werden Multi-Access LAN und Shared-Media LAN (exklusive IEEE 802.11 WLAN, denn hier wirkt IEEE 802.11i) berücksichtigt. Dabei geht es insbesondere um den kaskadierten Anschluss von PC und IP-Telefon an einen Port eines Access Switch und um die Behandlung von VMs mit virtuellen MAC-Adressen auf einem Endgerät.

MACsec wurde für die Schaffung von Sicherheitszonen auf Layer 2 in LAN und Carrier Ethernet spezifiziert und geht über die reine Absicherung des Endgeräteanschlussbereichs deutlich hinaus.

Außerdem wurde MACsec für eine hohe Verschlüsselungsleistung konzipiert (40 Gbit/s und mehr). Hintergrund ist hier der Einsatz von MACsec im Datacenter-Bereich, wo die Möglichkeit einer Verschlüsselung unter hohen Leistungsanforderungen (ohne unwirtschaftlich zu werden) immer mehr gefordert wird. Ein Beispiel ist die Kopplung zweier Rechenzentren auf Layer 2 über Glasfaserstrecken. Wenn die Übertragungsstrecken das Unternehmensgelände verlassen bzw. über unsichere Bereiche laufen und ein hoher Schutzbedarf der Daten besteht (was bei einer RZ-Kopplung praktisch immer der Fall ist), kommt man eigentlich um eine Verschlüsselung nicht herum.

Eine dedizierte Verschlüsselung aus-

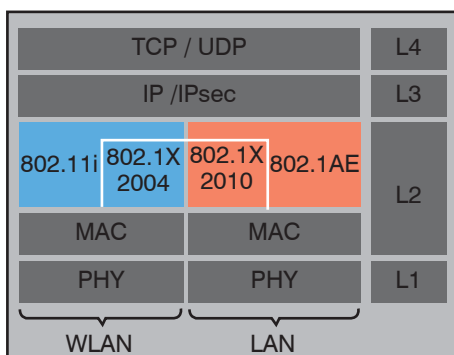


Abbildung 9: Einordnung von IEEE 802.1AE und IEEE 802.1X-2010 in den Protocol Stack

