



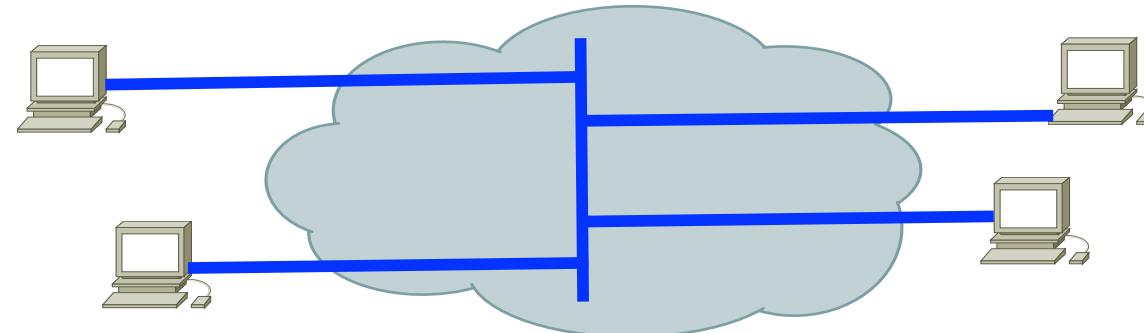
Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Kapitel 11: Netzsicherheit - Schicht 2: Data Link Layer

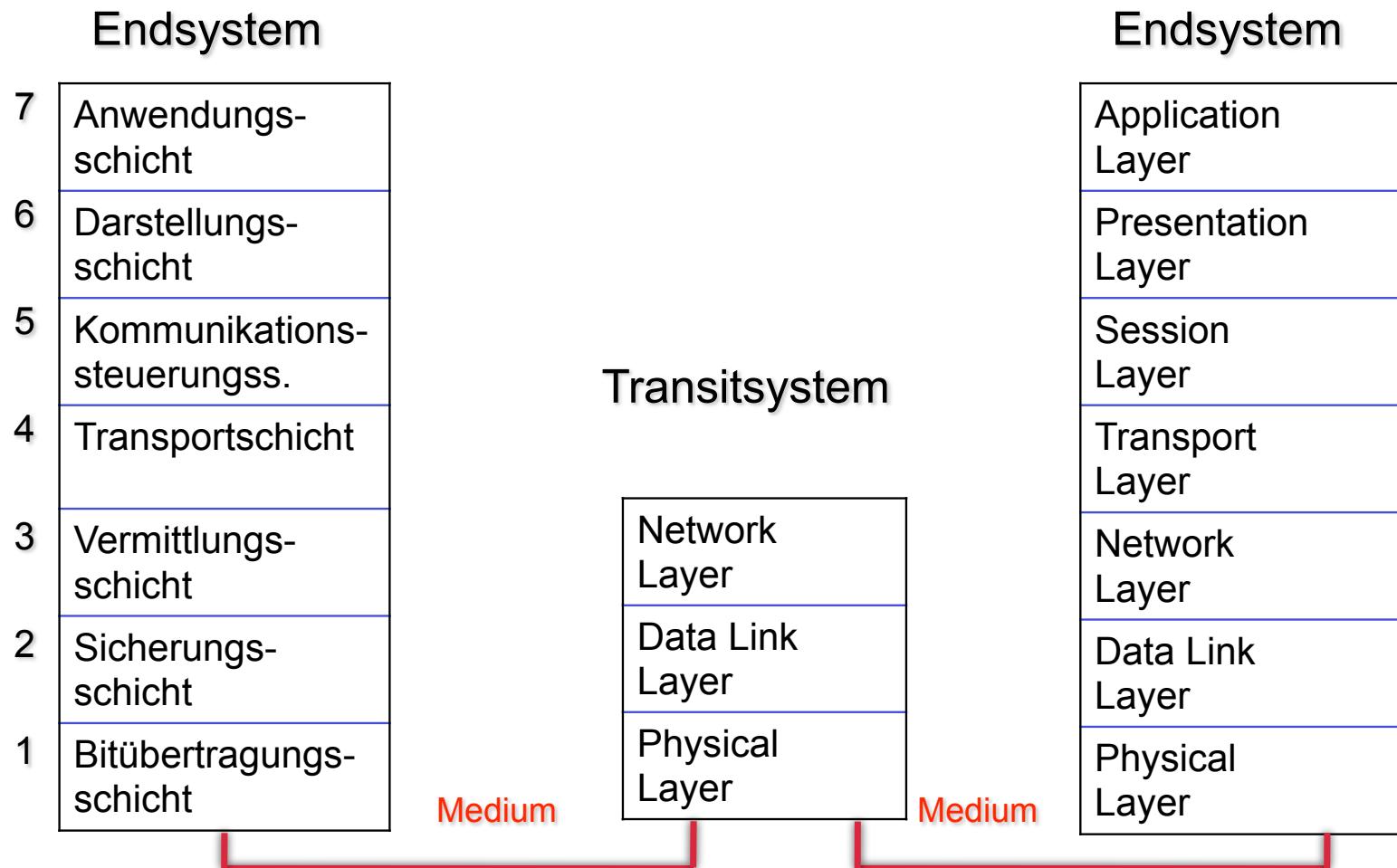
1. Virtualisierung von Netzen
 - Virtual Private Networks
 - VLAN
2. Point-to-Point Protocol (PPP)
 - Authentisierungsprotokolle:
 - PAP, CHAP, EAP
3. Point-to-Point Tunneling Protocol (PPTP)
4. IEEE 802.1x
5. WLAN und VPN im MWN

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

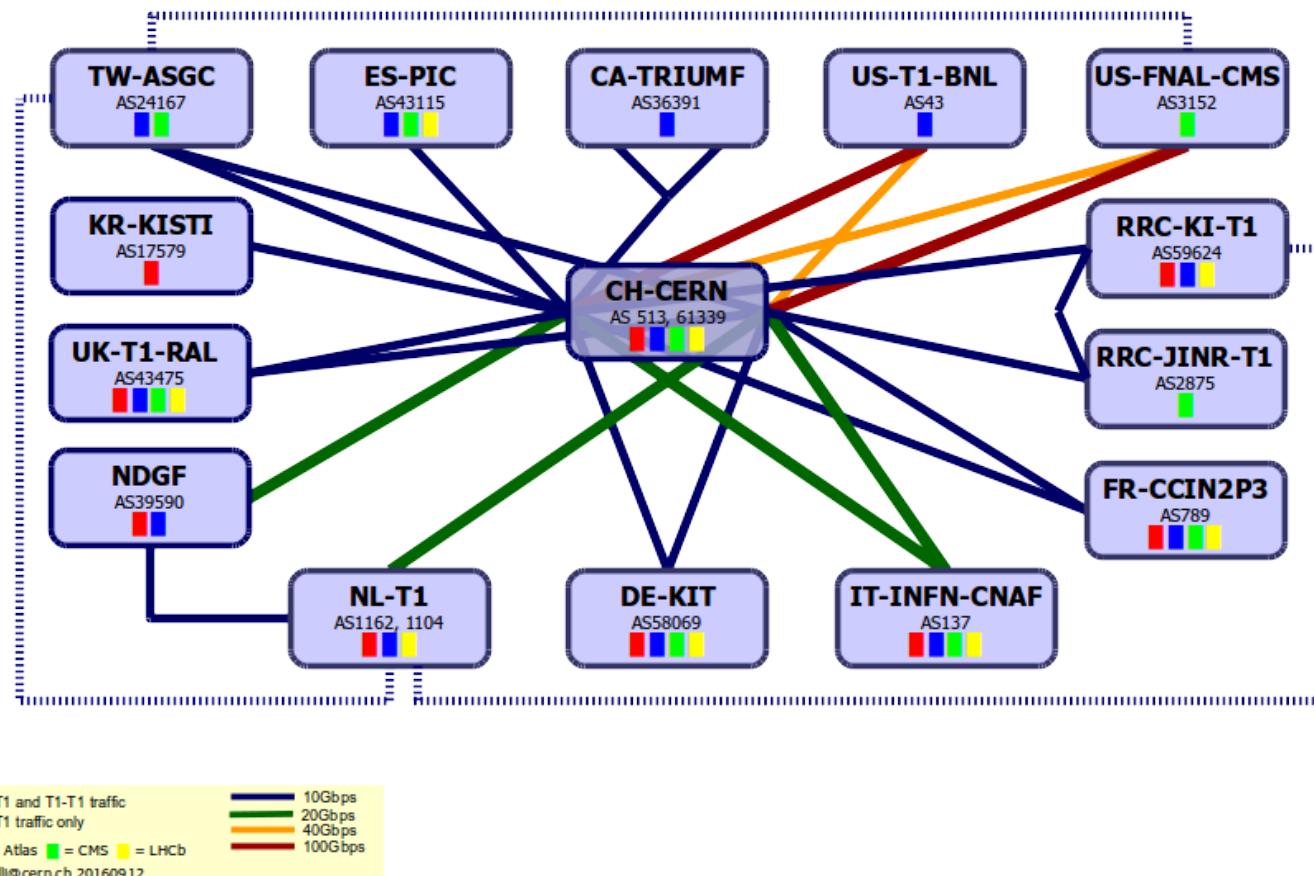


Virtual Network auf Schicht 1

- 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, Switching, etc. selbst kümmern
 - Über dieselben Glasfasern werden auch andere Kunden bedient

Beispiel für OPN

Large Hadron Collider



Virtual Network auf Schicht 2/3/4

■ Schicht 2:

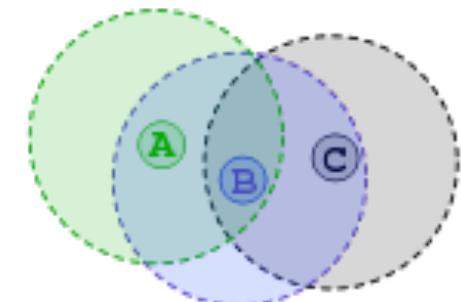
- Virtual LAN (VLAN)
 - Mehrere LAN Broadcast Domains über den selben physischen Link
 - Standard: VLAN Tagging (IEEE 802.1Q)
- Virtual Private LAN Services (Achtung: Abkürzung auch VPLS)
 - Verbindet physisch getrennte (V)LANs miteinander
- Point-to-Point Verbindungen
- Layer2 Tunneling Protocol
-

■ Schicht 3 und höher:

- IPSec
- SSL / TLS
- OpenVPN, eduVPN
- ...

