

IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 9: Netzsicherheit - Schicht 2: Data Link Layer

Einschub: BSI empfiehlt Deinstallation v. Java

- 10.01.13: gefährliche Schwachstelle in Java
 - kritische Sicherheitslücke in aktueller Java Version 7 Update 10
 - bereits im großen Stil für Cyber Angriffe ausgenutzt
 - Einschleusen und aktivieren von Code im Betriebssystem über MBeanInstatiator
 - Java Sicherheitsarchitektur wird umgangen; Zugriff auf den Classloader
 - s. CVE-2013-0422 (vom 12.01.13)
 - Exploit-Kits existieren bereits; Angriffe mit geringem Aufwand möglich
 - drive-by-Angriffe werden massiv zunehmen
 - Empfehlung: Java Plugins deaktivieren
- 11.01.13: BSI-Empfehlung: komplette Deinstallation von Java
- 11.01.13: Mozilla und Apple deaktivieren Plugin automatisch
- 13.01.13: Oracle kündigt Patch an

Inhalt

■ Virtualisierung von Netzen

- Virtual Private Networks
- VLAN

■ Point-to-Point Protocol (PPP)

- Authentisierungsprotokolle:
 - PAP, CHAP, EAP

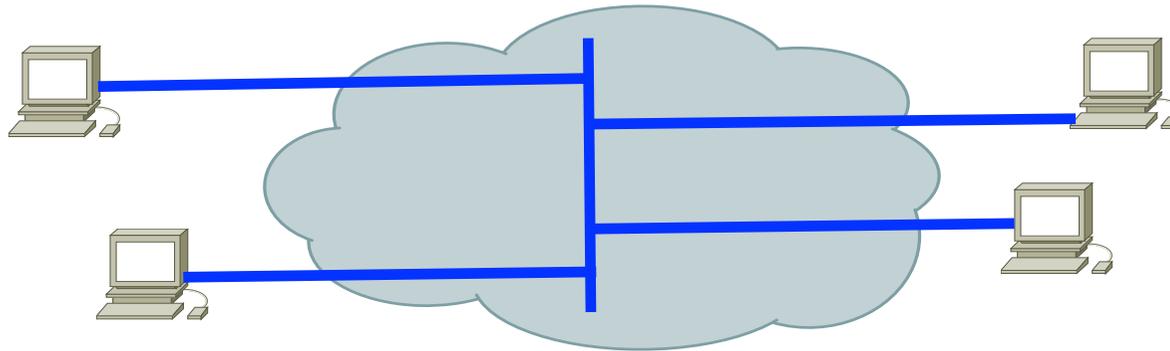
■ Point-to-Point Tunneling Protocol (PPTP)

■ Layer 2 Tunneling Protocol (L2TP)

■ IEEE 802.1x

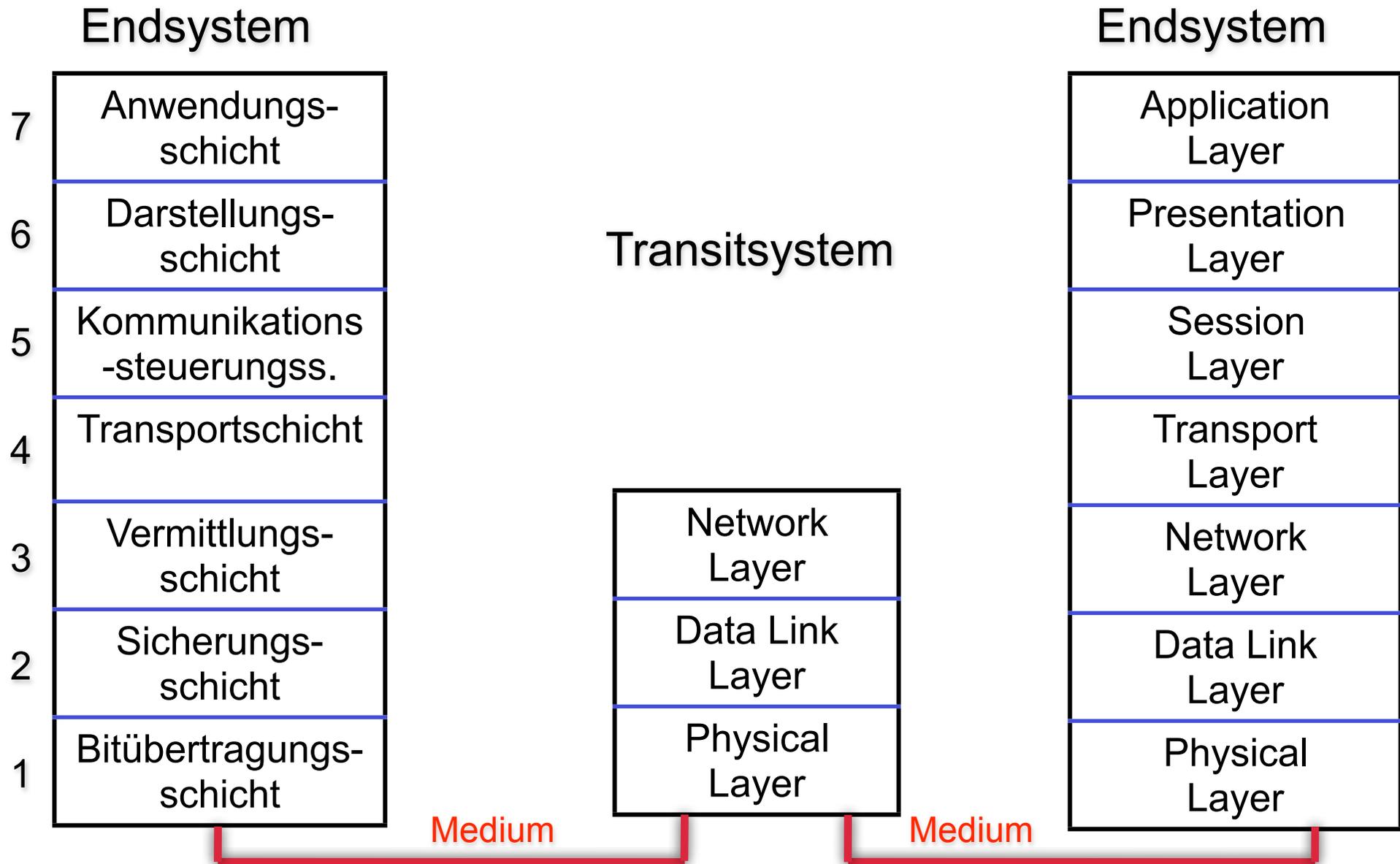
Virtual (Private) Network

- Grundidee:
Nachbildung einer logischen Netzstruktur („Local Area Network“ oder eines „nicht öffentlichen“ Netzes) in beliebigen Topologien/Technologien, z.B. auch über das Internet



- Das „virtuelle“ Netz soll u.a. bezüglich *Vertraulichkeit* und *Datenintegrität* mit physischen LANs vergleichbar sein
- Virtualisierung auf jeder Schicht des OSI-Modells möglich

Rückblick: ISO/OSI Schichtenmodell (Kapitel 2)



Virtual Network auf Schicht 1

- Virtual Private Wire Service (VPWS)
 - Provider bietet Punkt zu Punkt Verbindung

- Virtual Private Line Service (VPLS)
 - Provider bietet Punkt zu Multipunkt Verbindungen

- Beispiel:
Optical Private Link oder Optical Private Network (OPN)
 - Provider betreibt Glasfaserinfrastruktur
 - Kunde erhält eine Wellenlänge (Farbe) in dieser Infrastruktur
 - Kunde kann diese nutzen wie einen dedizierten Schicht 1 Link
 - Kunde muss sich um Routing, Bridging, etc. selbst kümmern
 - Über dieselben Glasfasern werden auch andere Kunden bedient

Virtual Network auf Schicht 2/3/4

■ Schicht 2:

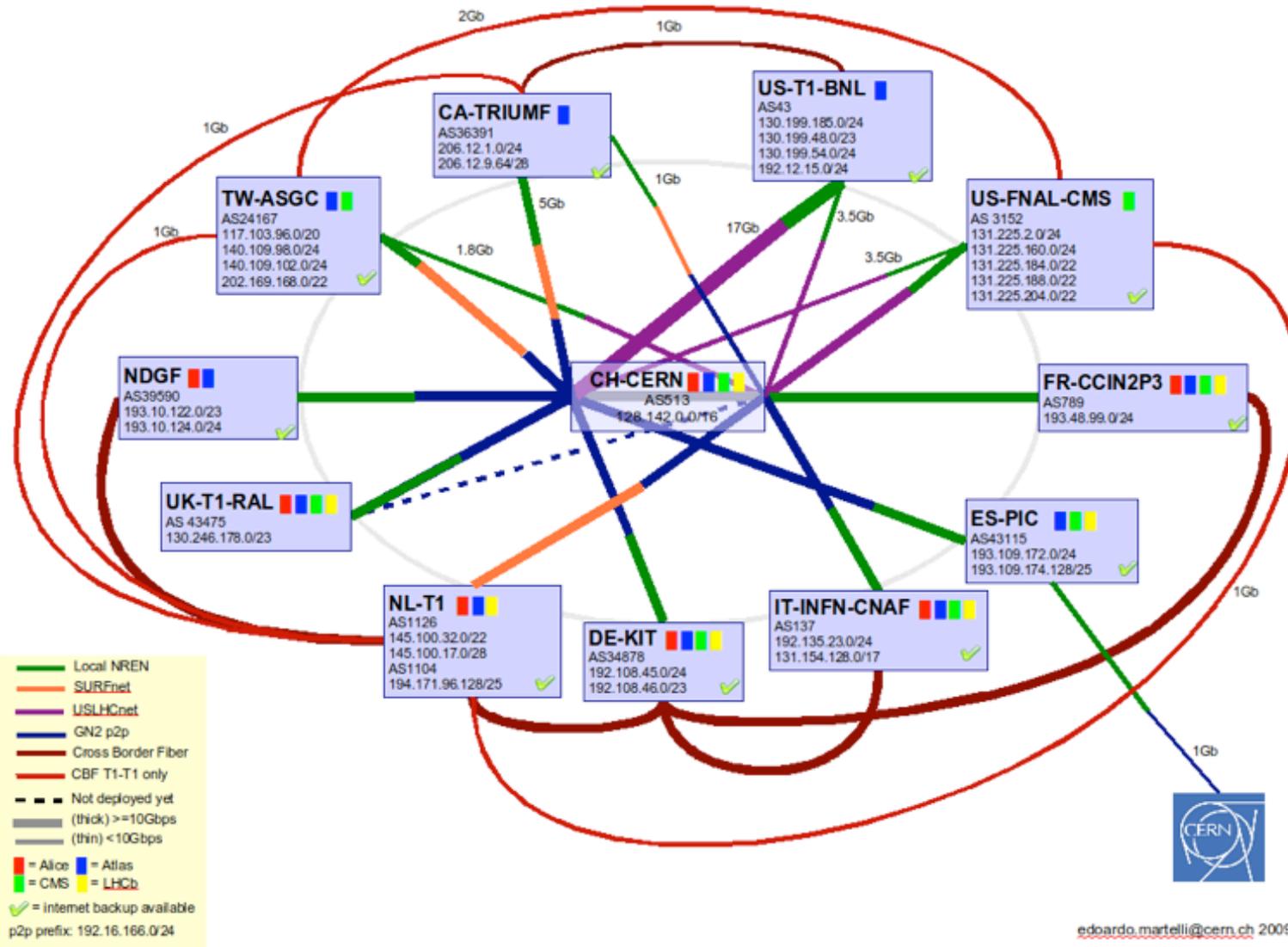
- Virtual LAN (VLAN)
 - Mehrere LAN Broadcast Domains über den selben physischen Link
 - Standard: VLAN Tagging (IEEE 802.1Q)
- Virtual Private LAN Services (Achtung: Abkürzung auch VPLS)
 - Verbindet physisch getrennte (V)LANs miteinander
- Point-to-Point Verbindungen
- Layer2 Tunneling Protocol
-

■ Schicht 3 und höher:

- IPSec
- SSL / TLS
- OpenVPN
- ...

Beispiel für OPN: Large Hadron Collider

LHCOPN – current status

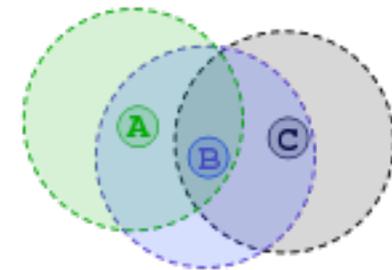


- Ca. 15 Petabytes an Rohdaten pro Jahr
- Auswertung verteilt auf über 100.000 CPUs
- Verteilung an ca. 6.000 Benutzer in über 450 Instituten

edoardo.martelli@cern.ch 20091103

Aufgaben der Schicht 2

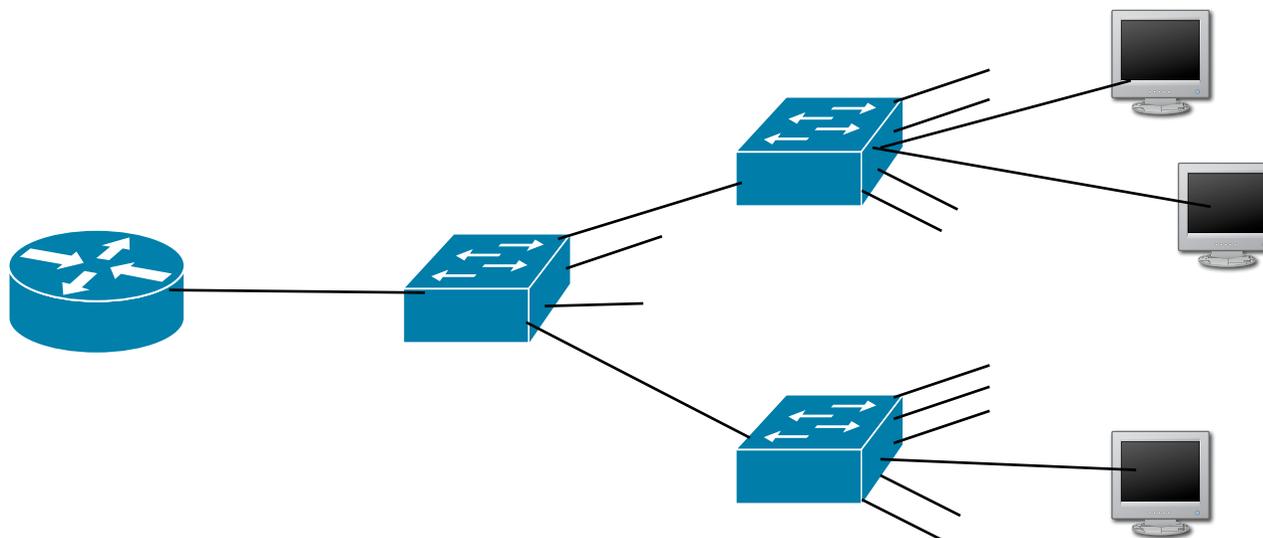
- Fehlerfreie Übertragung von Frames (Rahmen)
 - Aufteilung von Bitströmen in Frames
 - Fehlerkontrolle über Prüfsummen (z.B. Cyclic Redundancy Check, CRC)
- Flusskontrolle (Verhindert, dass der Empfänger mit Frames überflutet wird und diese verwerfen muss)
- Medienzugriffsverfahren für gemeinsam genutztes Übertragungsmedium
 - CSMA/CD bei Ethernet (IEEE 802.3)
 - CSMA/CA bei WLAN (IEEE 802.11)
 -



WLAN: Problem der „hidden stations“

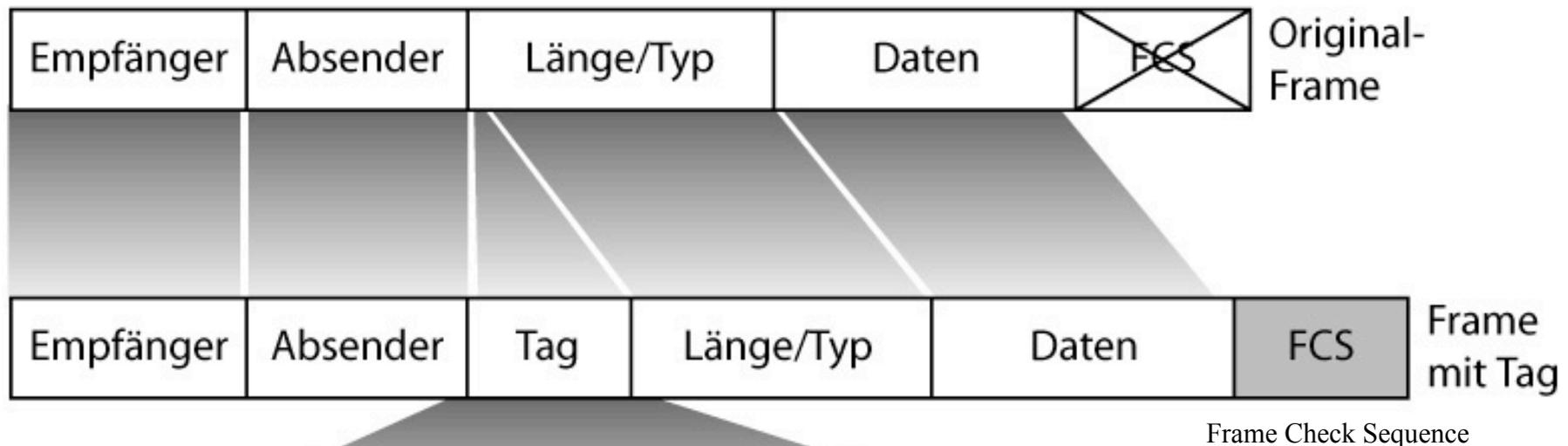
Virtual LAN (VLAN)

