

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick

4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick

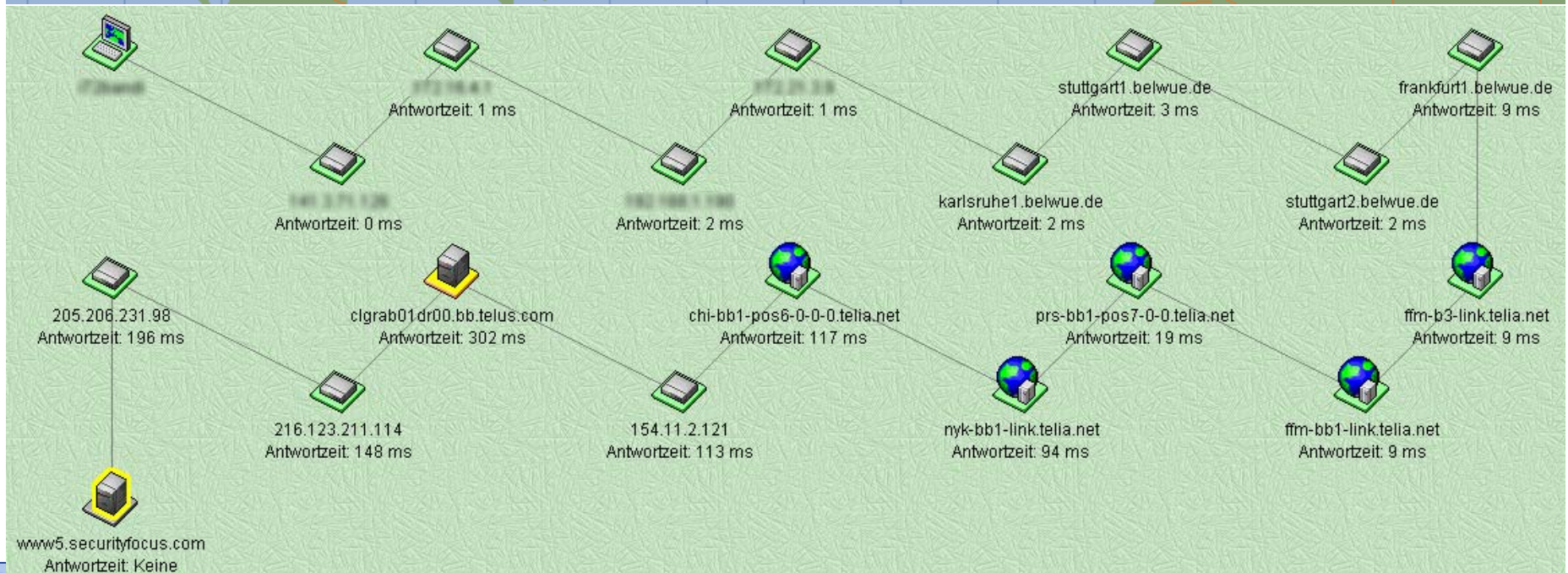
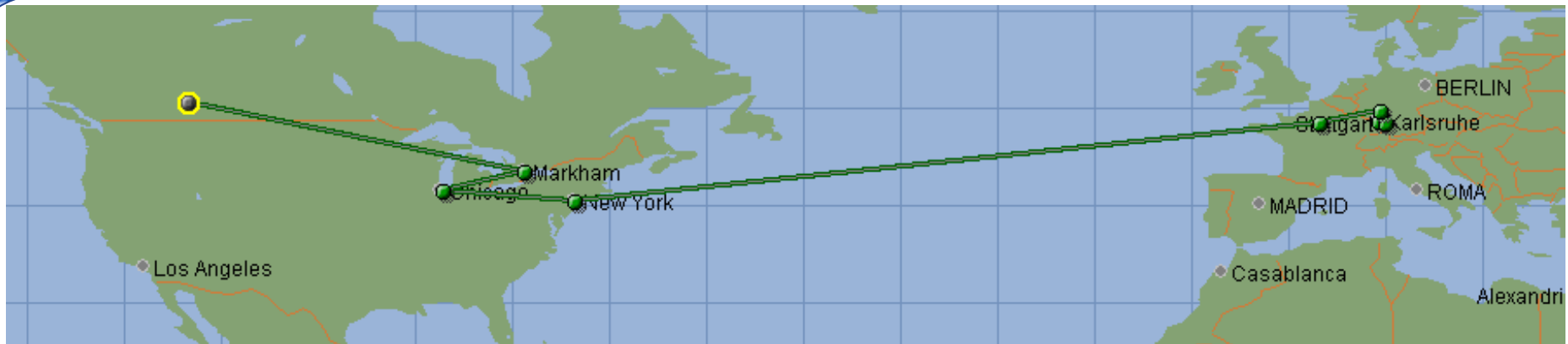
4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung

nächste VL



- Welche **Zugangsmöglichkeiten** zum Internet?
 - DSL, Modem, ISDN, DUKATH, Ethernet, Satellit, ...
- Wie geht es **im Netz** weiter?
 - > **traceroute www.securityfocus.com**
 - ▶ Daten laufen über mehrere Netzwerke (17 Hops)
 - ▶ BelWue (4 Hops), Telia (5 Hops), Telus, ...
 - ▶ 3 Hops ohne DNS Eintrag
- Schutzbedarf
 - wie kann der **Zugang zum Internet** geschützt werden?
 - ... und im Netz **Schutz der Infrastruktur!**?





- Beispiel **Netzinfrastruktur: Router**
 - Autorisierung über Passwort im Klartext (z.B. Telnet oder Weboberfläche über HTTP)
 - was kann ein Angreifer tun?
 - ▶ Passwort mitschneiden und sich selbst anmelden
- Beispiel **Netzzugang: WLAN**
 - ungesicherter WLAN-Zugang noch weit verbreitet
 - ▶ wie sicher ist denn ein LAN-Zugang?
 - was kann ein Angreifer tun?
 - ▶ über ARP-Spoofing allen Verkehr mitschneiden und Passwörter mitlesen
 - wie kann man sich schützen?
 - ▶ Mechanismen zur Verschlüsselung (WEP, WPA)
 - ▶ bis zu welchem Punkt schützen diese?