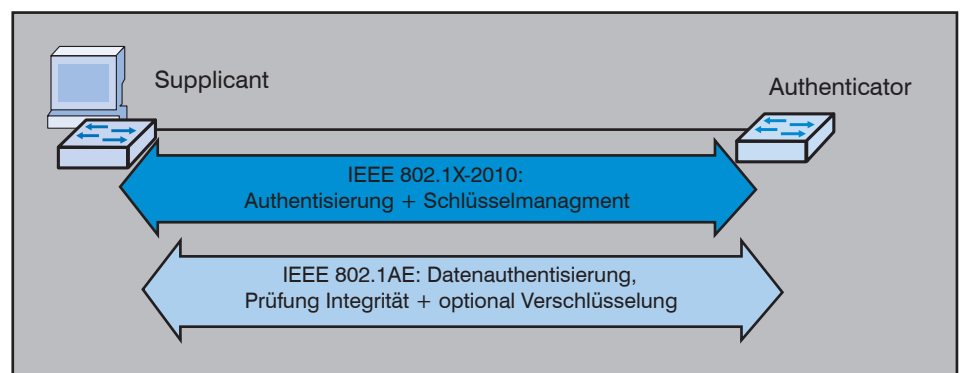


Abbildung 10: Beziehung zwischen IEEE 802.1X-2010 und IEEE 802.1AE

Neue Verfahren für mandantenfähige Netze

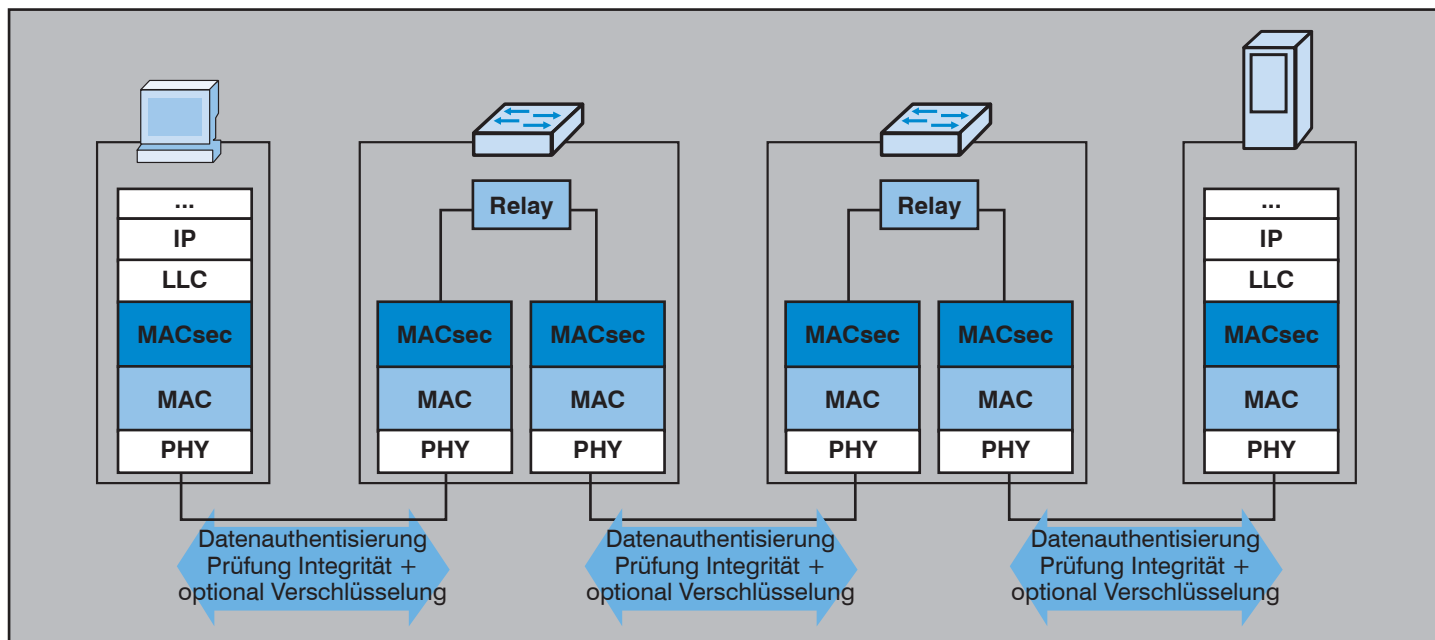


Abbildung 11: Hop-by-Hop-Sicherheit mit MACsec

schließlich der Daten mit hohem Schutzbedarf auf höheren Protokollebenen (z.B. IPsec und TLS) ist zwar grundsätzlich machbar, erfordert jedoch aufwendige Einzelfallbetrachtungen. Daher besteht schnell der Wunsch nach einer pauschalen Verschlüsselung auf Layer 2. Hier kamen in der Vergangenheit proprietäre Layer-2-Kryptoboxen zum Einsatz. MACsec bietet hier eine standardisierte Alternative, die keine zusätzlichen Kryptoboxen mehr benötigt, da diese Funktion mit MACsec in die Switches bzw. Bridges integriert ist.

Durch diese Skalierbarkeit der Leistung vom Endgeräteanschluss bis zum Backbone setzt sich MACsec von Sicherheitsmechanismen auf höheren Protokollebenen wie IPsec und TLS, die bei den Leistungsanforderungen moderner LANs im Campus- und Datacenter-Bereich immer mehr an Grenzen stoßen, deutlich ab.

Aufbau sicherer Kommunikationsbeziehungen

Die Schaffung von gesicherten Vertrauensbereichen (Sicherheitszonen) im LAN erfolgt bei MACsec durch den Aufbau sogenannter Secure Connectivity Associations (CAs), wie in Abbildung 12 gezeigt. Im einfachsten Fall sind dies zwei Parteien, etwa ein Endgerät und ein Switch oder zwei Switches.

Für den Aufbau sicherer Kommunikationsbeziehungen muss MACsec notgedrungen das Layer-2-Frame-Format erweitern. Dabei kommt ergänzend ein Security TAG und als kryptographische Prüfsumme ein Integrity Check Value (ICV) hinzu. Letzterer schützt im Wesentlichen die ge-

samten Layer-2-Daten, also nicht nur den Payload, sondern auch MAC-Quelladresse und -Zieladresse. Eine Station, die ein Paket empfängt, kann die im Paket übertragene kryptographische Prüfsumme auswerten und feststellen, ob das Paket tatsächlich von der angegebenen MAC-Adresse kommt und ob der Inhalt manipuliert worden ist (Abbildung 13). Es besteht also automatisch ein Schutz vor MAC-Adress-Spoofing, d.h. MAC-Adressen werden durch MACsec zu verlässlichen Identifikationsmerkmalen.