- LAN-Infrastruktur über mehrere Switches (Gebäude) hinweg
- Logisch verschiedene LANs auf einer Netzkomponente
- Wunsch nach Verkehrsseparierung
- Heute Standard in Unternehmens- und Hochschulnetzen
 - Von den meisten Switchen im Consumer-Bereich nicht unterstützt

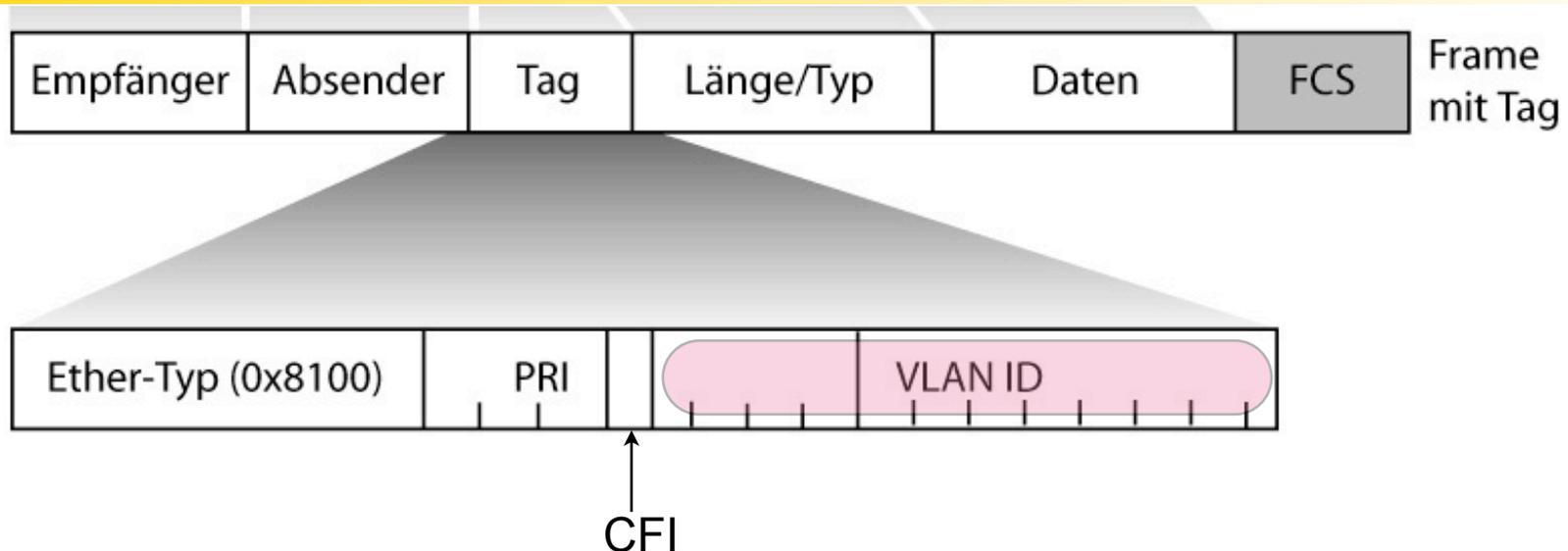


VLAN: Datenpakete

- Virtual Local Area Network (VLAN); IEEE 802.1Q
- VLAN definiert Broadcast-Domäne
- Idee: Erweiterung des Ethernet-Frame um sog. Tag



VLAN: Tag Format



■ Erweiterung des Ethernet-Frame um 32-bit Tag:

- ❑ TPID (Tag Protocol Identifier): konstant 0x8100; d.h. 802.1Q Tag Information im Frame enthalten (2 Byte)
- ❑ PRI (Priority): Priorisierung nach 802.1p (3 Bit)
- ❑ CFI (Canonical Format Indicator): MAC Adressen in kanonischer Form (1 Bit); bei Ethernet 0; sonst (z.B. Token Ring) 1
- ❑ **VLAN-ID**: Identifizierung des VLANs („VLAN NR.“) (12 Bit)
 - ID 0 = „kein VLAN“, ID 0xFFF ist reserviert
 - Somit 4094 verschiedene VLANs möglich

PPP: Überblick

- Punkt-zu-Punkt Protokoll; Entwickelt für Verbindungsaufbau über Wählleitungen
 - DSL, ISDN, Modem, Mobilfunk, Funk, serielle Leitungen,....
 - WAN-Verbindungen zwischen Routern
 - Angelehnt an HDLC (Highlevel Data Link Control); Schicht 2 Protokoll
- Spezifiziert in RFC 1661, 1662 und 2153
 - Frame Format mit Begrenzungssymbolen (Delimiter) und Prüfsumme
 - Link Control Protocol (LCP) für:
 - Verbindungsauf- und -abbau
 - Test
 - Aushandeln der Konfiguration (u.a. Nutzdatenlänge pro Frame)
 - Network Control Protocol (NCP) :
 - Aushandeln der Konfiguration der unterstützten Schicht 3 Protokolle (z.B. IP, IPX, Appletalk,...), verschiedene Schicht 3 Protokolle über einen PPP-Link möglich
- Weitere Varianten: PPPoE (over Ethernet), PPPoA (over ATM)

PPP: Sicherheitsdienste

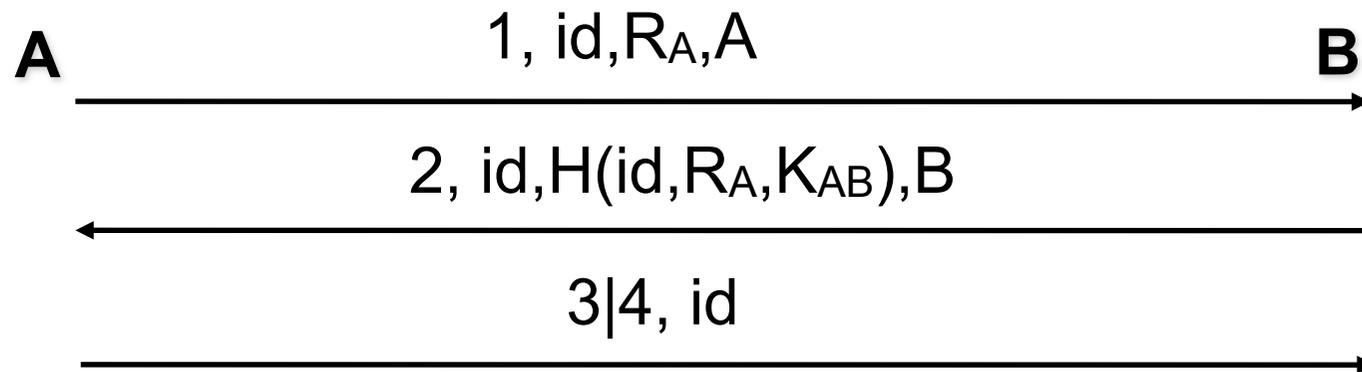
- Authentifizierung optional
- Im Rahmen der LCP-Aushandlung der Konfiguration kann jeder Partner eine Authentifizierung fordern
- Definierte Authentifizierungsprotokolle:
 - Password Authentication Protocol (PAP)
 - Challenge-Handshake Authentication Protocol (CHAP)
 - Extensible Authentication Protocol (EAP)

Password Authentication Protocol (PAP)