Aufgaben der Schicht 2

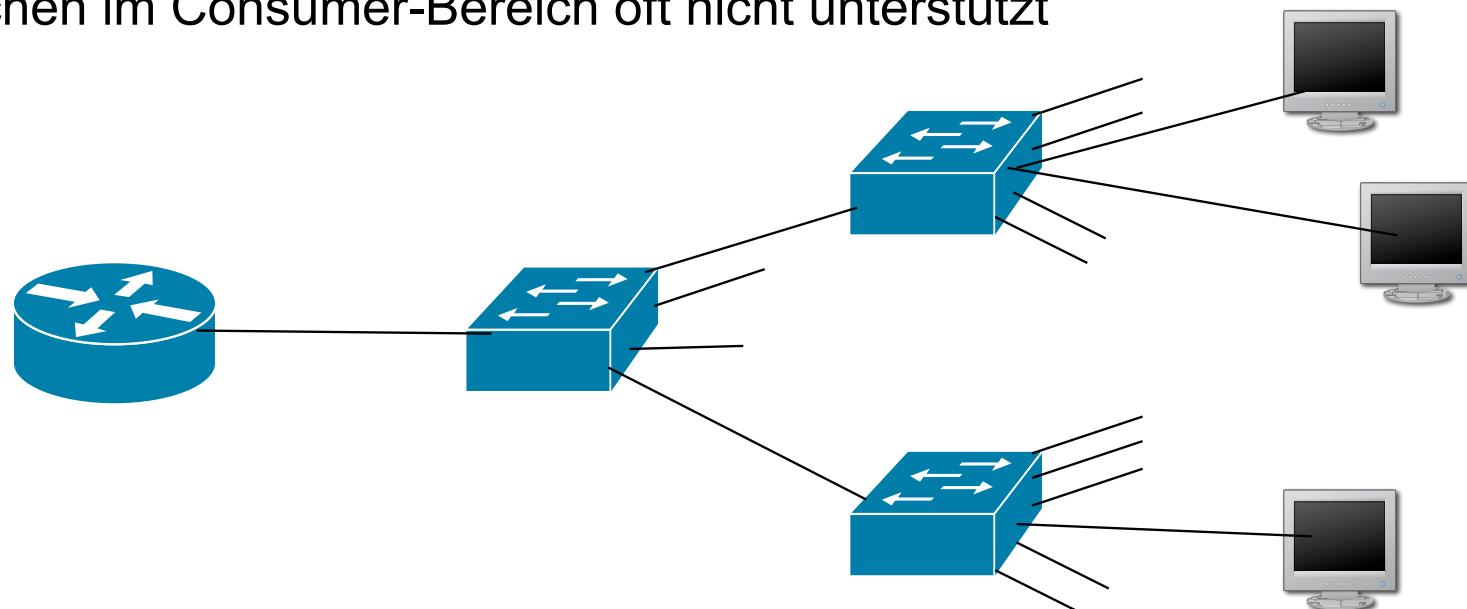
- Fehlerfreie Übertragung von Frames (Rahmen)
 - Aufteilung von Bitströmen in Frames
 - Fehlerkontrolle über Prüfsummen (z.B. Cyclic Redundancy Check, CRC)
- Flusskontrolle (Verhindert, dass der Empfänger mit Frames überflutet wird und diese verwerfen muss)
- Medienzugriffsverfahren für gemeinsam genutztes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



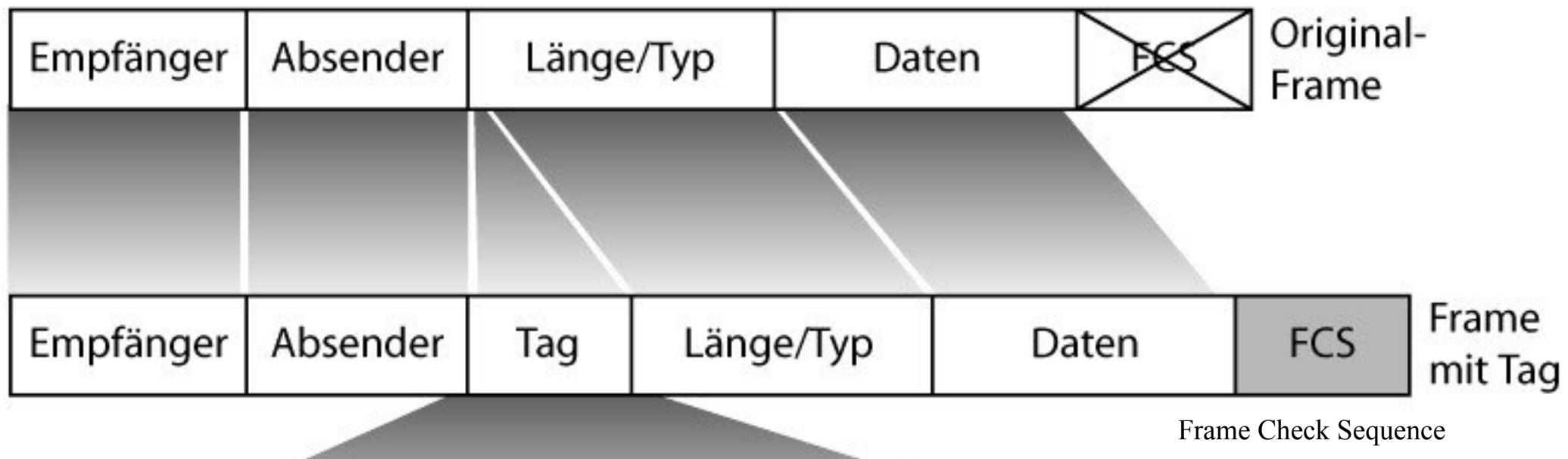
WLAN: Problem der „hidden stations“

Virtual LAN (VLAN)

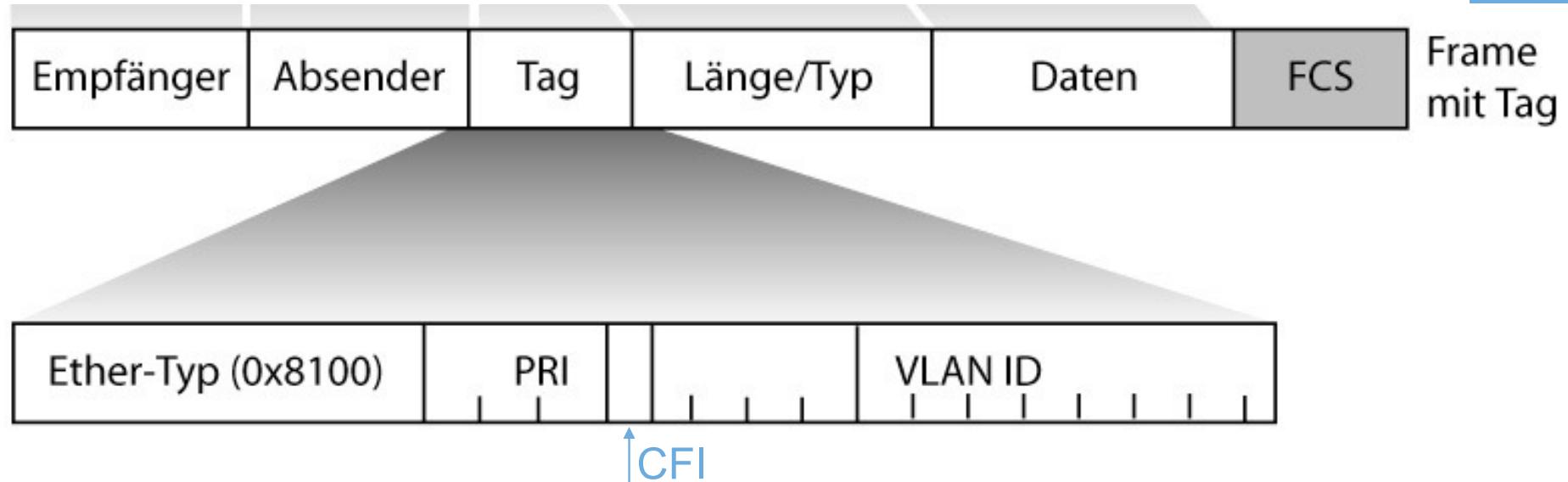
- LAN-Infrastruktur über mehrere Switches (Gebäude) hinweg
- Logisch verschiedene LANs auf einer Netzkomponente
- Wunsch nach Verkehrsseparierung
- Heute Standard in Unternehmens- und Hochschulnetzen
 - Von Switchen im Consumer-Bereich oft nicht unterstützt



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

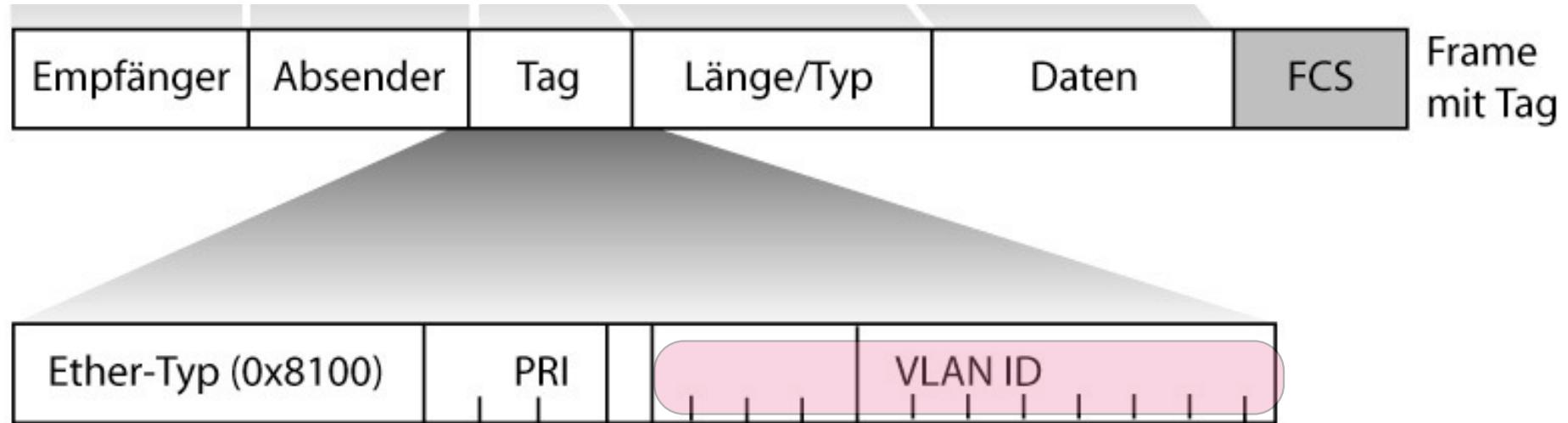


Tag-Format



- 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

Tag-Format (Forts.)