Als Konsequenz muss für Switches zwingend neue Hardware eingesetzt werden. Eine Migration zu IEEE 802.1AE hat daher eher einen langfristigen Charakter.

Den grundsätzlichen Ablauf des Aufbaus einer abgesicherten Kommunikationsbeziehung zeigt zusammengefasst Abbildung 14. Im ersten Schritt erfolgt optional eine Authentisierung mit EAP bzw. IEEE 802.1X, verbunden mit einer Autorisierung, die eine VLAN- und/oder ACL-Zuweisung beinhalten kann. Mit dieser Authentisierung wird dynamisch ein symmetrisches Schlüsselmaterial abgeleitet. Alternativ kann ein statischer PSK verwendet werden.

Auf dieser Basis wird in einem zweiten Schritt das Schlüsselmaterial über das MACsec Key Agreement Protocol (MKA) zwischen den beteiligten Port Access Entities (PAEs), d.h. zwischen Supplicant und Authenticator, verhandelt. Die-

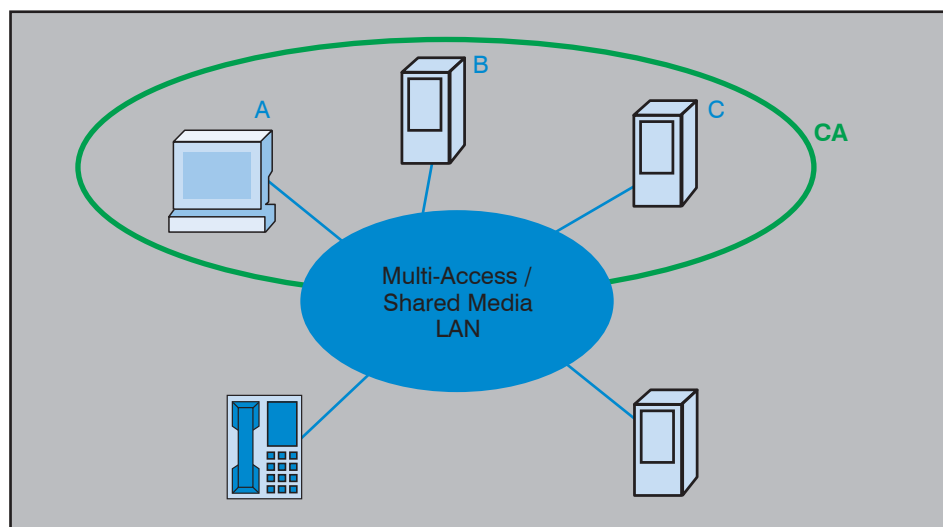


Abbildung 12: Secure Connectivity Association (CA) zwischen den Stationen eines Vertrauensbereichs