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit

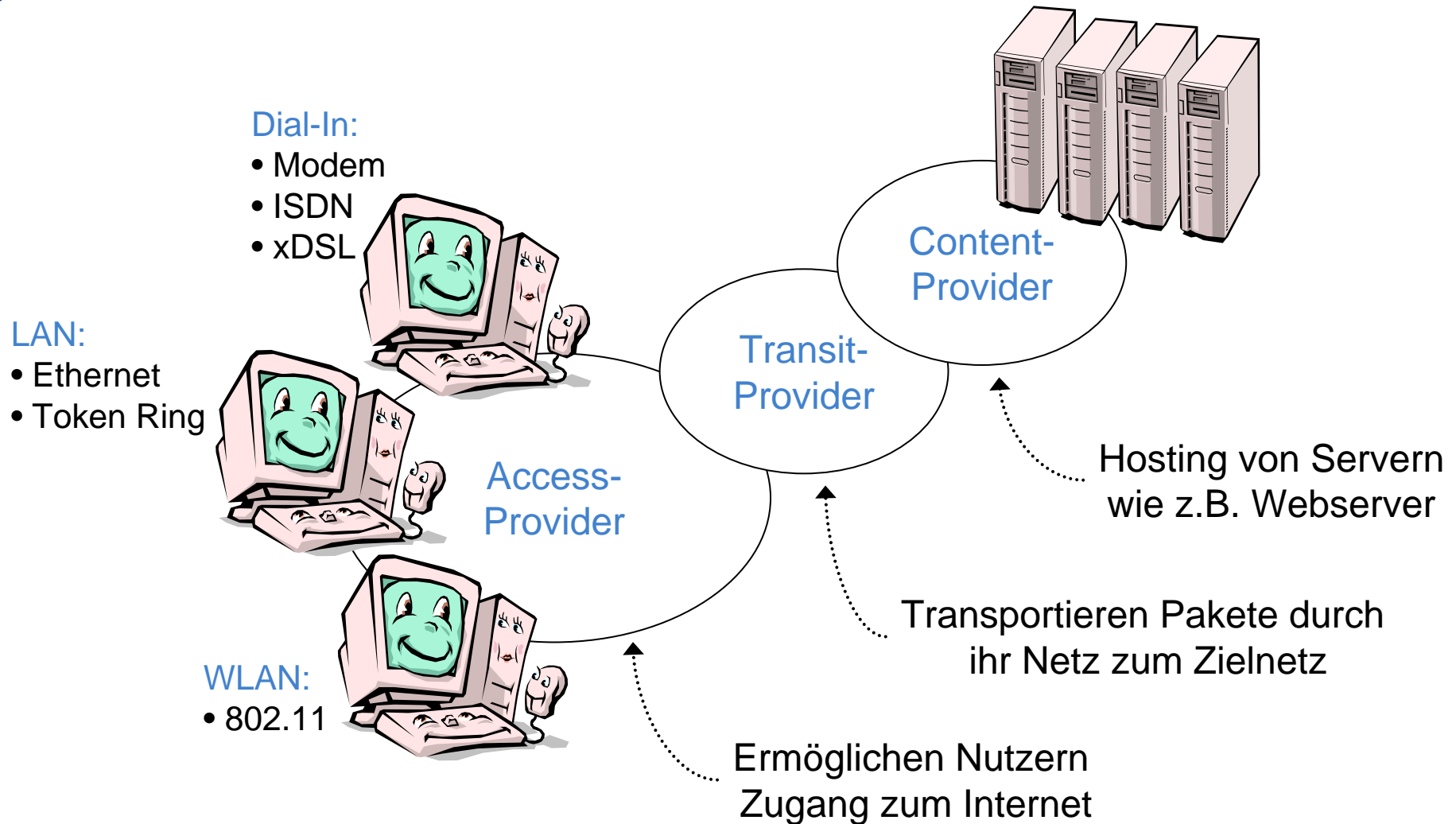


1. Motivation
2. Der Weg ins Internet
3. Überblick

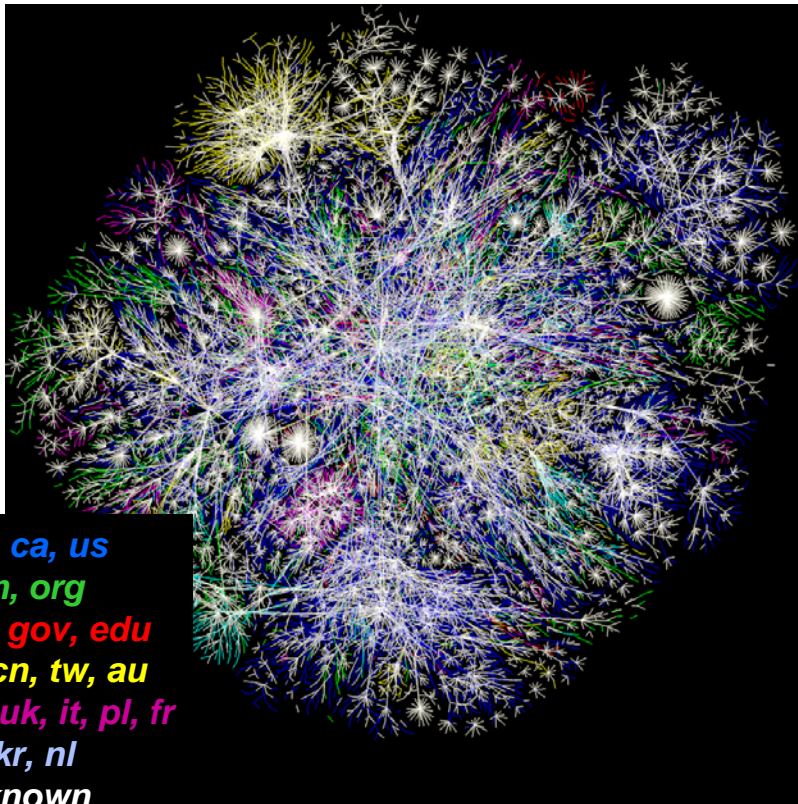
4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