- Erweiterung des Ethernet-Frame um 32-bit Tag:
 - **VLAN-ID:** Identifizierung des VLANs („VLAN NR.“) (12 Bit)
 - ID 0 = „kein VLAN“, ID 0xFFFF ist reserviert
 - Somit 4094 verschiedene VLANs möglich

Fake Bitcoin ETF Nachricht



- SEC (Amerikanische Börsenaufsicht) entscheidet für Zulassung von Bitcoin ETFs
 - ETF (exchange-traded fund) - börsengehandelter Fonds
 - Entscheidung wird für den 10. Januar erwartet
- SEC veröffentlicht am 10. Januar auf X die Zulassung
 - 30 Minuten später wird Post gelöscht
 - 10 Minuten später: Konto kompromittiert
- SEC Ratschläge an Banken: MFA unerlässlich
- MFA beim X-Account der SEC **nicht** aktiviert
- Das X-Tweets börsenrelevant sein können ist SEC klar
 - Musk muss Tweets mit Tesla Bezug von Anwalt absegnen lassen
- Preis von Bitcoins stieg kurzfristig um 3 %
- SEC erteilt Freigabe für Bitcoin ETFs kurz danach

 U.S. Securities and Exchange Commi...  ...
@SECGov

Today the SEC grants approval for #Bitcoin  ETFs for listing on all registered national securities exchanges.

The approved Bitcoin ETFs will be subject to ongoing surveillance and compliance measures to ensure continued investor protection.


U.S. SECURITIES AND EXCHANGE COMMISSION
Today's approval enhances market transparency and provides investors with efficient access to digital asset investments within a regulated framework.
Chair, Gary Gensler

3:11PM · 1/9/24 From Earth · 4.6M Views

1. Virtualisierung von Netzen
 - Virtual Private Networks
 - VLAN
2. Point-to-Point Protocol (PPP)
 - Authentisierungsprotokolle:
 - PAP, CHAP, EAP
3. Point-to-Point Tunneling Protocol (PPTP)
4. IEEE 802.1x

Point to Point Protokoll (PPP)

- Punkt-zu-Punkt Protokoll; Entwickelt für Verbindungsauftbau über Wähleitungen
 - 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](#), [1663](#) 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)

- 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)

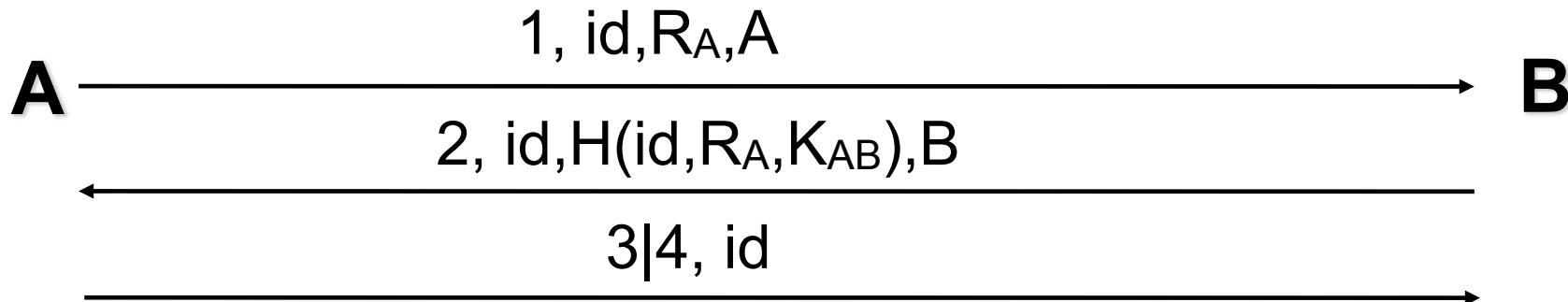
- Spezifiziert in [RFC1334](#)
- Authentisierende Entität kennt ID und Passwort aller Clients
- Client wird mit LCP zur Authentisierung via PAP aufgefordert
- Client schickt ID und Passwort im Klartext
- Server schickt im Erfolgsfall ACK

- 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, [RFC1994](#) und [RFC2484](#)
- 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

- 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](#), [RFC5247](#) und [RFC7057](#)
- 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 Authent. Prot.
 -

- 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 Autentisierungs-Token-Implementierungen
 - Request beinhaltet Nachricht, die dem Nutzer angezeigt wird
 - Nutzer gibt Token-Information ein
 - Server prüft und antwortet



1. Virtualisierung von Netzen
 - Virtual Private Networks
 - VLAN
2. Point-to-Point Protocol (PPP)
 - Authentisierungsprotokolle:
 - PAP, CHAP, EAP
3. Point-to-Point Tunneling Protocol (PPTP)
4. IEEE 802.1x
5. WLAN und VPN im MWN

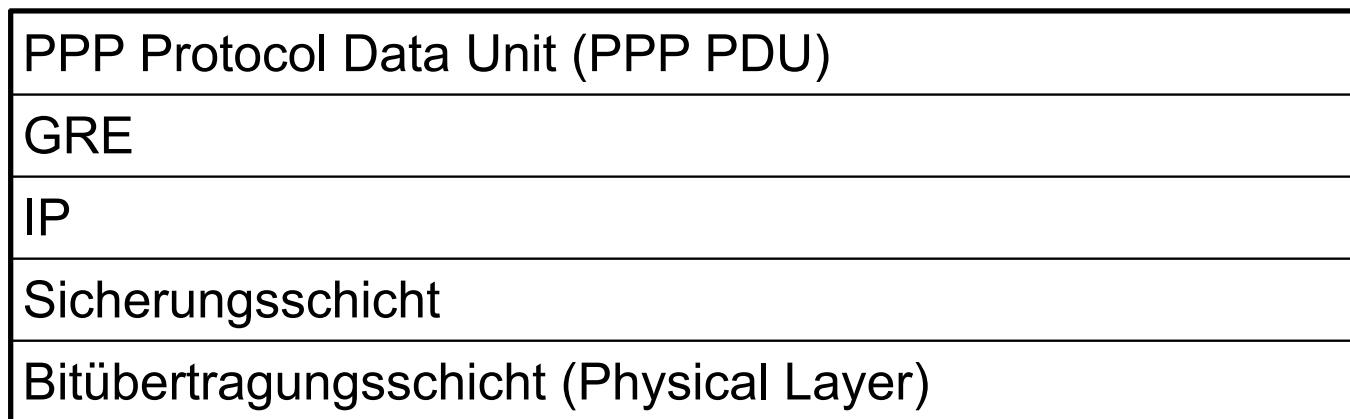
Führungen durch den Rechnerwürfel des LRZ



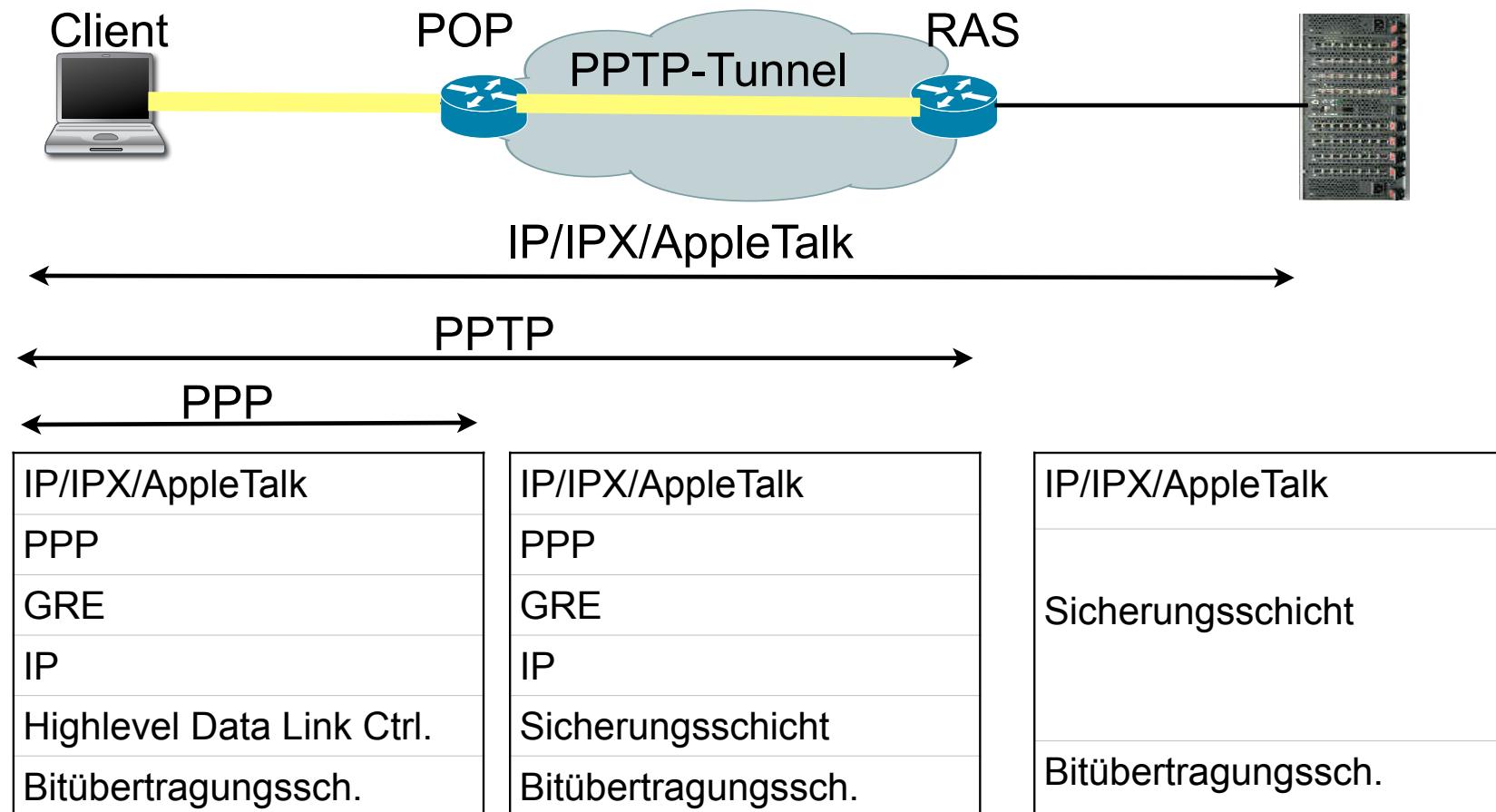
- Termin:
Mo. 05.02.24 (letzte VL) im LRZ in Garching (<https://www.lrz.de/wir/kontakt/weg/>)
 - Slot 1: 16:00 bis 17:00 Uhr
 - Slot 2: 17:15 bis 18:00 Uhr
- Anmeldung über Umfragetool <https://survey.lrz.de/index.php/232563?lang=de> spätestens Fr. 26.01.2024
- WICHTIG:
 - **Personalausweis mitbringen** und anmelden - ohne Perso und Anmeldung kommt man NICHT rein