Neue Verfahren für mandantenfähige Netze

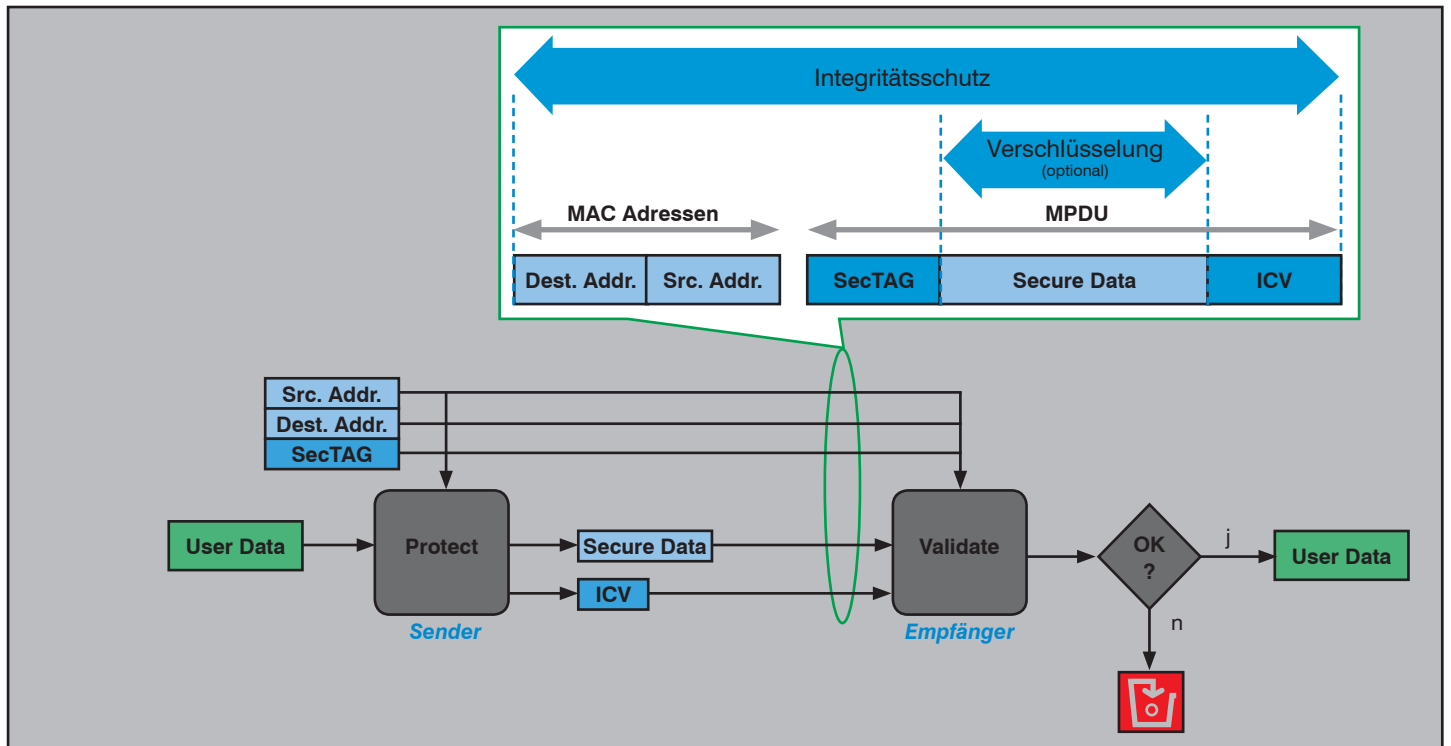


Abbildung 13: Sicherung der Übertragung mit MACsec

ses Material wird zur jeweiligen MAC Security Entity (SecY) übertragen, die hiermit die CA aufbauen kann (Schritte 3 und 3.1 in Abbildung 14). Im letzten Schritt kann dann der Port freigeschaltet werden. CAs müssen nicht individuell zwischen zwei Parteien bestehen, es sind auch Group CAs möglich.

viele Strecken abgesichert werden müssen, bzw. ob das Risiko durch die Verwendung eines statischen PSK akzeptiert werden kann. Durch eine Group CA entsteht mit MACsec dann im Prinzip ein gesichertes VPN auf dem Provider-Netz. Unter anderem sind dabei folgende Varianten möglich, die auch miteinander kombiniert

werden können:

- MACsec zwischen Customer Bridges:** Customer-Bridges, die an eine Provider Bridge angeschlossen sind, können untereinander über MACsec gesichert über das Provider-Netz kommunizieren (siehe Abbildung 15). Damit wird die

Verschlüsselungsendpunkte bilden bei MACsec die Switches untereinander bzw. die Switches und die Endgeräte. Es gibt also keine Ende-zu-Ende-Absicherung wie etwa bei TLS. Den Switches muss also vertraut werden.

11. Carrier Ethernet und IEEE 802.1X-2010

Die Unterstützung von Carrier Ethernet ist ein integraler Bestandteil von MACsec und von IEEE 802.1X-2010. Damit ist sowohl die Absicherung der Kommunikation zwischen Customer Bridges über das Provider-Netz hinweg, zwischen Customer Bridge und Provider-Netz als auch zwischen adjazenten Provider Bridges möglich.