- Spezifiziert in RFC1334
 - Authentisierende Entität kennt ID und Passwort aller Clients
 - Client wird mit LCP zur Authentisierung via PAP aufgefordert
 - Client schickt ID und Passwort **im Klartext**
 - Server schickt im Erfolgsfall ACK
-
- Keine Verschlüsselung, Übertragung der Passwörter im Klartext
-
- ➔ Unsicheres Protokoll
- RFC 1334: „Any implementations which include a stronger authentication method (such as CHAP, described below) **MUST** offer to negotiate that method prior to PAP.“

Challenge-Handshake Authentication Protocol: CHAP

- (Auch) RFC1334 und RFC1994
- Periodische Authentisierung durch 3-Way-Handshake Protokoll
- Basiert auf gemeinsamen Geheimnis (Passwort) K_{AB}
- A (Authenticator) fordert B zur Authentisierung auf:



- id: 1 Byte Identifier („incrementally changing“) gegen Replay-Angriffe
 - R_A : Zufallszahl, H: Hash Verfahren, im Standard MD5
 - 3 = success; 4 = failure
- Auth-Request kann später beliebig neu geschickt werden

Sicherheitsrisiko PAP-Fallback

- Viele Clients unterstützen immer noch Server, die nur PAP anbieten
 - Für Client-Hersteller einfach zu implementieren
 - Abwärtskompatibilität vom Markt gewünscht
 - Die meisten Anwender kennen den Unterschied zwischen PAP, CHAP, etc. sowieso nicht: Hauptsache, es funktioniert!

- Man-in-the-middle-Angriff
 - Client kommuniziert nicht direkt mit Server, sondern über Angreifer
 - Angreifer gibt sich als „nur PAP“-Server aus
 - Angreifer erhält Klartext-Passwort vom Client
 - Somit kann der Angreifer u.a. als CHAP-fähiger Client gegenüber dem richtigen Server auftreten

Extensible Authentication Protocol (EAP)

- RFC3748 und RFC5247
- Authentisierungs-Framework, bietet gemeinsame Funktionen und Aushandlungsmechanismen für konkretes Verfahren (als Methode bezeichnet)
- Rund 40 Methoden werden unterstützt:
 - EAP-MD5; äquivalent zu CHAP
 - EAP-OTP (One Time Password); vgl. Kapitel 8
 - EAP-GTC (Generic Token Card)
 - EAP-TLS (Transport Layer Security) vgl. Abschnitt über SSL/TLS
 - EAP-SIM (Global System for Mobile Communications (GSM) Subscriber Identity Modules (SIM))
- Herstellerspezifische Methoden:
 - LEAP (Cisco) Lightweight Extensible Authentication Protocol
 - PEAP (Cisco, Microsoft, RSA) Protected Extensible Authentication Prot.
 -

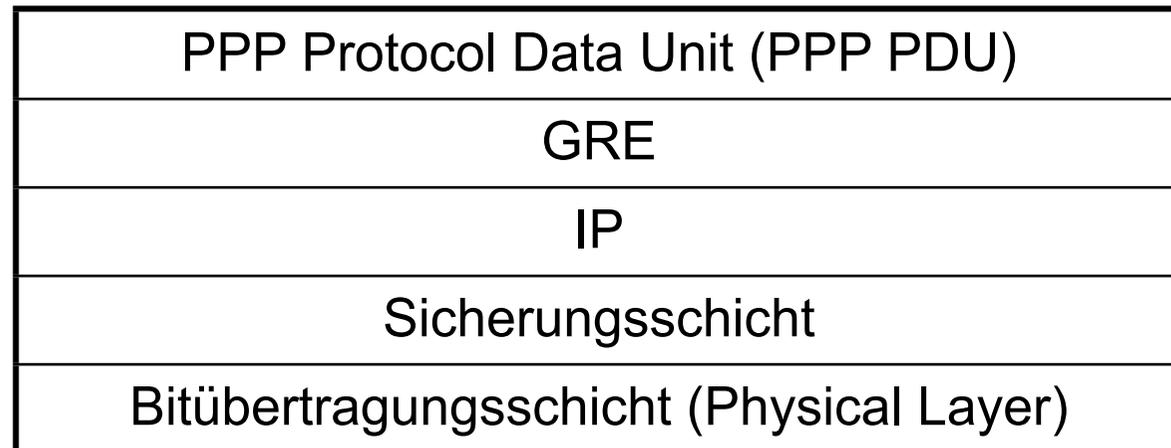
EAP Grundlagen

- EAP kann Sequenz von Verfahren verwenden
- Verfahren muss aber vollständig abgeschlossen werden, bevor neues beginnt
- Request - Response Schema mit Success / Failure Antwort
- Beispiel: EAP-GTC (Generic Token Card, RFC3748)
 - Nutzbar für verschiedenste Authentisierungs-Token-Implementierungen
 - Request beinhaltet Nachricht, die dem Nutzer angezeigt wird
 - Nutzer gibt Token-Information ein
 - Server prüft und antwortet



Point to Point Tunneling Protocol (PPTP)

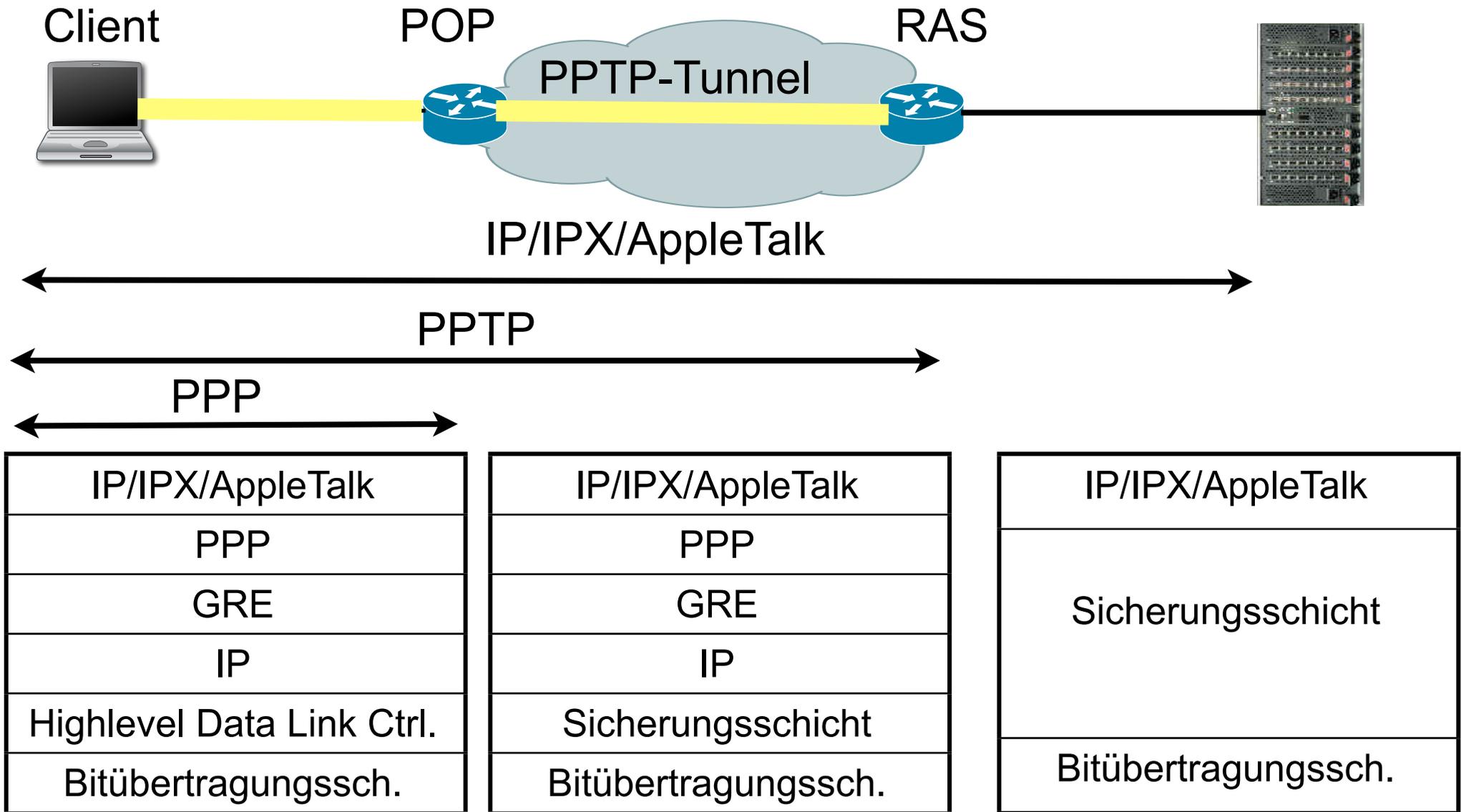
- PPP wurde für „direkt“ verbundene Systeme entwickelt
- Idee von PPTP (RFC2637):
 - Ausdehnung von PPP über Internet
 - PPTP realisiert Tunnel durch / über das Internet
 - Transport von PPP PDUs in IP-Paketen
 - Dazu werden PPP PDUs mit Generic Router Encapsulation Protocol (GRE) gekapselt
 - GRE ist ein Schicht 4 Protokoll