Point to Point Tunneling Protocol (PPTP)

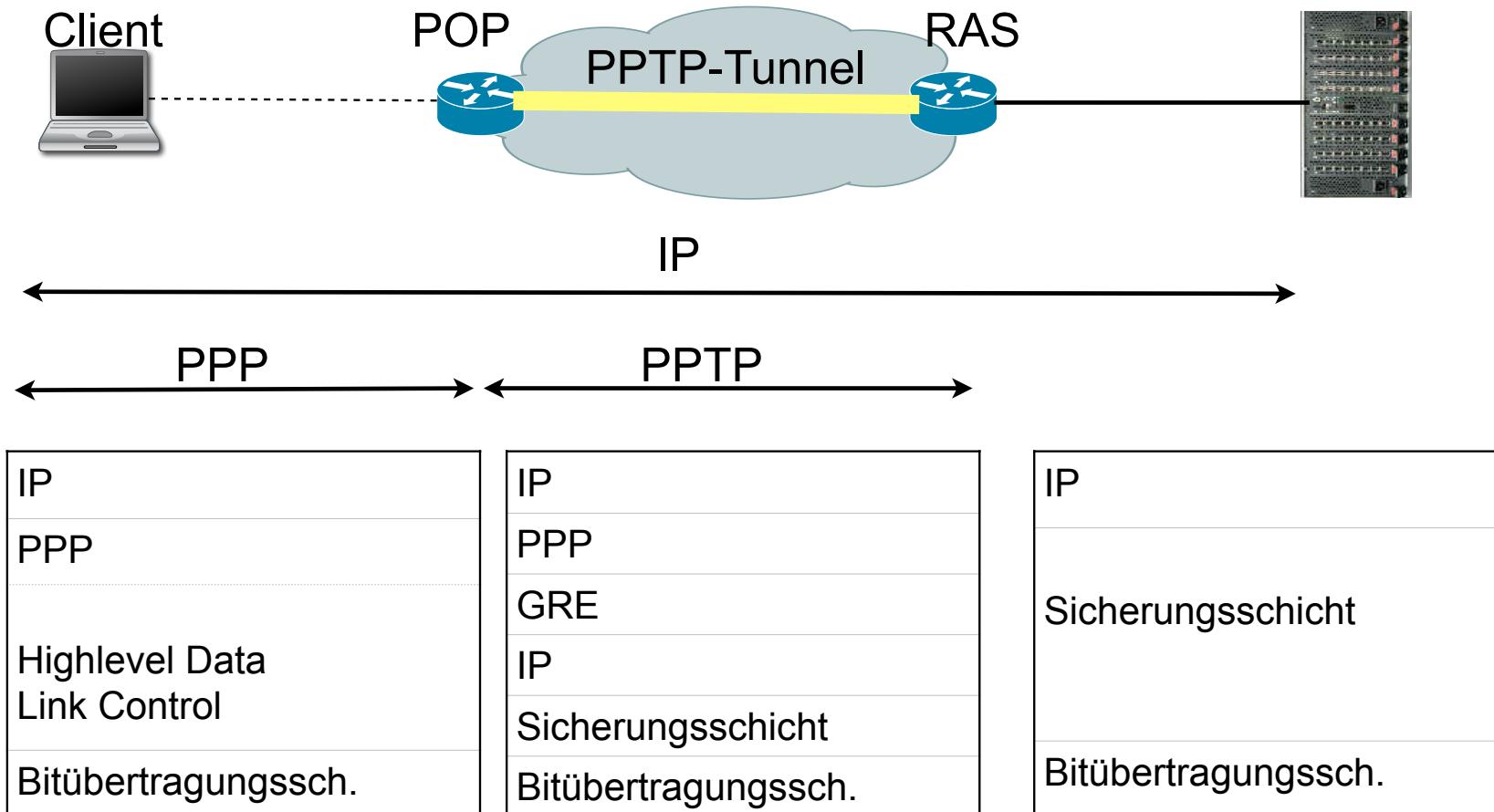
- PPP wurde für „direkt“ verbundene Systeme entwickelt
- Idee von PPTP (RFC2637):
 - Ausdehnung von PPP über Internet
 - PPTP realisiert Tunnel durch / über das Internet
 - Transport von PPP PDUs in IP-Paketen
 - Dazu werden PPP PDUs mit Generic Router Encapsulation Protocol (GRE) gekapselt
 - GRE ist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



- 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



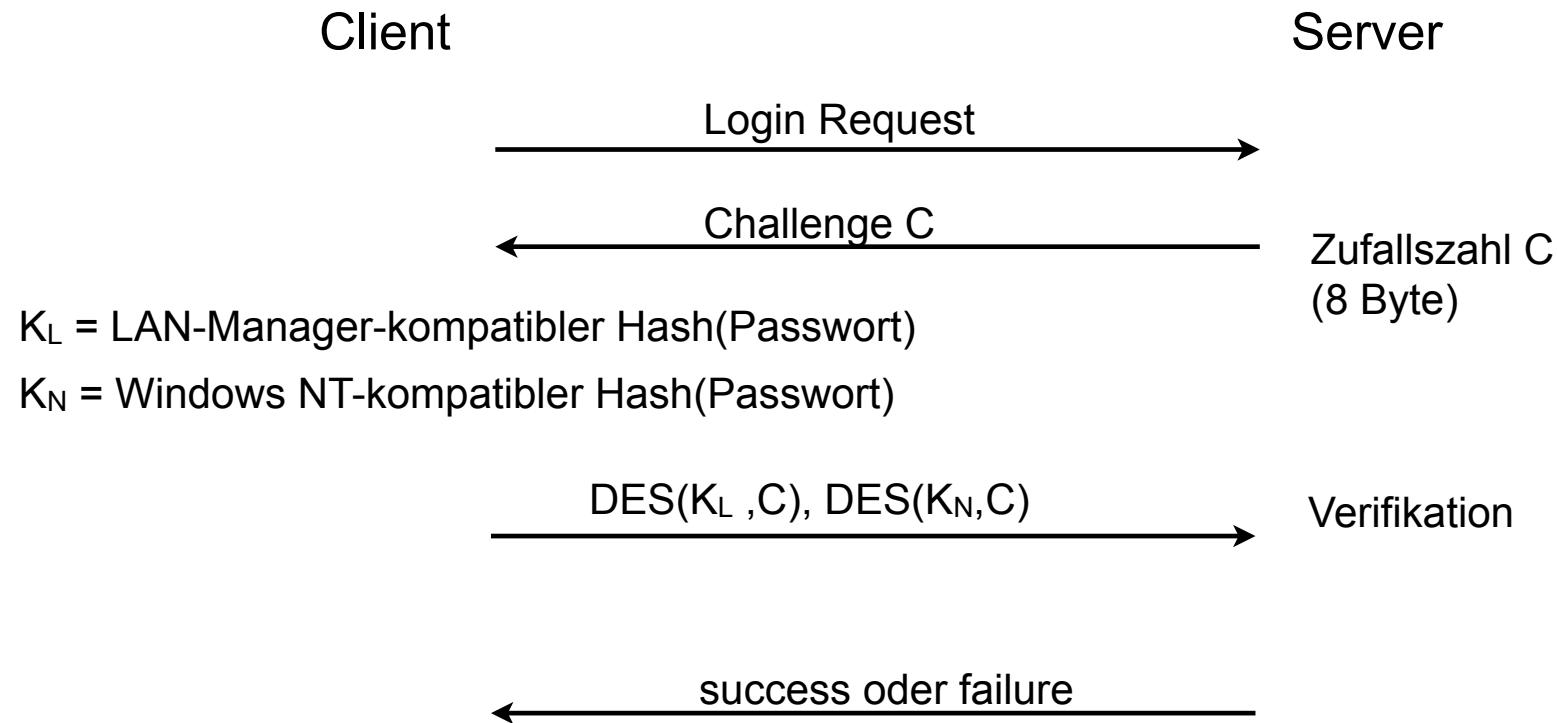
Compulsory Tunneling



- 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 besserte nach: PPTP v2 und MS-CHAPv2 [[RFC 2759](#)]

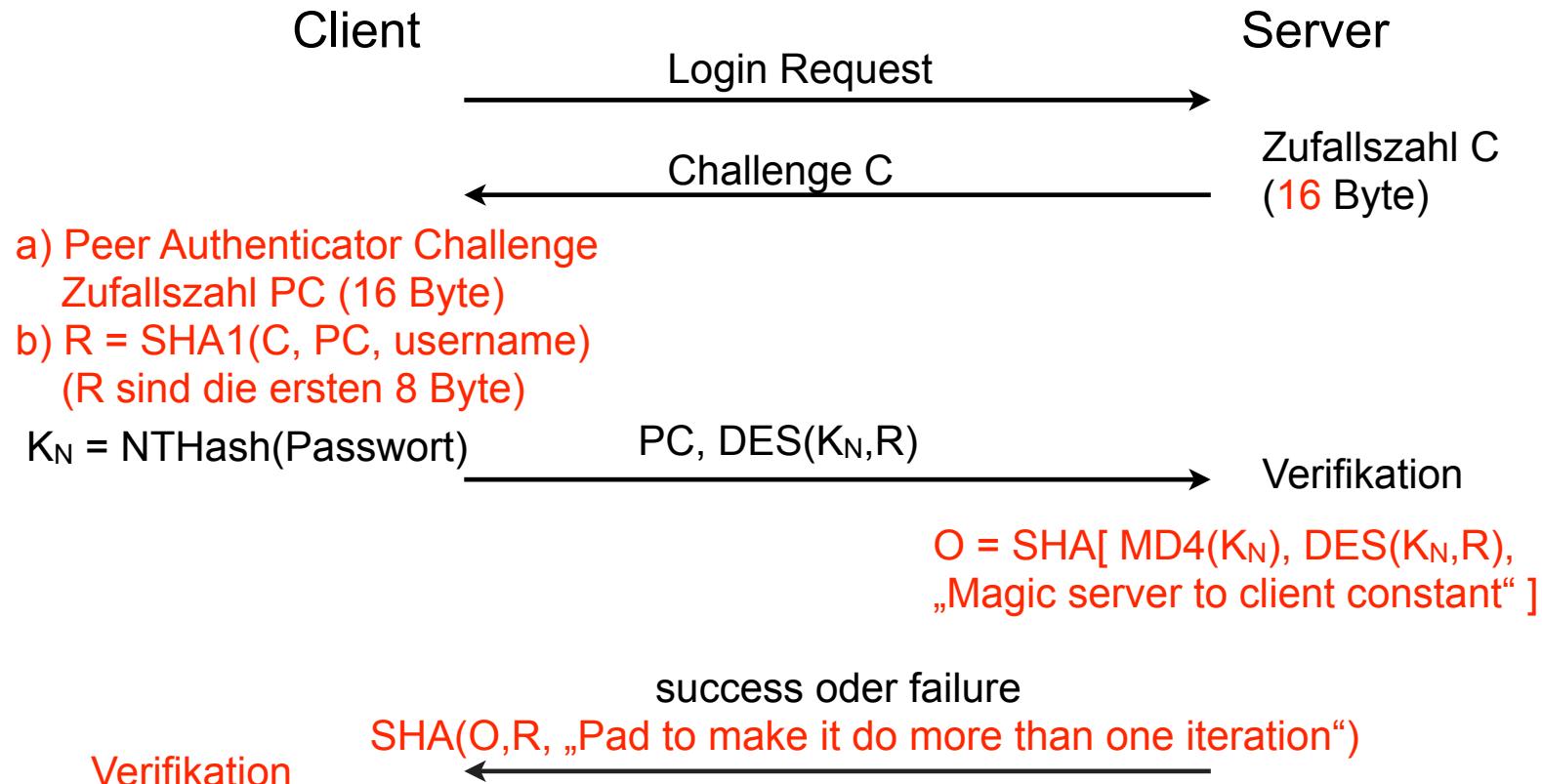
Vergleich MSCHAP v1 und v2

■ Version 1:



Vergleich MSCHAP v1 und v2

■ Änderungen in der Version 2



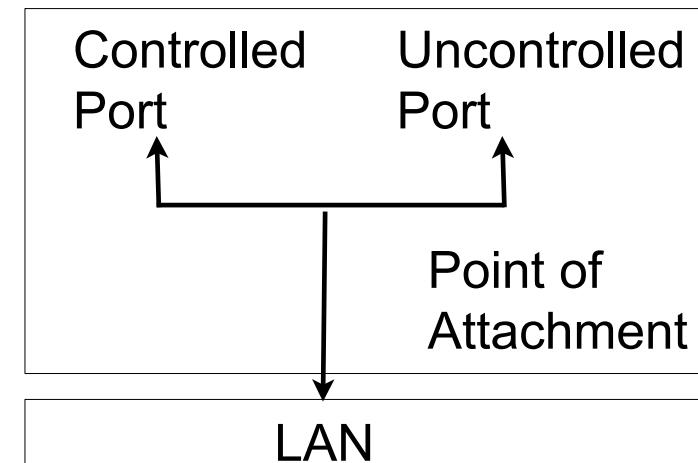
- Protokoll komplizierter als nötig
- Nutzen der „piggybacked“ Peer Authenticator Challenge PC fragwürdig
- Fazit:
 - Auch MS-CHAP v2 hat keinen integrierten Schutz vor Angriffen
 - Starke Abhängigkeit von der Wahl eines „guten“ Benutzerpassworts
 - Bessere Verfahren (z.B. Encrypted Key Exchange und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

1. Virtualisierung von Netzen
 - Virtual Private Networks
 - VLAN
2. Point-to-Point Protocol (PPP)
 - Authentisierungsprotokolle:
 - PAP, CHAP, EAP
3. Point-to-Point Tunneling Protocol (PPTP)
4. IEEE 802.1x
5. WLAN und VPN im MWN

- 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

■ Rollen:

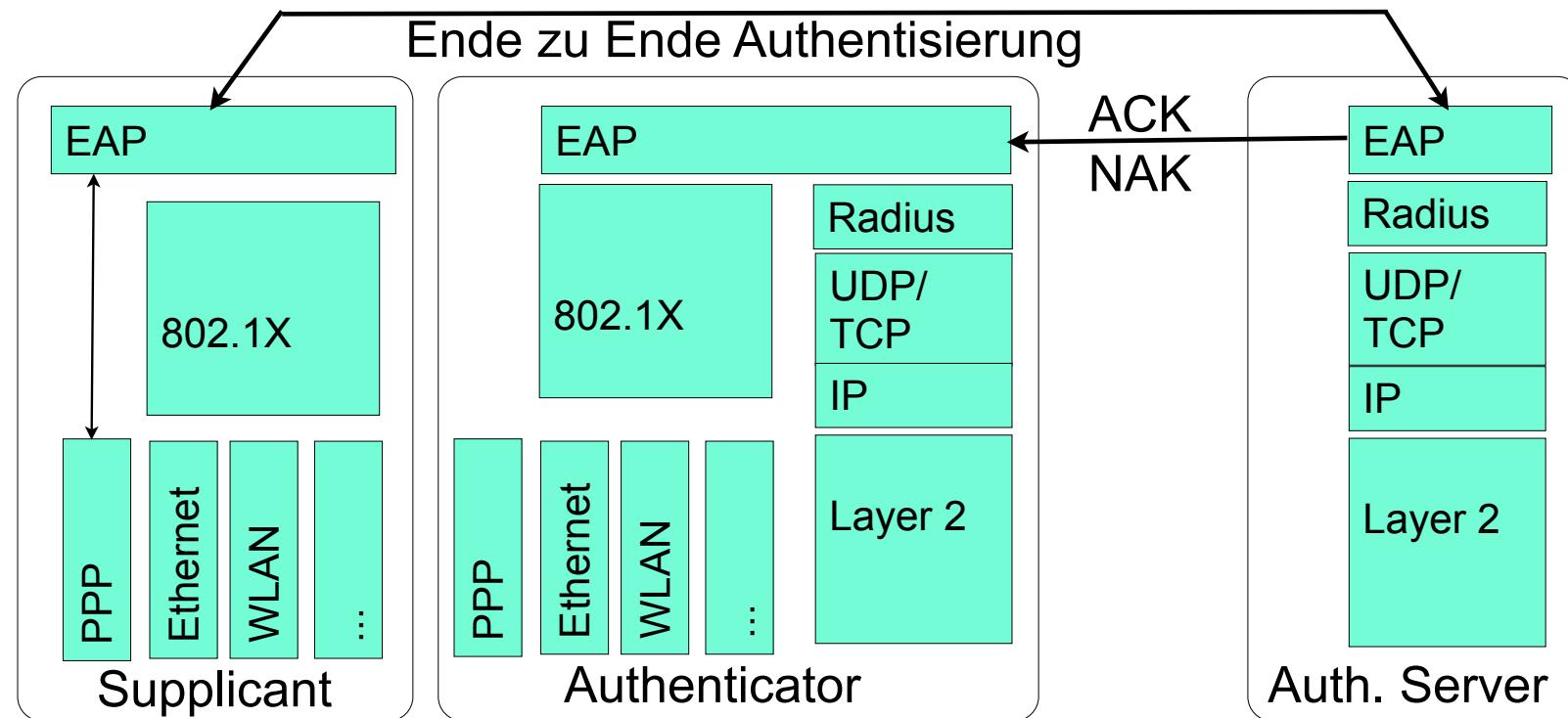
- Supplicant: 802.1X Gerät, das sich authentisieren möchte
- Authenticator: Gerät, an dem der Supplicant angebunden ist (z.B. Switch oder WLAN Access Point), erzwingt Authentisierung und beschränkt ggf. Konnektivität
- Authentication Server: führt die eigentliche Authentisierung durch (z.B. RADIUS-Server 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



- 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)