Der Weg ins Internet

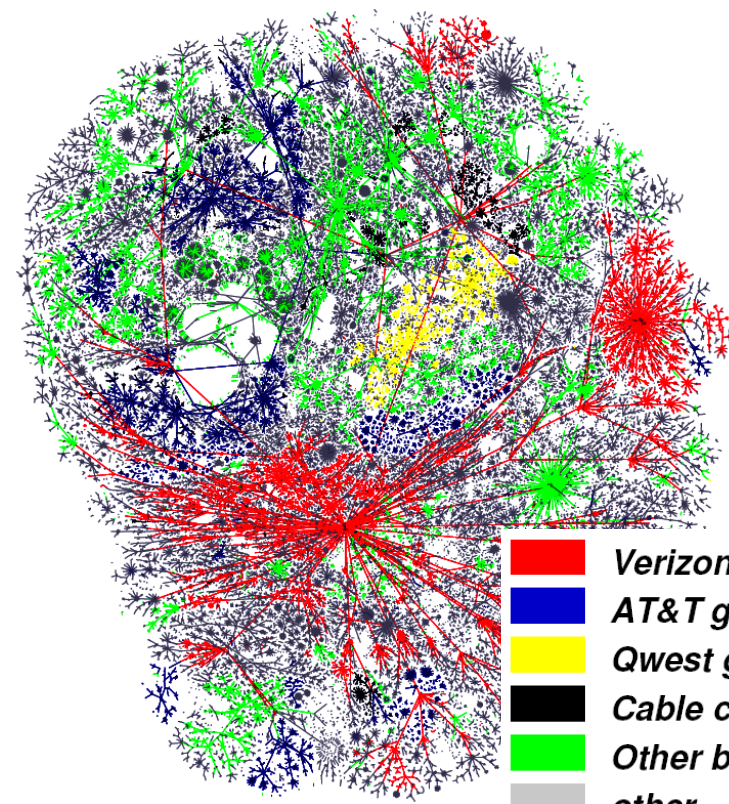


- Viele Zugänge, viele Provider, viele Netze, ...
→ überall **Sicherheitsmechanismen** notwendig



net, ca, us
com, org
mil, gov, edu
jp, cn, tw, au
de, uk, it, pl, fr
br, kr, nl
unknown

<http://www.opte.org/maps>



■ Verizon group
■ AT&T group
■ Qwest group
■ Cable companies
■ Other backbones
■ other