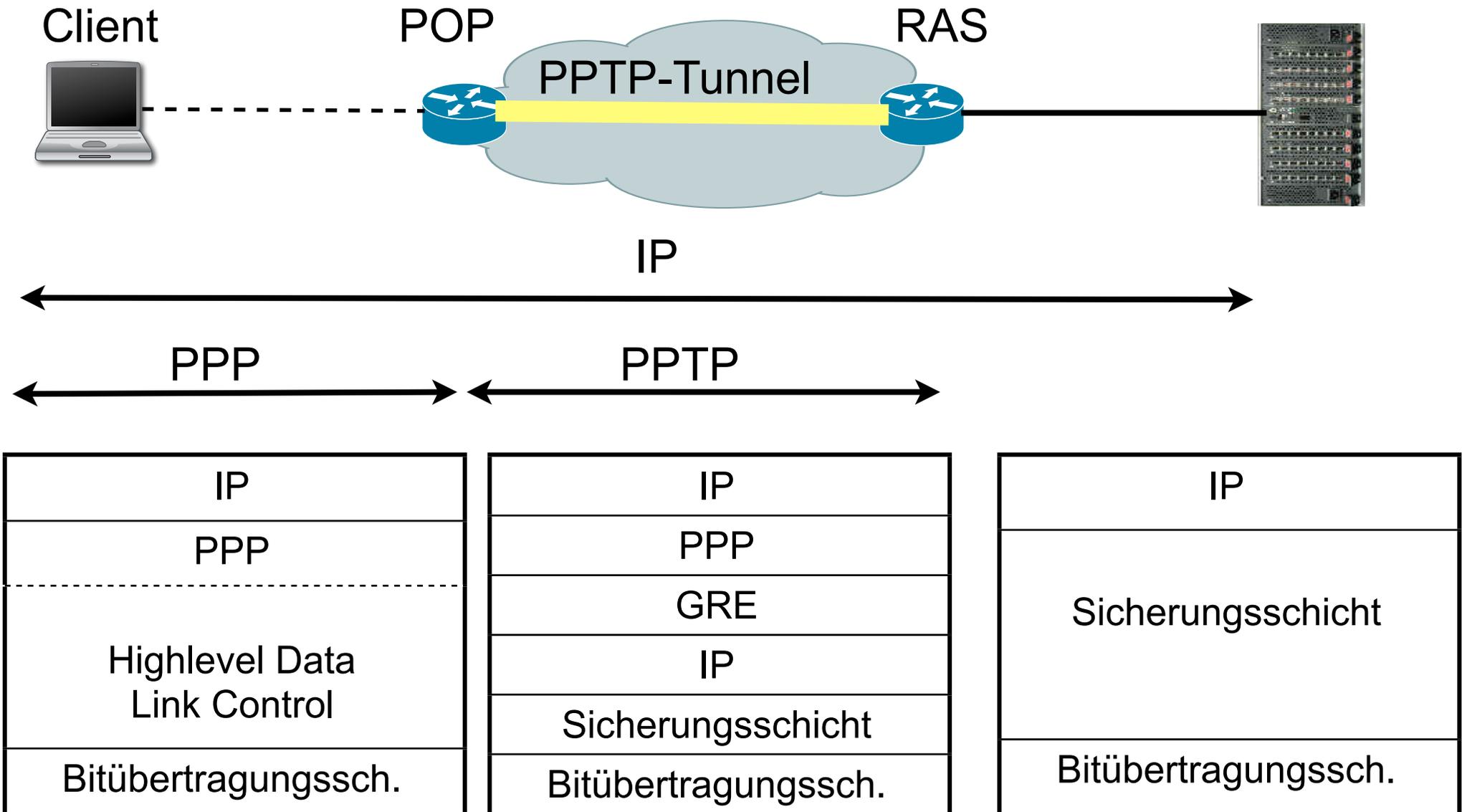
PPTP: Anwendungsfälle

- Eines der ersten einfach zu konfigurierenden VPN-Protokolle mit weiter Verbreitung seit Microsoft Windows 95
- Verbindung eines Clients mit einem Remote Access Server (RAS)
 - Voluntary Tunneling
 - Client setzt PPTP aktiv ein
- Verbindung eines ISP Point of Presence (POP) mit einem PPTP Remote Access Server
 - Compulsory Tunneling
 - Client weiß nichts von PPTP
 - ISP POP handelt als Proxy (Stellvertreter) des Clients