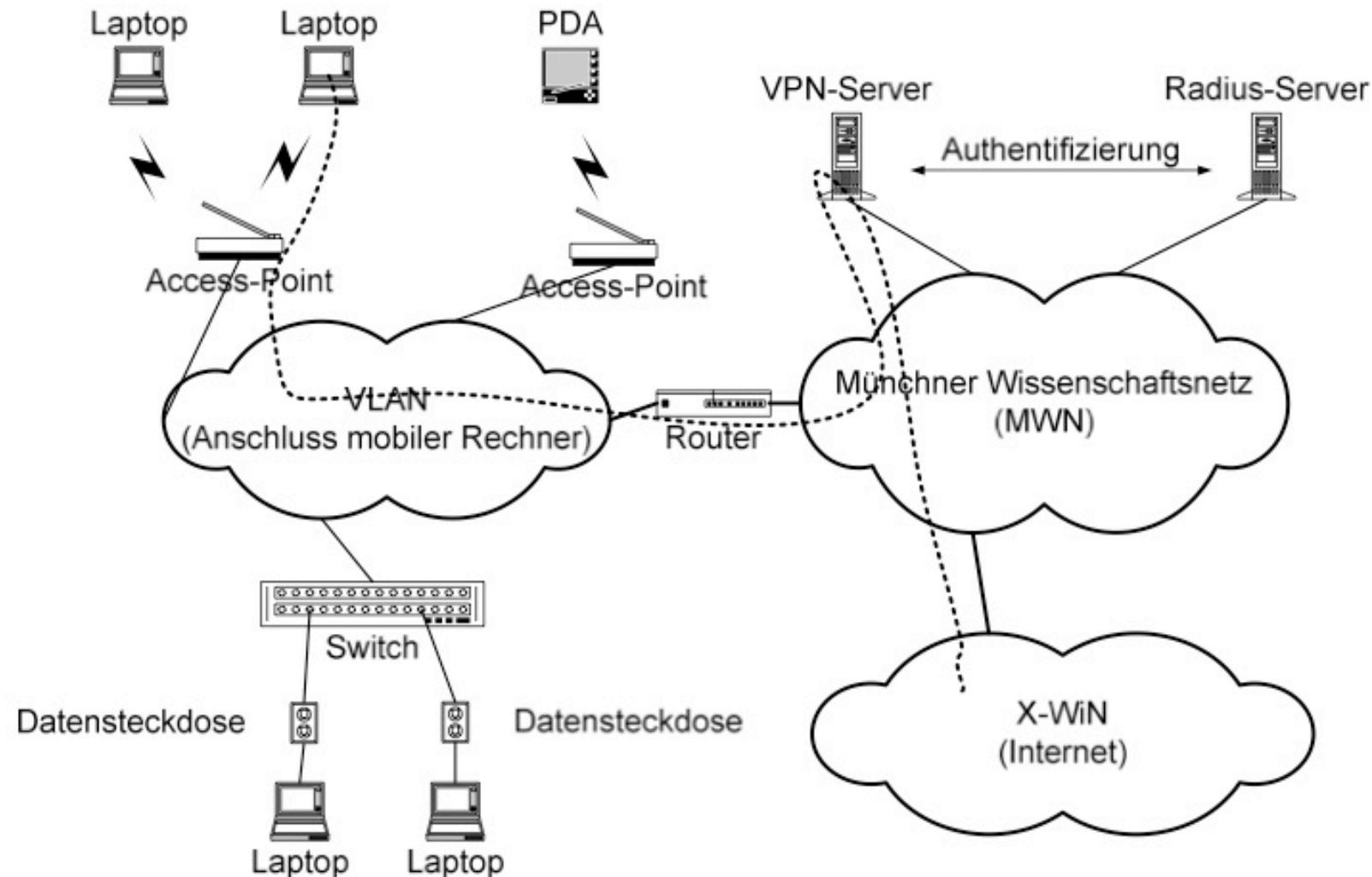
Extensible Authentication Protocol

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



Beispiel

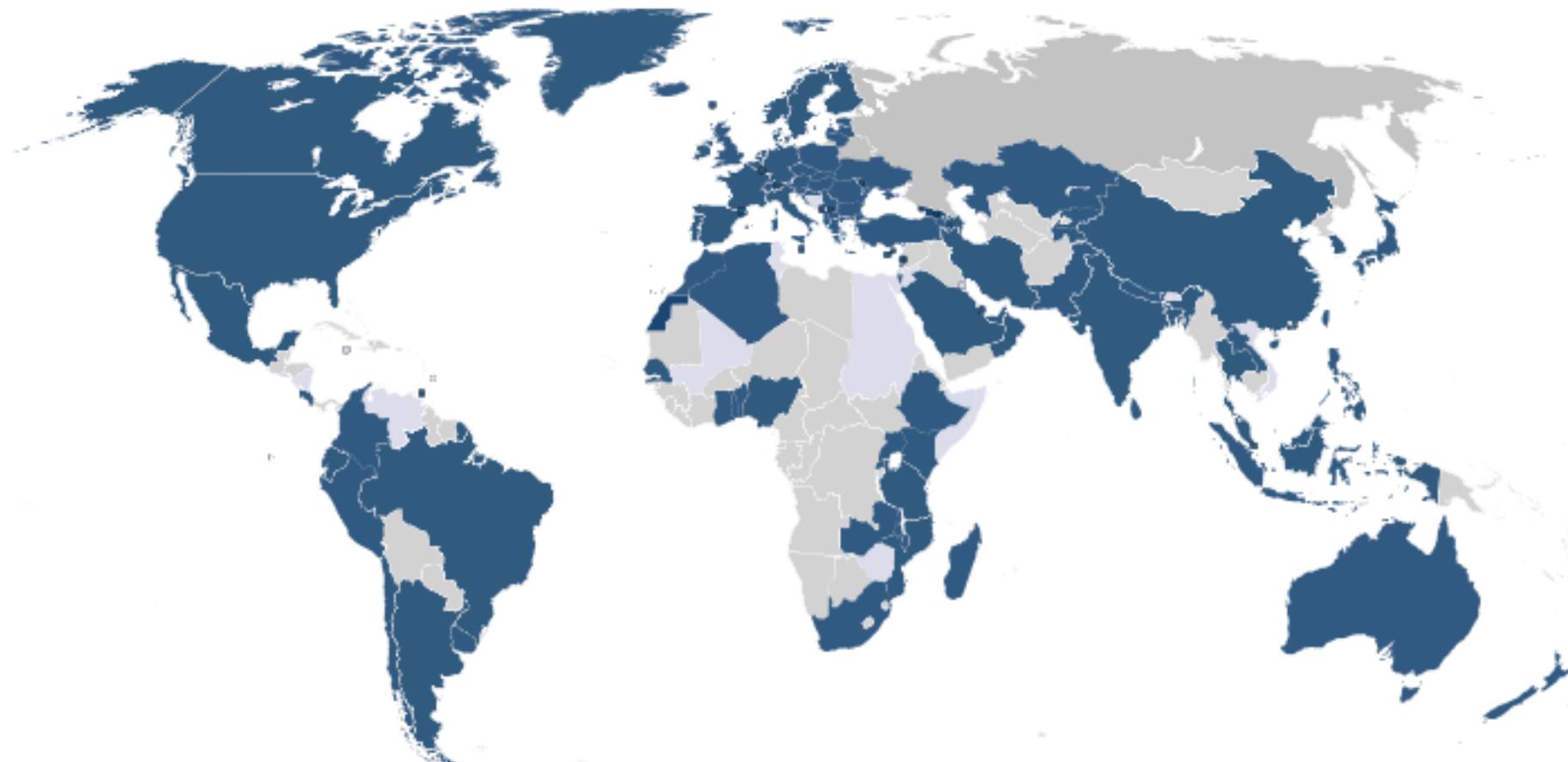
Datenzugang in öffentlichen Bereichen im MWN



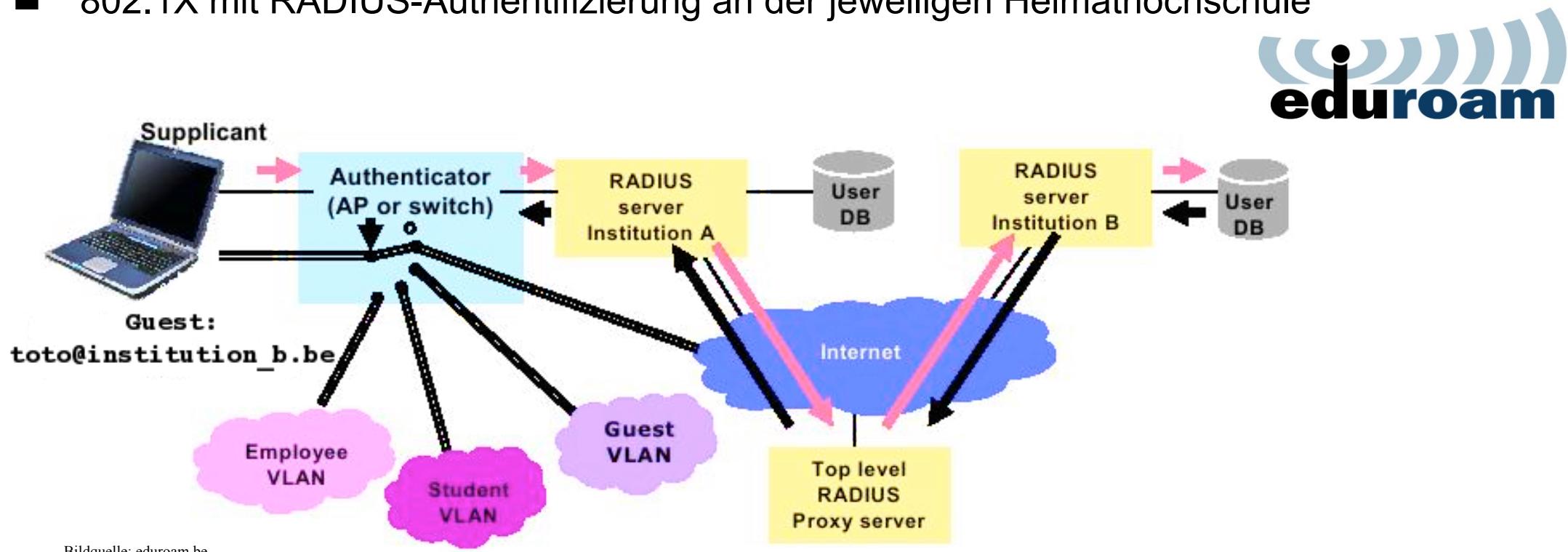
1. Virtualisierung von Netzen
 - Virtual Private Networks
 - VLAN
2. Point-to-Point Protocol (PPP)
 - Authentisierungsprotokolle:
 - PAP, CHAP, EAP
3. Point-to-Point Tunneling Protocol (PPTP)
4. IEEE 802.1x
5. WLAN und VPN im MWN

- Hintergrund
 - Eduroam wurde im Rahmen von GÉANT Forschungsprojekten
 - GÉANT ist Verbund von europäischen NRENs (National Research & Education Networks) und betreibt ein europäisches Backbone zur Anbindung der NRENs
 - Beteiligt sich an Forschungsprojekten: aktuell GN4 - Planungen für GN5 laufen
 - LRZ arbeitet im Auftrag des DFN an GN4 mit
- Eduroam ermöglicht **Mitarbeitern und Studenten** von partizipierenden [...] Organisationen den **Internetzugang** an den Standorten aller teilnehmenden Organisationen unter Verwendung ihres eigenen Benutzernahmen und Passwortes [aus [Wikipedia](#)]

- Where can I eduroam?