Insbesondere können so mit MACsec die WAN-Strecken transparent für höhere Protokolle zielgerichtet für ausgewählte Kunden-VLANs abgesichert werden. Dabei werden individuelle CAs oder eine Group CA zwischen den beteiligten Stationen mit MKA aufgebaut. Die Rolle von EAP hängt hier stark davon ab, ob nur wenige oder

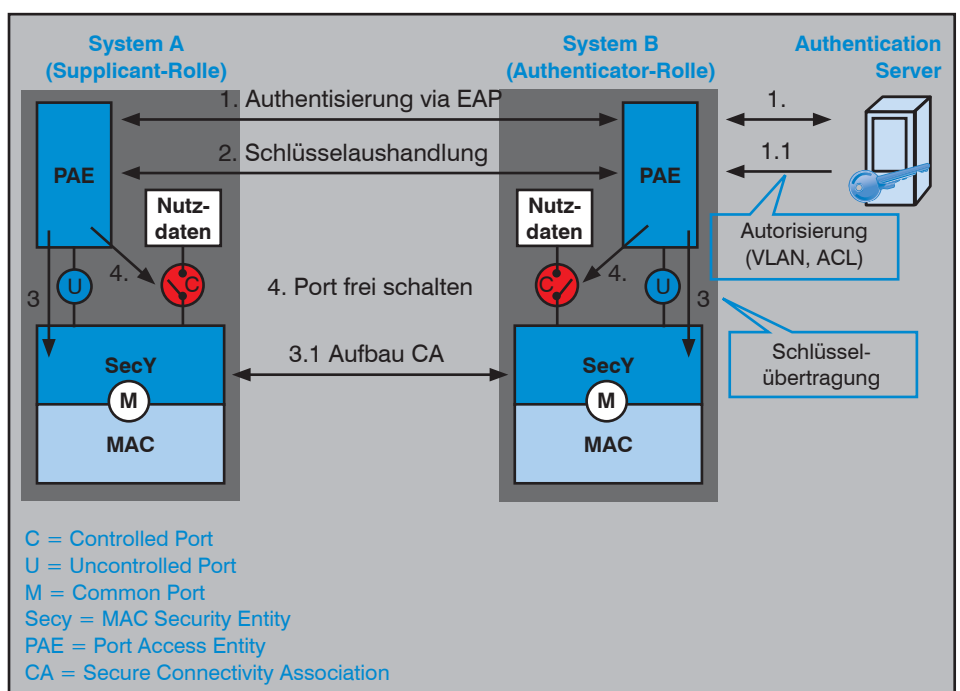


Abbildung 14: Schritte für den Aufbau einer abgesicherten Kommunikationsbeziehung mit IEEE 802.1X-2010 unter Verwendung von EAP