PPTP: Voluntary Tunneling



PPTP: Compulsory Tunneling

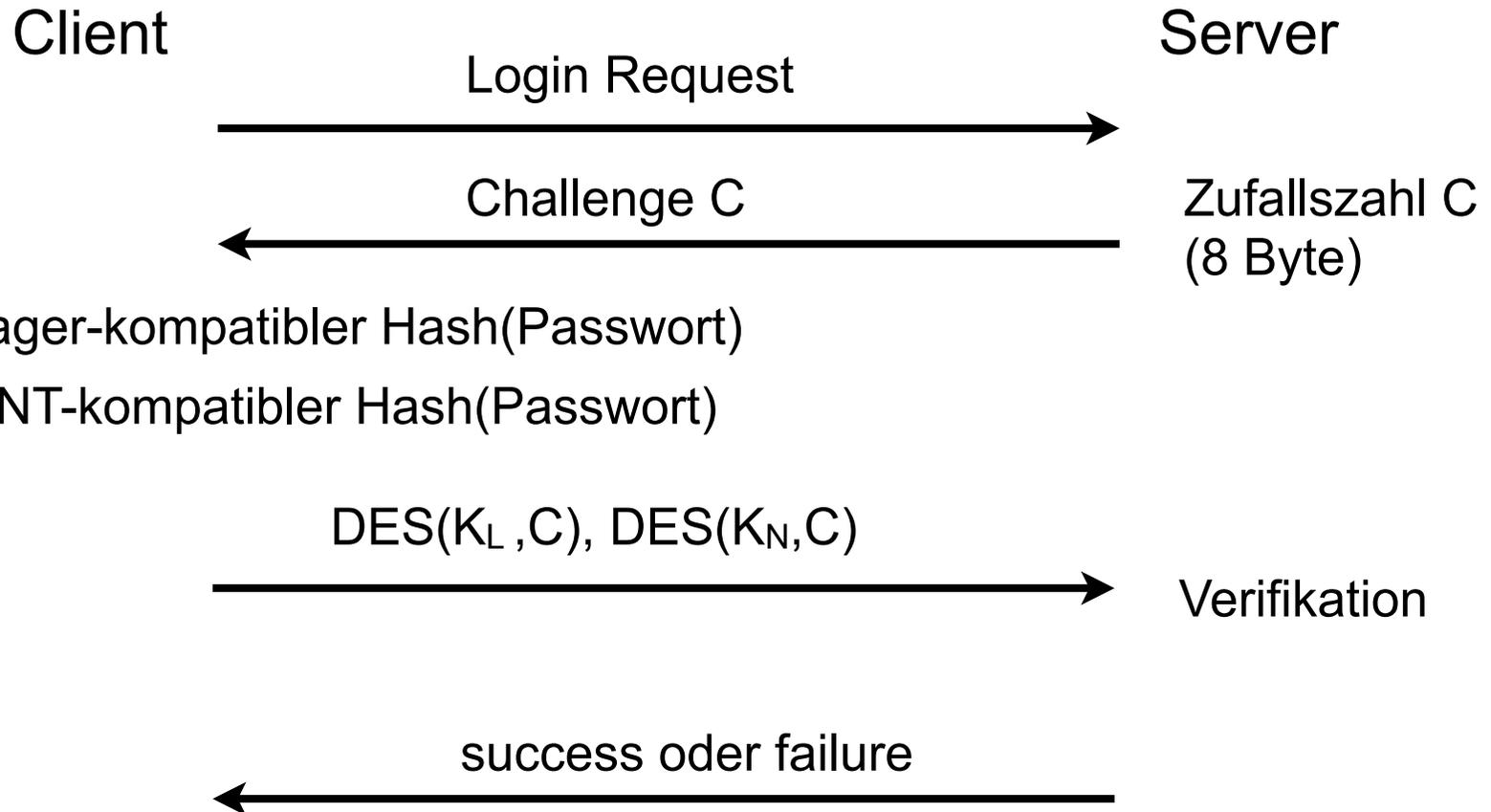


PPTP Sicherheit

- Von Microsoft entwickelt [RFC 2637] als Teil des Remote Access Service (RAS)
- Microsoft-eigene Erweiterungen:
 - Microsoft PPP CHAP (MS-CHAP) [RFC 2433]
 - Microsoft Point to Point Encryption Protocol (MPPE) [RFC 3078]
- Analyse von Bruce Schneier 1998; Fehler in
 - Password Hashing: schwacher Algorithmus erlaubt Eve, das Passwort zu ermitteln (Stichworte: LAN Manager Passwort und L0phtCrack)
 - Challenge/Response Protokoll erlaubt Maskerade-Angriff auf RAS Server (keine beidseitige Authentifizierung)
 - Verschlüsselung: Implementierungsfehler erlaubt Dekodierung
 - Verschlüsselung: Geratenes Passwort erlaubt Entschlüsselung
 - Kontrollkanal: Unautorisierte Nachrichten erlauben DoS (Crash des Servers)
 - Details: <http://www.schneier.com/paper-pptp.pdf>
- Microsoft verbesserte nach: PPTP v2 und MS-CHAPv2 [RFC 2759]

Vergleich MS-CHAP v1 und v2

■ Version 1:



K_L = LAN-Manager-kompatibler Hash(Passwort)

K_N = Windows NT-kompatibler Hash(Passwort)

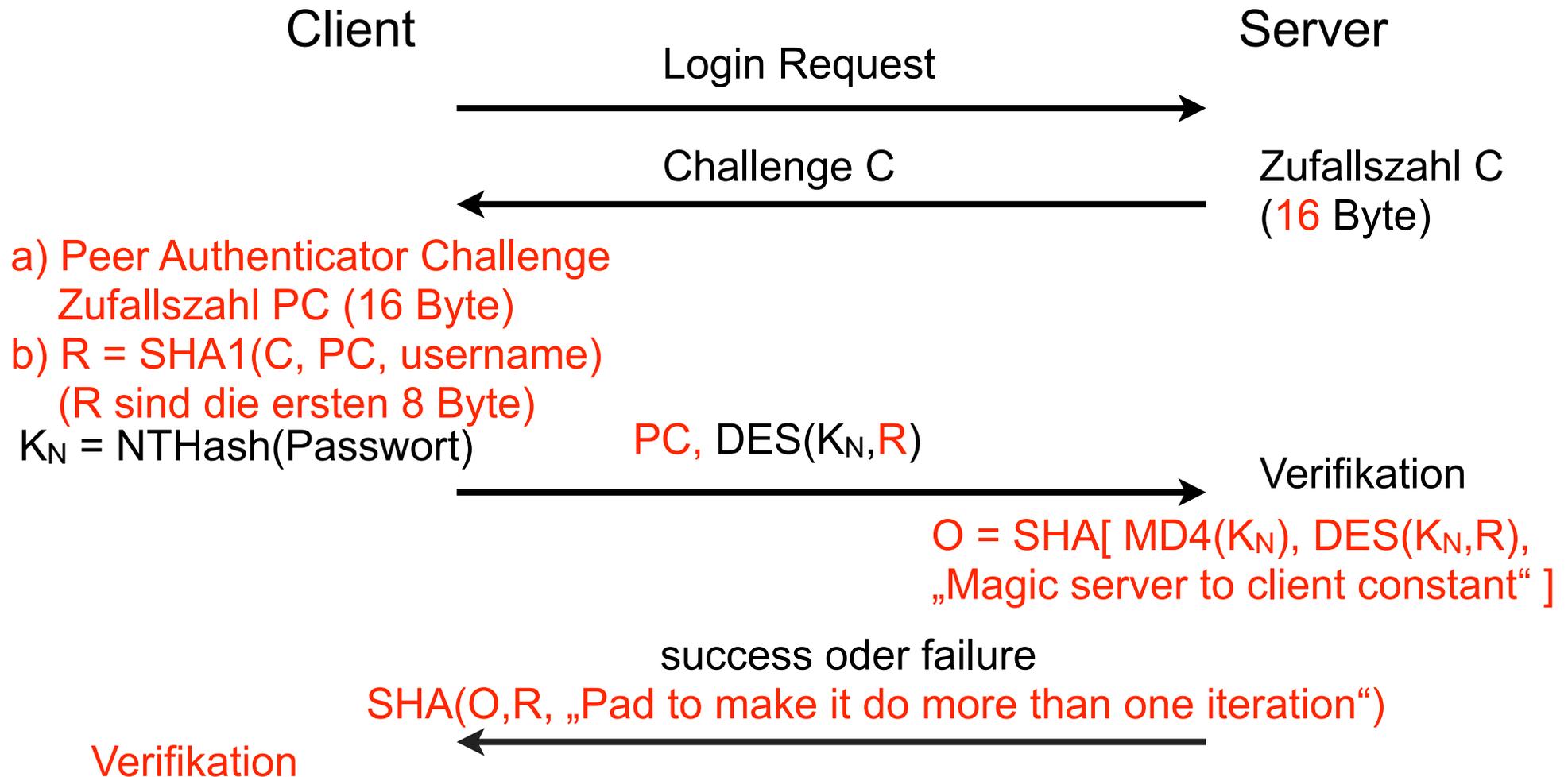
$DES(K_L, C), DES(K_N, C)$

Verifikation

success oder failure

Vergleich MS-CHAP v1 und v2

■ Änderungen in der Version 2



Sicherheit MS-CHAP v2

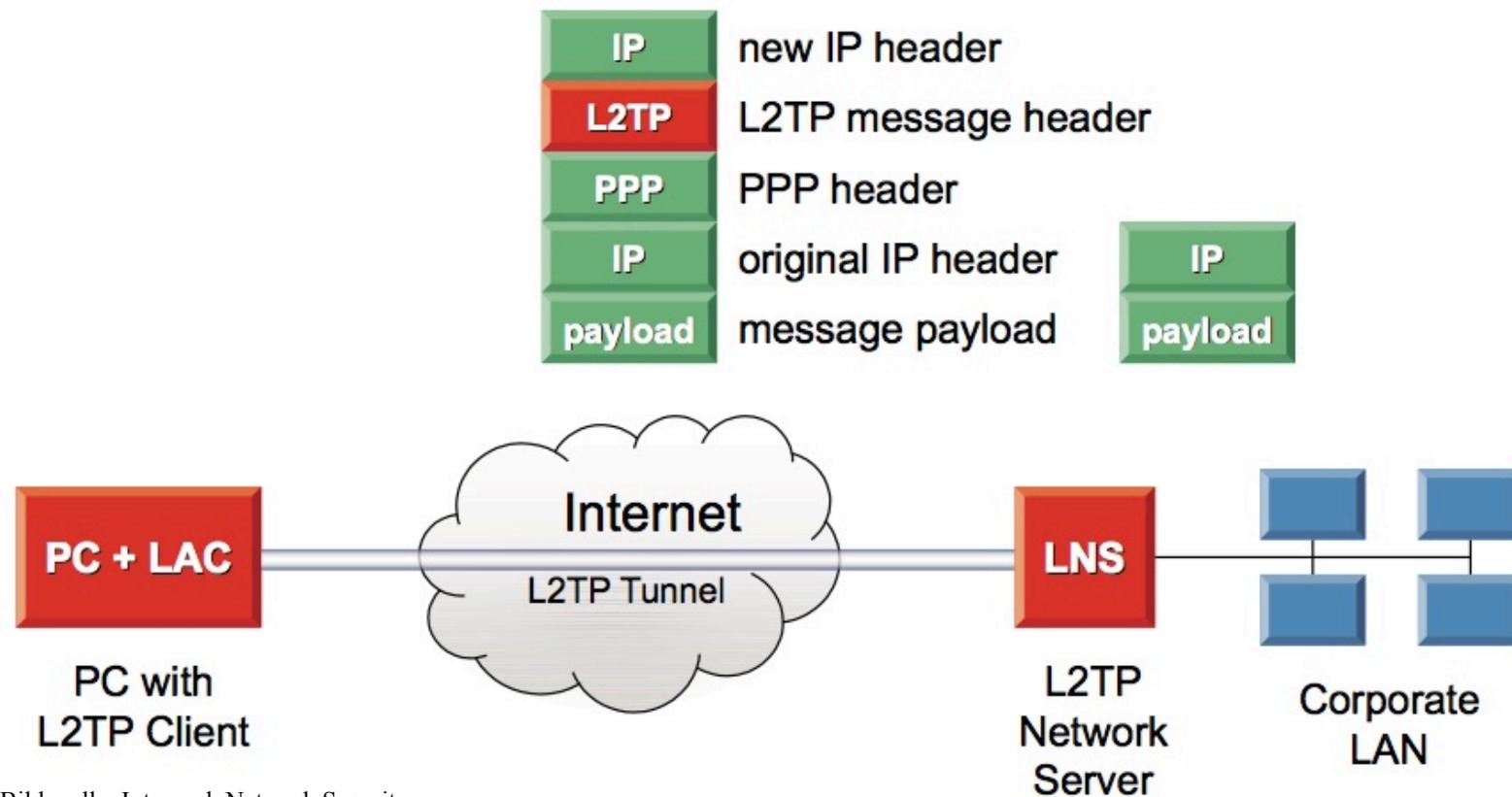
- Protokoll komplizierter als nötig
- Nutzen der „piggybacked“ Peer Authenticator Challenge PC fragwürdig
- Fazit:
 - Auch MS-CHAP v2 hat keinen integrierten Schutz vor Angriffen
 - Starke Abhängigkeit von der Wahl eines „guten“ Benutzerpassworts
 - Bessere Verfahren (z.B. Encrypted Key Exchange und Varianten) waren bereits verfügbar, wurden von Microsoft aber nicht genutzt
- Version Rollback Attack möglich:
Mallet „überzeugt“ Client und Server, MS-CHAP v1 zu verwenden