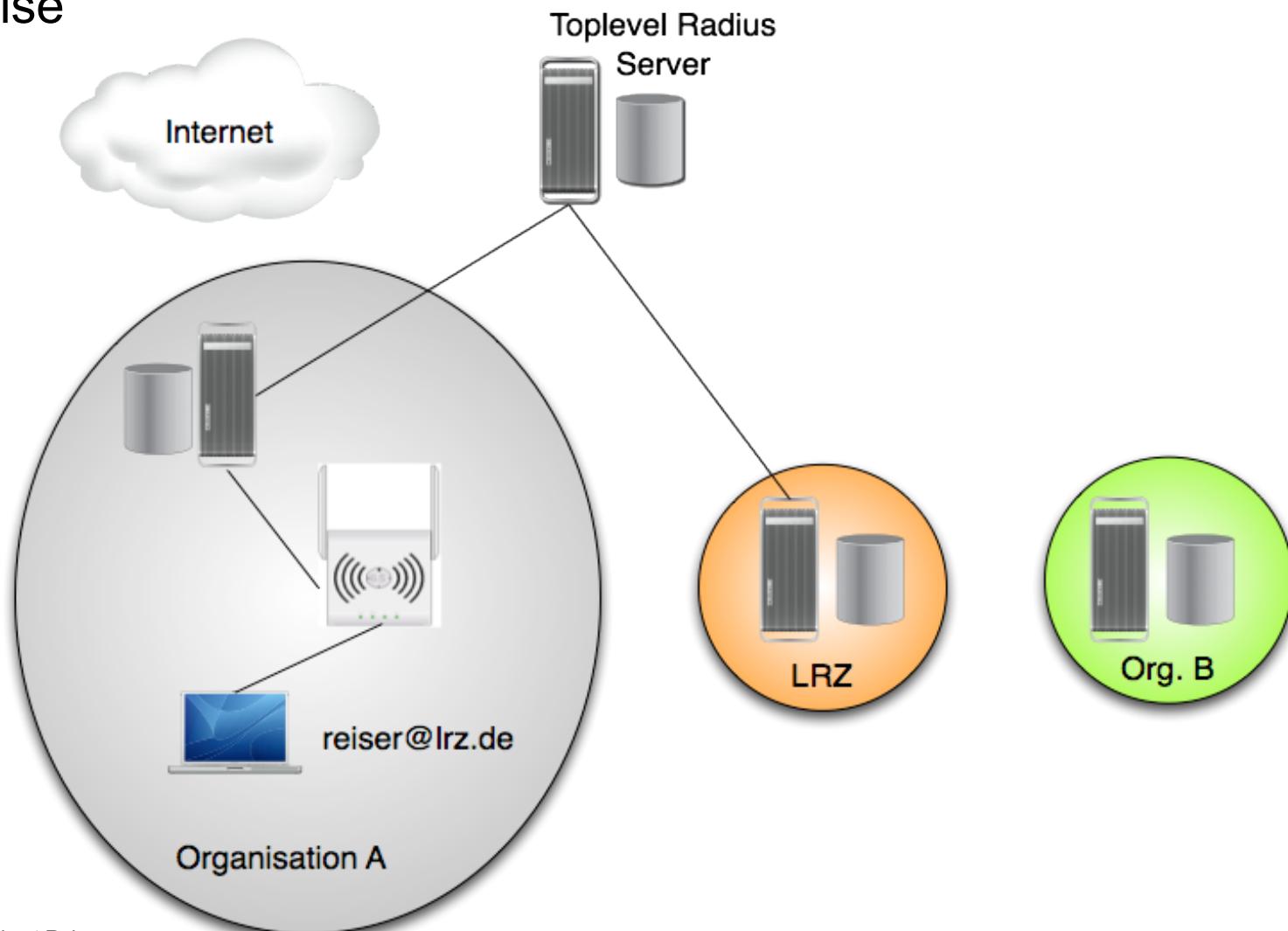


- Weltweites Roaming in Hochschul-(WLAN-)Netzen
- 802.1X mit RADIUS-Authentifizierung an der jeweiligen Heimathochschule