Neue Verfahren für mandantenfähige Netze

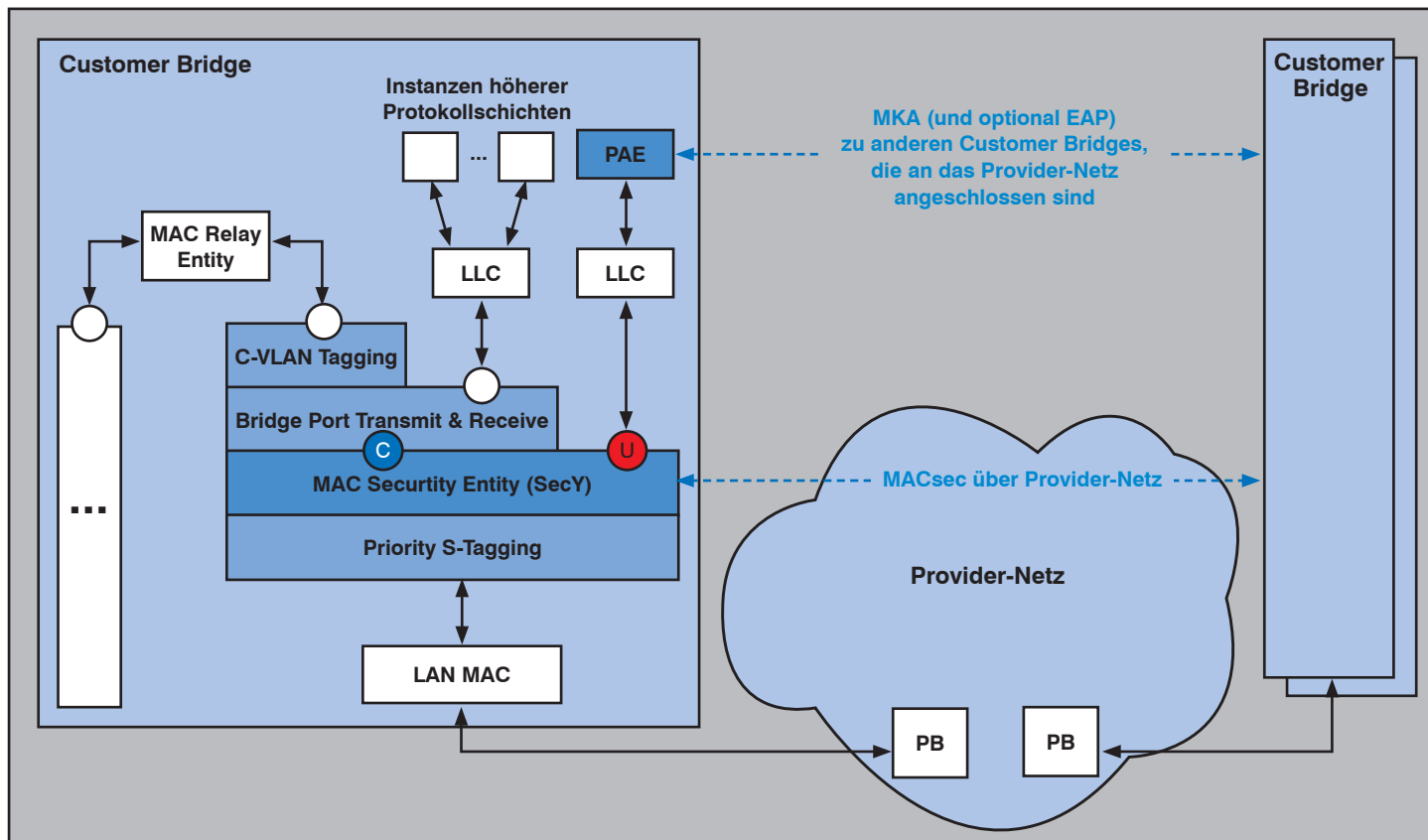


Abbildung 15: Absicherung der Übertragung zwischen Customer Bridges über ein Provider-Netz

gesamte Übertragung der Nutzdaten zwischen den Kundennetzen abgesichert. Ungesichert ist jedoch die Provider-spezifische Information wie S-VLAN, Priority und äußere MAC-Adressen.

2. MACsec zwischen Customer Bridge und Provider Bridge: Die Verbindung zwischen Customer Bridge und Provider Bridge kann mit den beschriebenen Mitteln natürlich ebenfalls mit MACsec abgesichert werden (Abbildung 16). Hierzu müssen den Kunden die zu verwendenden Credentials für den Aufbau einer kundenspezifischen CA mitgeteilt werden. Wenn hier ein höheres Sicherheitsniveau erreicht werden soll, sind PSKs eigentlich nicht Stand der Technik, d.h. EAP ist dann eher das Mittel der Wahl. MACsec kann aber auch im Provider-Netz selbst eingesetzt werden.

3. IEEE 802.1X zwischen Customer Bridge und Provider Bridge aber ohne MACsec: Der Anschluss einer Customer Bridge an eine Provider Bridge kann mit den Mitteln von IEEE 802.1X authentisiert werden (mit PSK oder EAP), ohne dass anschließend eine CA mit MACsec aufgebaut wird. Dies schützt eigentlich nur vor versehentlichem Fehlanschluss.

12. Produktunterstützung IEEE 802.1X-2010 und MACsec

Auf Seiten der Netzerkäufer ist bislang immer noch Cisco am weitesten. In einem ersten Schritt hatte Cisco mit TrustSec für die Serie Nexus 7000 eine Implementierung von IEEE 802.1AE herausgebracht. Hier wurde zunächst der Aufbau von hoch-performanten Sicherheitszonen im RZ adressiert. TrustSec ist konform zu IEEE 802.1X-2010, d.h. insbesondere ist die Verwendung von IEEE 802.1X für das dynamische Schlüsselmanagement umgesetzt worden. Seit Frühjahr 2010 gibt es TrustSec auf den Switches der Serie Catalyst 3750-X und 3560-X. Damit ist die Implementierung von IEEE 802.1AE auch im Bereich des Endgeräteanschlusses angekommen. Bei Catalyst 3750-X und 3560-X wird IEEE 802.1X-2010 und MACsec jedoch nur auf den Downlink-Ports unterstützt.