Layer 2 Tunneling Protocol (L2TP)

- L2TP [RFC 2661] entwickelt für Tunneling von PPP-Paketen
- Unterstützt verschiedene darunterliegende Protokolle:
UDP, ATM, FrameRelay
- Tunnel-ID erlaubt Multiplexing von Verbindungen/Tunneln
- Authentisierung mittels CHAP oder PAP
- Vertraulichkeit über IPSec möglich [RFC 3193]
(IPSec später in der Vorlesung)

L2TP Datenfluss

- L2TP Access Concentrator (LAC) verpackt Frames im lokalen Netz in eine L2TP-Nachricht
- L2TP-Nachricht wird über das Internet an den L2TP Network Server (LNS) geschickt und dort „ausgepackt“



Bildquelle: Interpeak Network Security

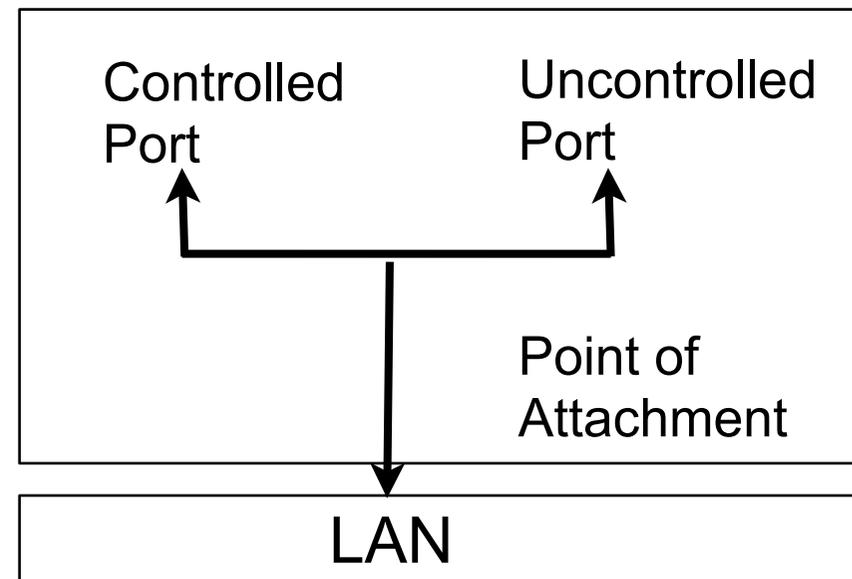
IEEE 802.1X

- 802er Standards für Local Area Networks (LAN), insbesondere für Schicht 1 und 2, z.B.
 - 802.1Q Virtual Bridged LANs (VLAN)
 - 802.3 CSMA/CD (Ethernet)
 - 802.5 Token Ring
 - 802.6 Metropolitan Area Network
 - 802.11 Wireless LAN
 - 802.15 Wireless PAN (Personal Area Network)
 - 802.15.1 Bluetooth
- 802.1X Port Based Network Access Control
 - Authentisierung und Autorisierung in IEEE 802 Netzen
 - Häufig genutzt in WLANs und (V)LANs
 - Port-basierte Network Access Control

802.1X Grundlagen

■ Rollen:

- ❑ **Supplicant:** 802.1X Gerät, das sich authentisieren möchte
- ❑ **Authenticator:** Gerät, an dem der Supplicant angebunden ist (z.B. Switch oder WLAN Access Point), erzwingt Authentisierung und beschränkt ggf. Konnektivität
- ❑ **Authentication Server:** führt die eigentliche Authentisierung durch (z.B. RADIUS-Server mit LDAP-Backend)
- ❑ **Port Access Entity (PAE):** „Port“, an dem Supplicant angeschlossen ist
 - **Uncontrolled Port:**
erlaubt Authentisierung des Gerätes
 - **Controlled Port:**
erlaubt authentisiertem Gerät Kommunikation zum LAN