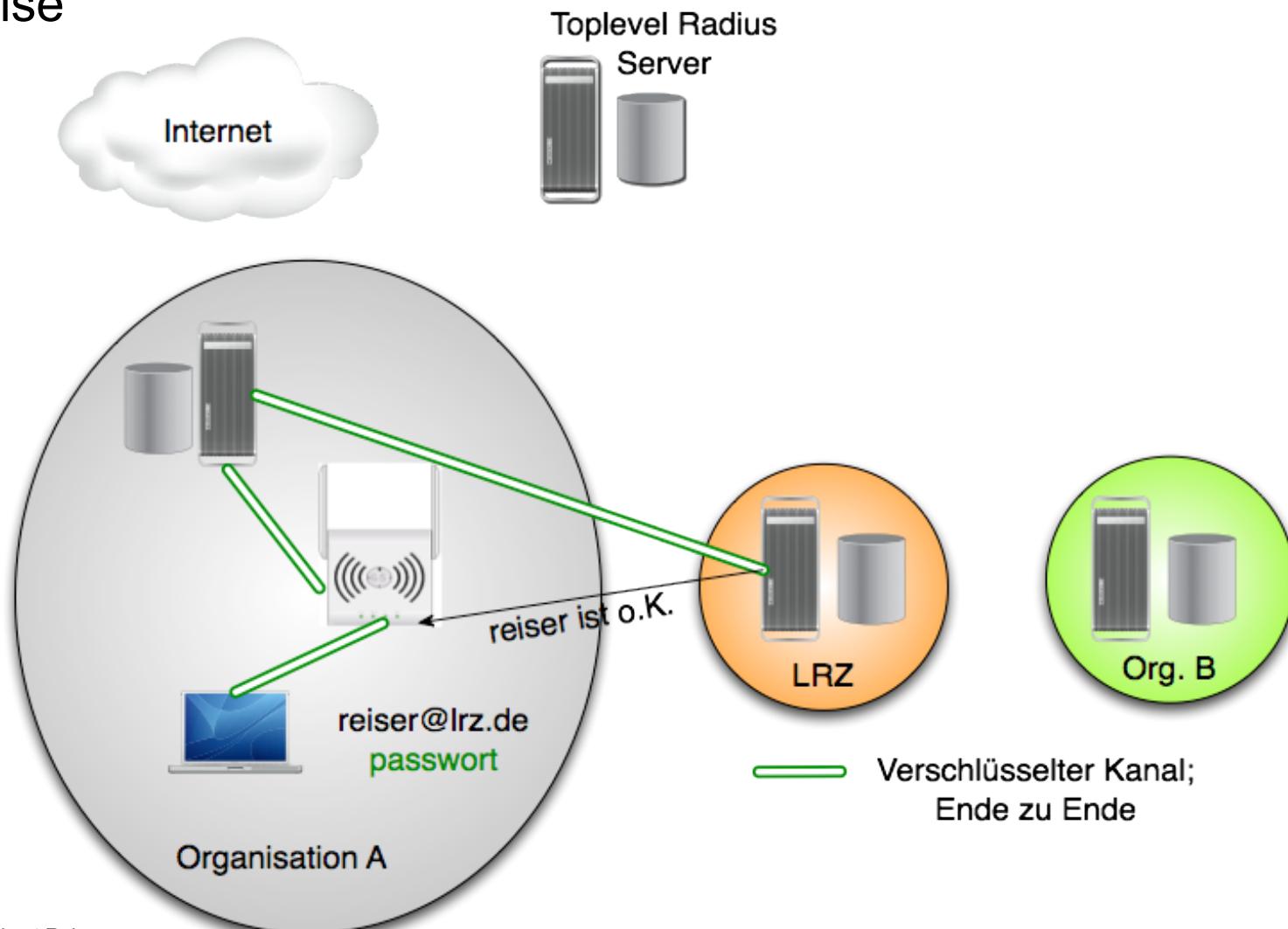


Bildquelle: eduroam.be

Funktionsweise

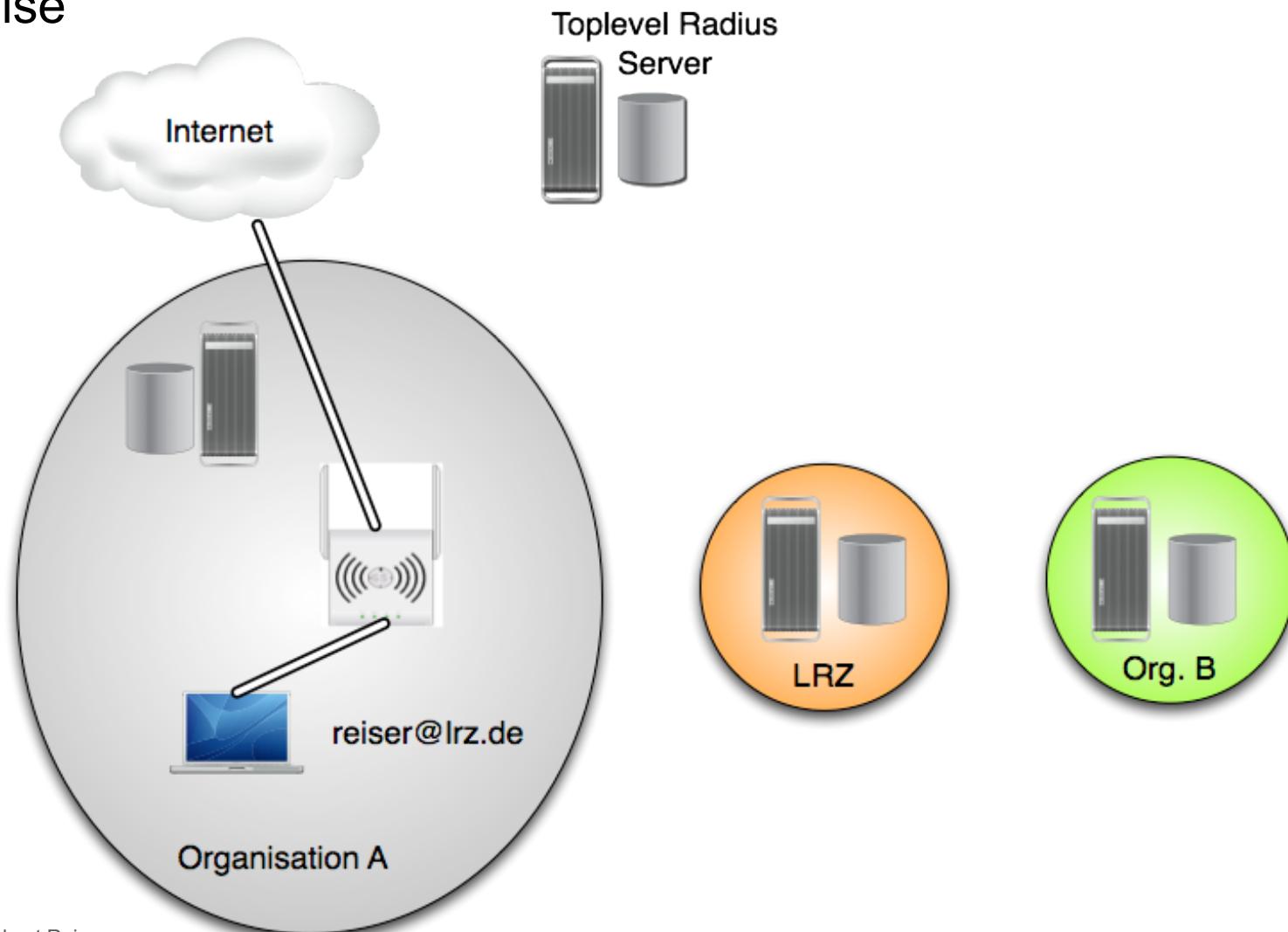


Funktionsweise



Praxisbeispiel Eduroam

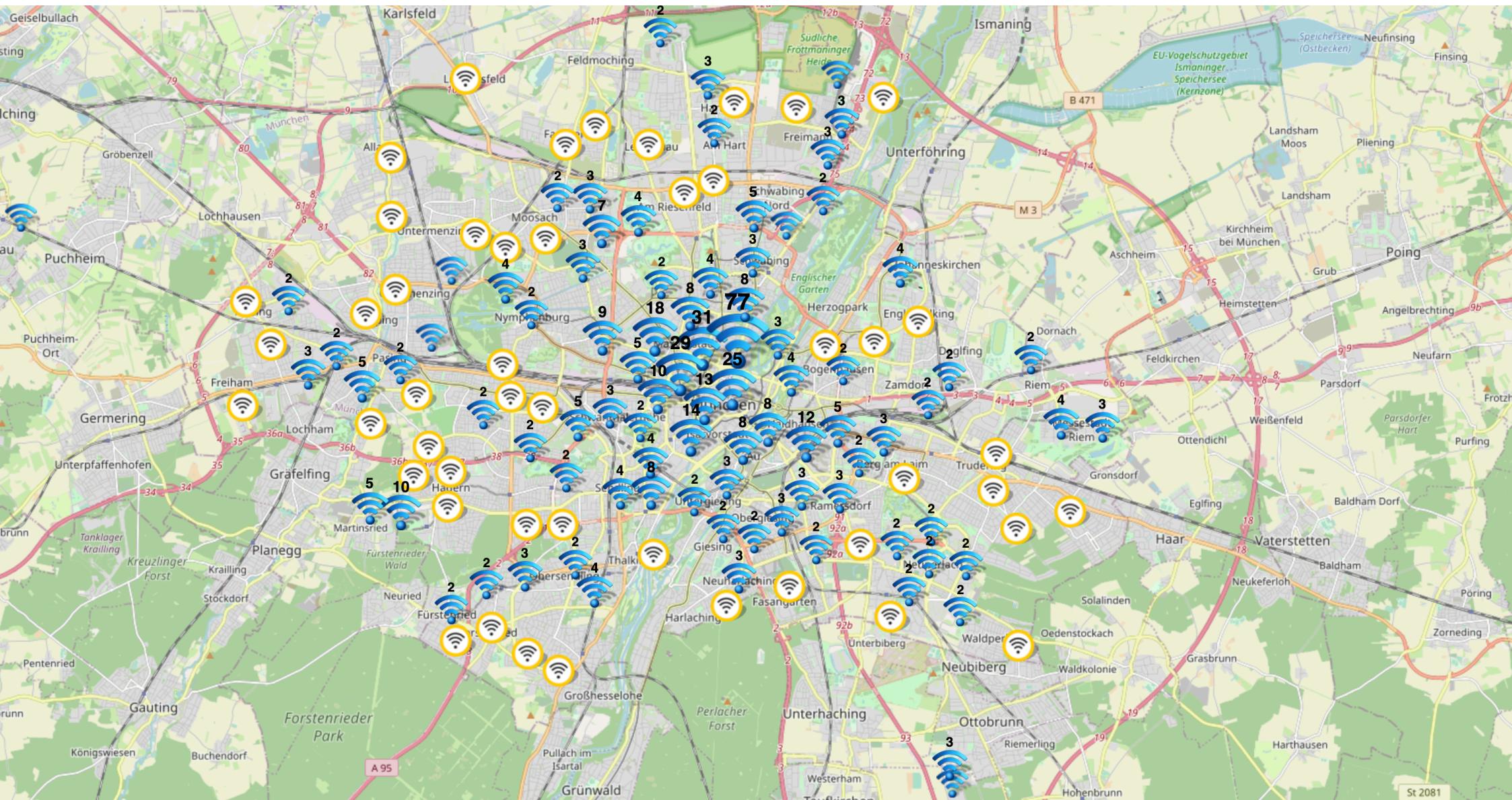
Funktionsweise



- Fake Access Points (eduroam-spoofing)
 - AP strahlt eduroam aus und simulieren Radius-Server
 - Gefahr Nutzerdaten und Passwörter abzugreifen
- Einfach zu erkennen durch Prüfung der Zertifikate, aber
 - Ältere Android Version prüfen Zertifikate nicht (richtig)
 - Konfigurationsfehler können dazu führen das Zertifikate nicht geprüft werden
- Zur Konfiguration **immer** das Configuration Assistant Tool (CAT) verwenden
 - <https://cat.eduroam.de>
 - Gibt es auch als Smartphone App

City-WLAN in München

- Stadtwerke München (SWM) betreiben zusammen mit M-net „M-WLAN“
- Eduroam wurde im April 2014 freigeschaltet
- Alle APs erhalten eduroam



eduroam off campus (EoC): Was braucht der Provider?

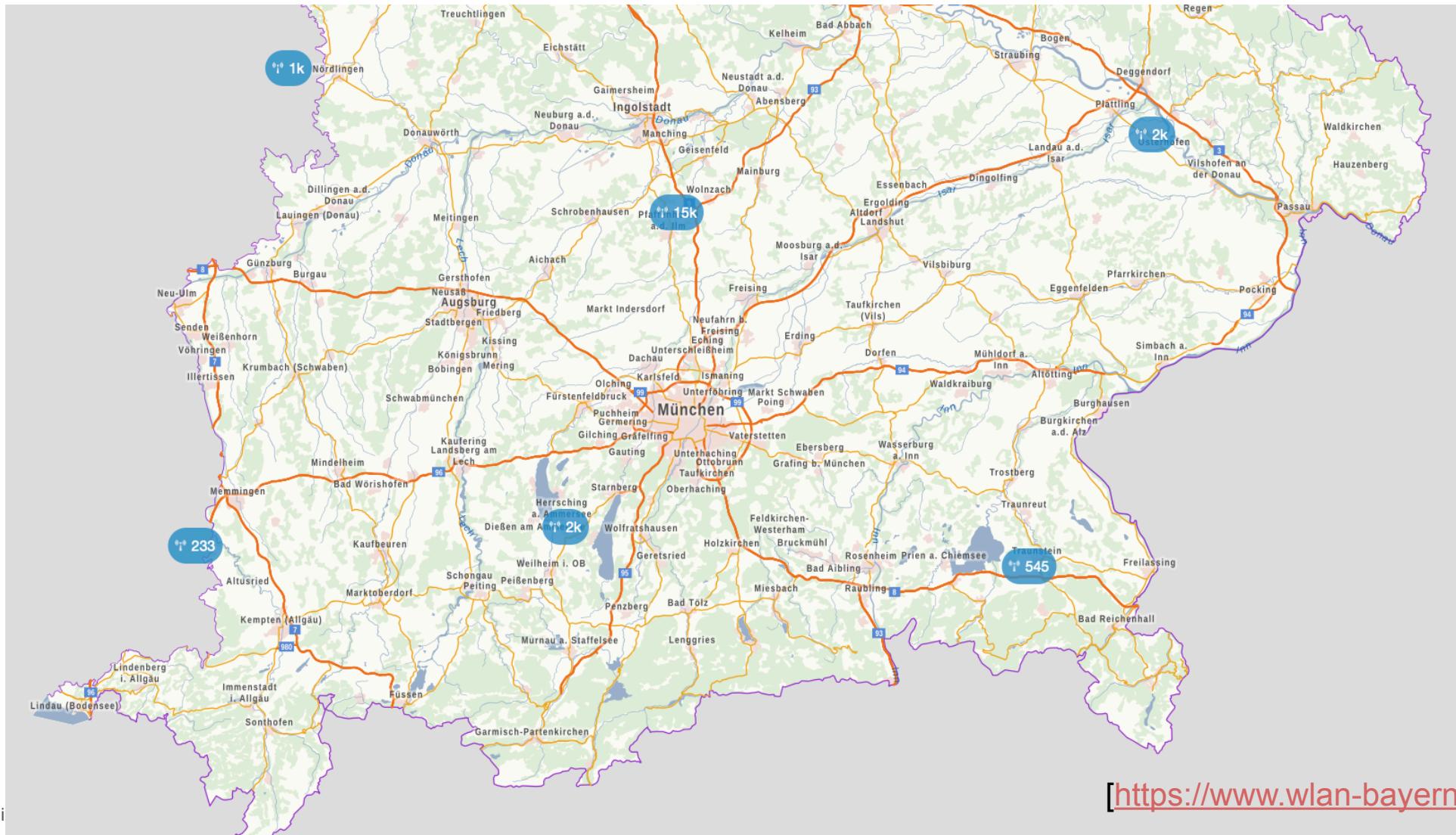


- Deutsches Forschungsnetz (DFN) unterstützt EoC
 - eduroam-Anbietervereinbarung mit dem DFN: regelt technische und organisatorische Randbedingungen
 - kostenfrei
- Access Points
 - Multi-SSID Fähigkeit: müssen (zus.) SSID „eduroam“ ausstrahlen
 - 802.1x mit WPA2 als Authentisierungsverfahren
 - Anfragender Radius-Server beim DFN (Deutsches Forschungsnetz)
- Radius-Server Verbund
 - Installation eines „radsecproxy“ (kostenfreie Software)
 - Musterkonfiguration und Dokumentation sind vorhanden
 - Anbindung an den Verbund über ein Zertifikat des DFN (kostenlos)

- Ausschreibung des Freistaats Bayern für „offenes WLAN“
- Bezugsrecht für alle staatlichen Behörden, Landkreise und Kommunen in Bayern für Hotspots
- Gewinner muss eduroam auf allen APs unterstützen und ausstrahlen
- Zuschlag wurde Anfang 2016 an Vodafone erteilt
- Ziel: 20.000 APs in ganz Bayern bis 2020
- Aktuell (Stand Herbst 2022)
 - ~ 28.000 APs davon 60 % (knapp 17.000) von Unis und Hochschulen

- Universitäten und Hochschulen können @BayernWLAN in ihren Netzen ausstrahlen
- Problem: Geschlossene Benutzergruppe innerhalb des Wissenschaftsnetzes (DFN)
- BayernWLAN Verkehr darf nicht über X-WiN geführt werden
- Deshalb eigener kommerzieller Übergang ins Internet
- Abwicklung von BayernWLAN macht Vodafone
 - Adresszuteilung
 - Abwicklung des Verkehrs
 - Abuse-Bearbeitung
- BayernWLAN-Ziel: 20.000 APs in ganz Bayern bis 2020
- Aktueller Stand Herbst 2022: ~28.000 APs , davon 60 % (17.000) von Unis und Hochschulen (gut 6.100 vom LRZ ;-)

@BayernWLAN Karte



eduroam & BayernWLAN Links



- Where can I Eduroam
 - <https://www.eduroam.org/where/>
 - In Deutschland: <https://map.eduroam.de/leaflet/eduroam/eduroam-map.html>
 - App Eduroam Companion (für Android und iOS)
- BayernWLAN Map
 - <https://www.wlan-bayern.de>
- WLAN im MWN
 - <https://monitoring.mwn.de/maps/wlan/>
 - Auslastungsstatistik: <http://wlan.lrz.de/apstat>
 - Wo bin ich im MWN?: <http://wobinich.mwn.de/>

Beispiel aus dem MWN

eduVPN



- Sicherer verschlüsselter Zugang von außen ins MWN
- eduVPN <https://www.edvpn.org/>
 - Entwickelt im Rahmen des GEANT Forschungsprojektes
 - Setzt auf openvpn auf
 - Managementerweiterungen
 - Client für Desktop und Mobilbetriebssysteme
 - Ermögliche 2 Faktorauthentisierung
 - „Automatische“ Anmeldung über Zertifikate mit kurzer Gültigkeit
 - Kooperation von 100 Sites und 18 Ländern
 - Damit „Ausgang“ in verschiedenen Ländern möglich
- <https://www.edvpn.org/>
- <https://doku.lrz.de/display/PUBLIC/VPN+-+eduVPN>