http://advice.cio.com/themes/CIO.com/cache/Internet_map_labels_0.pdf

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit

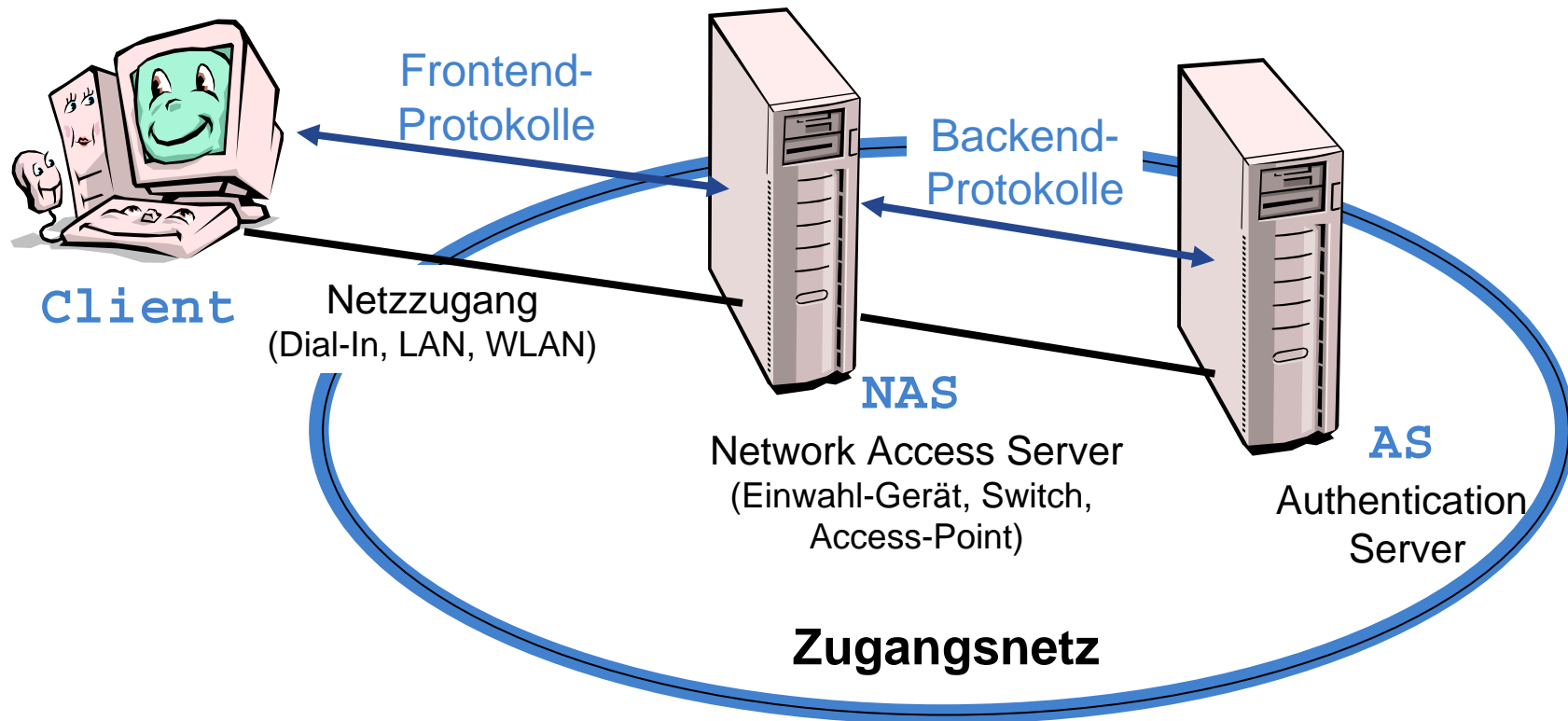


1. Motivation
2. Der Weg ins Internet
3. Überblick

4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



- Protokolle zur **Zugangskontrolle**
 - **Frontend**-Protokolle: zwischen **Client** und **NAS**
 - **Backend**-Protokolle: zwischen **NAS** und **AS**



- **Frontend-Protokolle:** *Kommunikation zwischen Endbenutzer und Netzwerkzugangsserver*
 - für Punkt-zu-Punkt Verbindungen: SLIP, PPP
 - für LAN: PPPoE, EAPoL (802.1x)
 - für WLAN: WEP (802.11), EAPoL (802.1x), WPA/WPA2 (802.11i)
- **Backend-Protokolle:** *Kommunikation zwischen Netzwerkzugangsserver und Authentifikationsserver*
 - auch AAA-Protokolle genannt (Authentifikation, Autorisierung, Accounting)
 - RADIUS
 - TACACS+
 - Diameter (Nachfolger von RADIUS)