Um MACsec sinnvoll im Endgerätebereich zu nutzen, müssen Switch und Endgerät IEEE 802.1X-2010 unterstützen. Es gibt aktuell jedoch nur wenige NICs, die MACsec unterstützen. Weiterhin gibt es derzeit auch noch keine Integration von IEEE 802.1X-2010 in den nativen Windows Suppliment zur Unterstützung von MACsec. Der erste Suppliment, der

dies leistet, ist der Cisco AnyConnect Client in der Version 3.0. Dabei verwendet der Client möglichst eine MACsec-Funktion der Hardware. Steht diese nicht zur Verfügung, erfolgt die Absicherung (durch Integritätssicherung und optional Verschlüsselung) in Software.

Geräte, die eine TrustSec-Hardware unterstützen, können auf den mit MACsec abgesicherten Links Nutzergruppen kryptographisch voneinander trennen. Hierzu dient der Security Group Tag (SGT), der Bestandteil des TrustSec-Layer-2-Paketformats ist. Im Rahmen von TrustSec hat Cisco zusätzlich das Security Group Tag Exchange Protocol (SXP) entwickelt, um Geräten, die keine TrustSec Hardware unterstützen, Informationen über den SGT, d.h. die Gruppenzugehörigkeit, zu übermitteln. Über SXP erfolgt die Zuordnung einer IP-Adresse zu einem SGT. SXP ist als Migrationsinstrument zu TrustSec wichtig. Außerhalb einer mit MACsec abgesicherten Verbindung liefert ein SGT keine höhere Sicherheit als ein VLAN oder eine VRF-Instanz. Eine sichere Trennung von Mandanten erfordert den durchgängigen Einsatz von MACsec.

Eine interessante Frage ist jedoch, ob TrustSec zusammen mit SXP bereits jetzt schon eine Alternative zu VRF für den