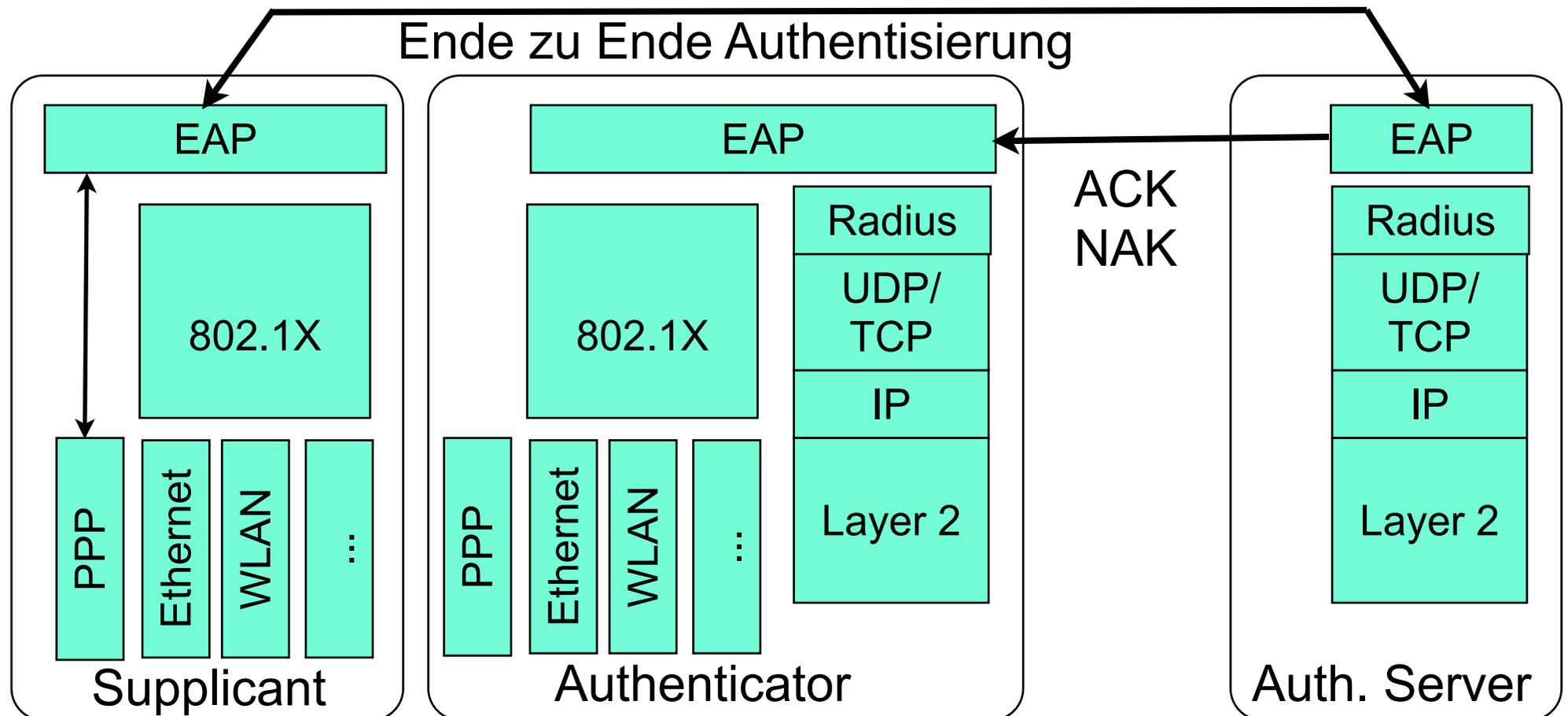


802.1X: Ablauf der Protokolle

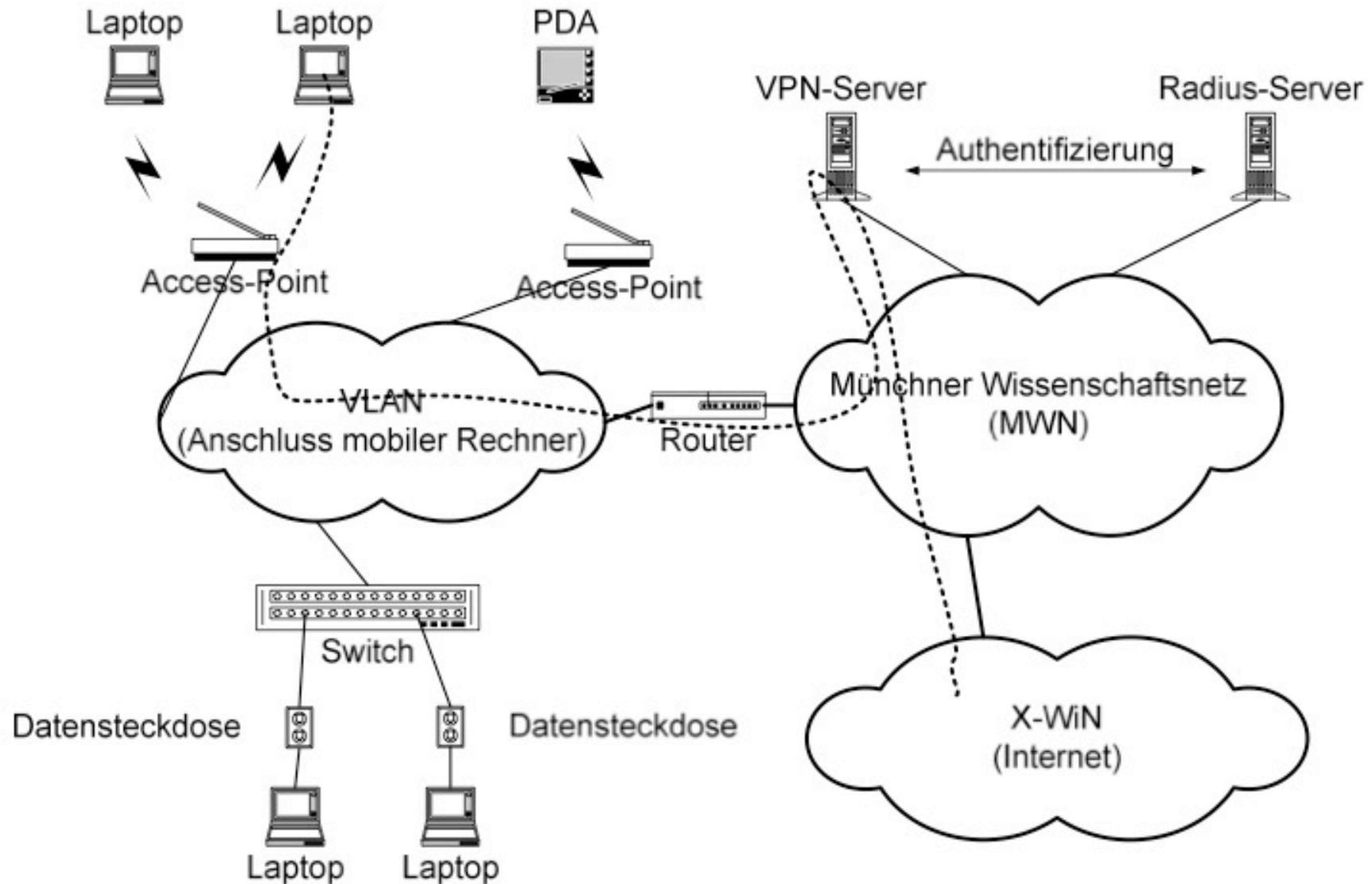
- Möglicher Ablauf:
 1. Supplicant fordert Controlled Port
 2. Authenticator fordert Authentisierung
 3. Nach erfolgreicher Authentisierung wird der Port freigeschaltet
- Supplicant oder Authenticator können Authentisierung initiieren
- 802.1X definiert keine eigenen Sicherheitsprotokolle, sondern nutzt bestehende:
 - Extensible Authentication Protocol (EAP) [RFC 3748] für Geräte-Authentisierung
 - EAP-TLS [RFC 5216] z.B. zur Aushandlung eines Session Key
 - RADIUS als AAA Protokoll (AAA = Authentisierung, Autorisierung und Accounting)

Extensible Authentication Protocol (EAP)

- Unterstützt verschiedene Auth.-Mechanismen
- Aushandlung erst während der Authentisierung mit Auth.-Server
- Authenticator ist nur Vermittler der Nachrichten



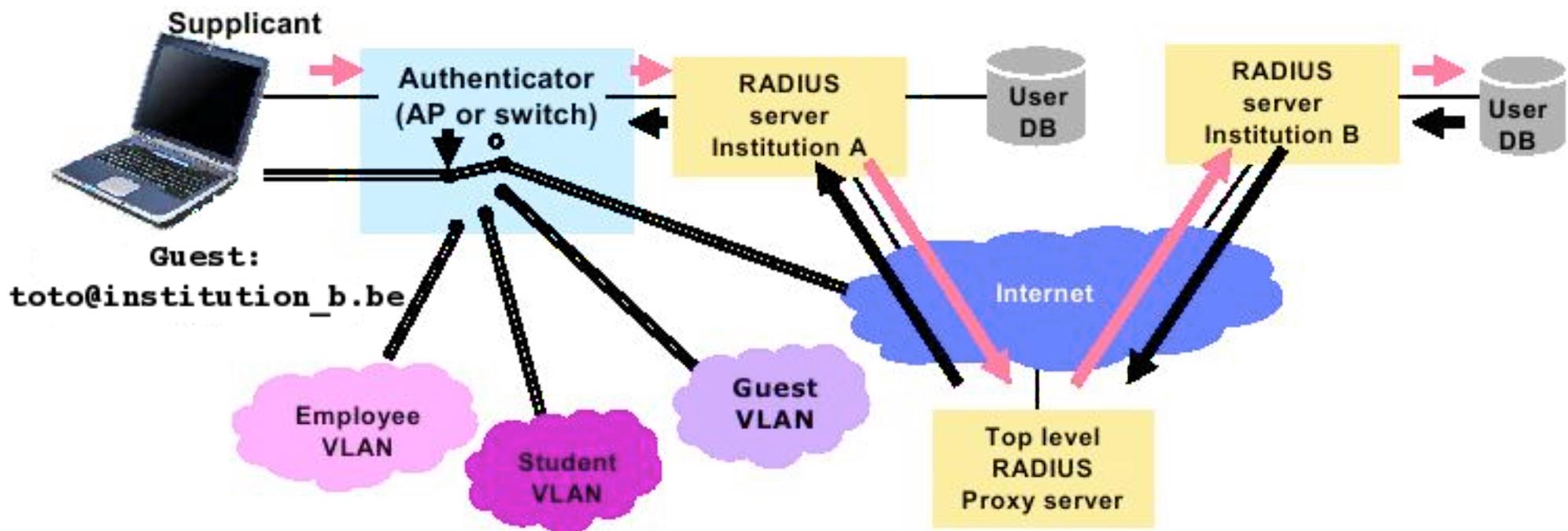
Beispiel: WLAN-Zugang im MWN



Beispiel: eduroam



- Weltweites Roaming in Hochschul-(WLAN-)Netzen
- 802.1X mit RADIUS-Authentifizierung an der jeweiligen Heimathochschule



Bildquelle: eduroam.be