Neue Verfahren für mandantenfähige Netze

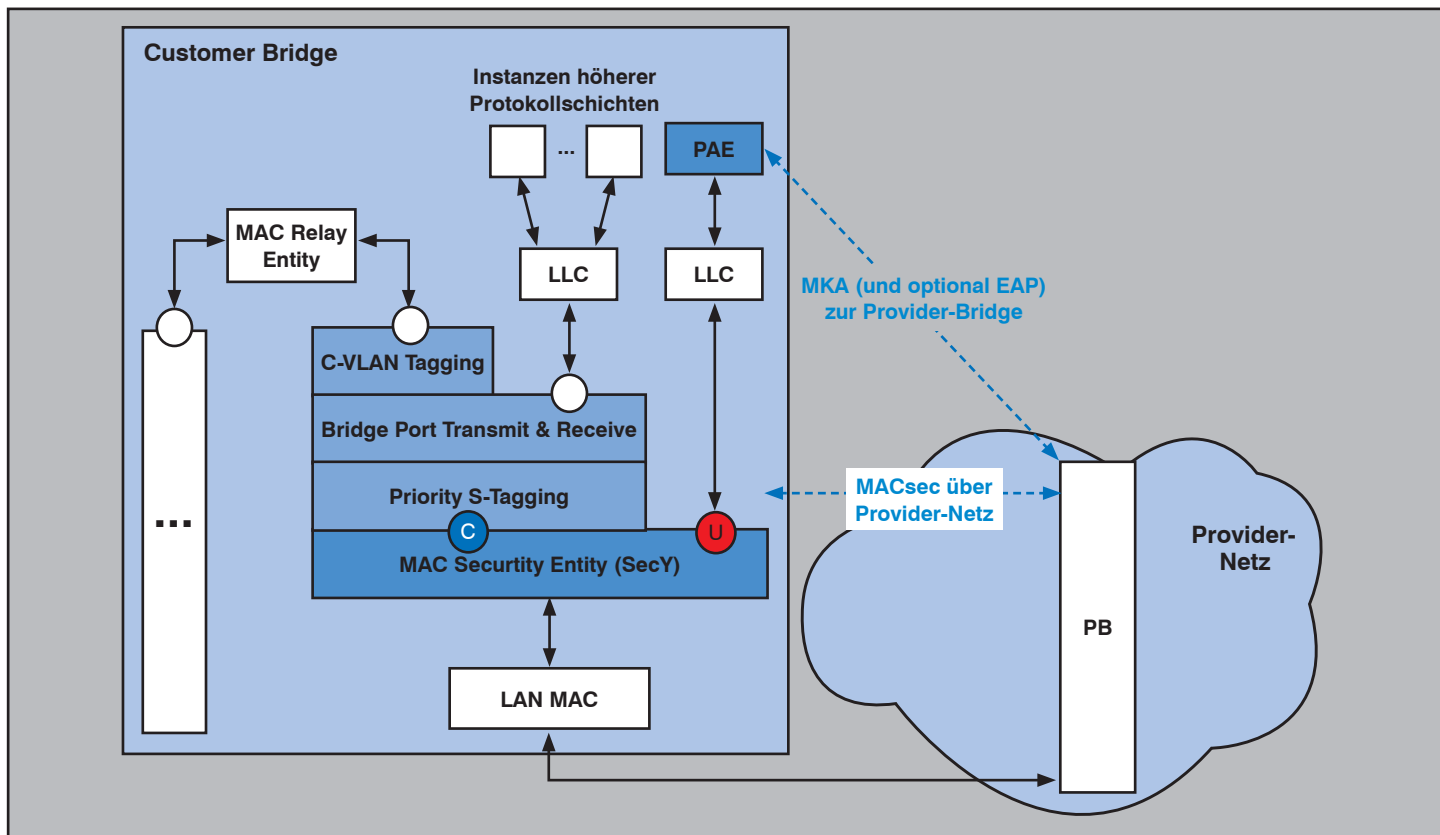


Abbildung 16: Absicherung der Übertragung zwischen Customer Bridge und Provider Bridge

Aufbau eines mandantenfähigen LAN darstellt. VRF ist eine seit Jahren bewährte Technik, die inzwischen von diversen Herstellern unterstützt wird. Die Zuordnung VRF zu MPLS-VPN ist ebenfalls praxiserprobt. Die Skalierbarkeit von VRF ist allerdings begrenzt und die Fehlersuche komplex. Es ist grundsätzlich möglich, mit SXP eine vergleichbare Trennung von Mandanten zu implementieren. Jedoch ist das erreichte Sicherheitsniveau zum heutigen Zeitpunkt nicht automatisch höher als das mit VRF erreichte. Daher kann ein Vorteil von SXP/TrustSec nur darin bestehen, dass SXP besser skaliert, die Komplexität in der Konfiguration geringer und die Fehlersuche weniger aufwendig ist.

Fassung von 2010 ein hohes Sicherheitsniveau durch MACsec geschaffen werden.

Allerdings ist IEEE 802.1X-2010 auch ohne MACsec von Bedeutung, da mit der normativen Berücksichtigung der Default Policy, der Erweiterung der Autorisierung um ACLs und des Konzepts virtueller Ports für die simultane Authentisierung mehrerer Endgeräte wichtige, bisher proprietäre Elemente im Standard spezifiziert wurden.

Für Carrier Ethernet kann mit IEEE 802.1X-2010 eine sichere Trennung der Mandanten geschaffen werden. Auf Layer 2 war dies bisher eine Domäne proprietärer Kryptoboxen.

Es bleibt die Frage, wann andere Netzwerkausrüster nachziehen. Nachdem Cisco vor etwas mehr als zwei Jahren mit TrustSec den Markt betreten hat, ist ungewöhnlich, dass zwischenzeitlich noch kein Mitbewerber seine Produkte ebenfalls mit MACsec-Funktion ausgestattet hat. Cisco könnte natürlich auch auf das falsche Pferd gesetzt haben. Mit den steigenden Anforderungen an eine sichere LAN-Kommunikation, im RZ-Bereich an eine sehr hohe Verschlüsselungsleistung auf Layer 2 und im Carrier-Ethernet-Bereich an den Aufbau sicherer Layer-2-VPN gibt es aber eigentlich keine Alternative zu MACsec und IEEE 802.1X-2010.

13. Fazit zur Rolle von IEEE 802.1X-2010 für mandantenfähige Netze

Der Standard IEEE 802.1X-2010 schließt entscheidende Lücken der Vorversion von 2004 und ist ein wesentliches Element für den Aufbau flächendeckender mandantenfähiger Netze. Bisher unterstützt jedoch lediglich Cisco diesen Standard konsequent. Produkte, die den Standard in der Version von 2004 mit herstellereigenen Elementen ergänzen, können natürlich ebenfalls für den Aufbau flächendeckender mandantenfähiger Netze eingesetzt werden, jedoch kann erst mit der

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen: <http://www.comconsult-akademie.de/de/registrierung.php>