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick

4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



- **RADIUS**

- Zugriffsschutz für Netzwerkressourcen
- Authentication, Authorization, Accounting (AAA)

- **PPP**

- Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
- **PAP, CHAP**: Einfache Authentifizierung
- **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung

- **PPPoE**

- Ethernet Verbindungen über xDSL

- **802.1x**

- Port-basierte Authentifizierung von Endgeräten

Backend

Frontend

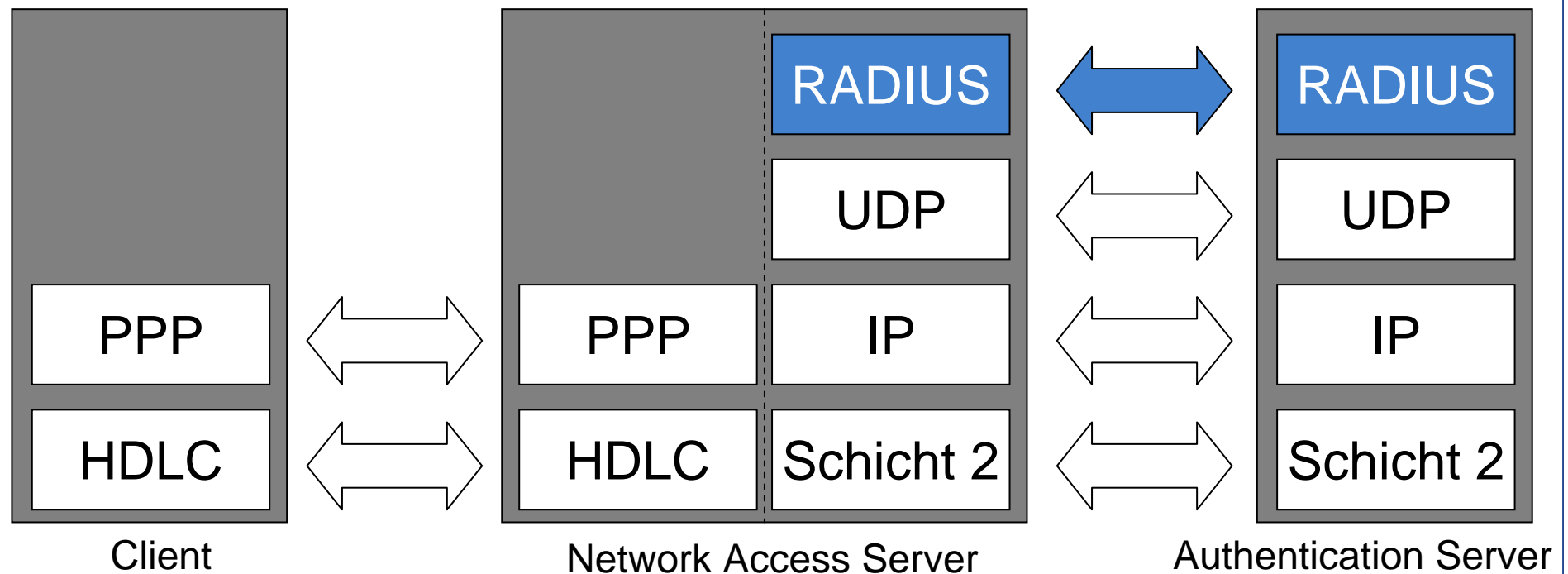
- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP**: Einfache Authentifizierung
 - **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

- Früher: Speicherung von Authentifikationsdaten auf **NAS**
 - Replizierung bei mehreren NAS Zugangspunkten
 - *Sicherheit der Authentifikationsdaten*
- Heute: Auslagerung auf **AS**
 - Protokoll zur Kommunikation zwischen NAS und AS notwendig

RADIUS: *Remote Authentication Dial In User Service*

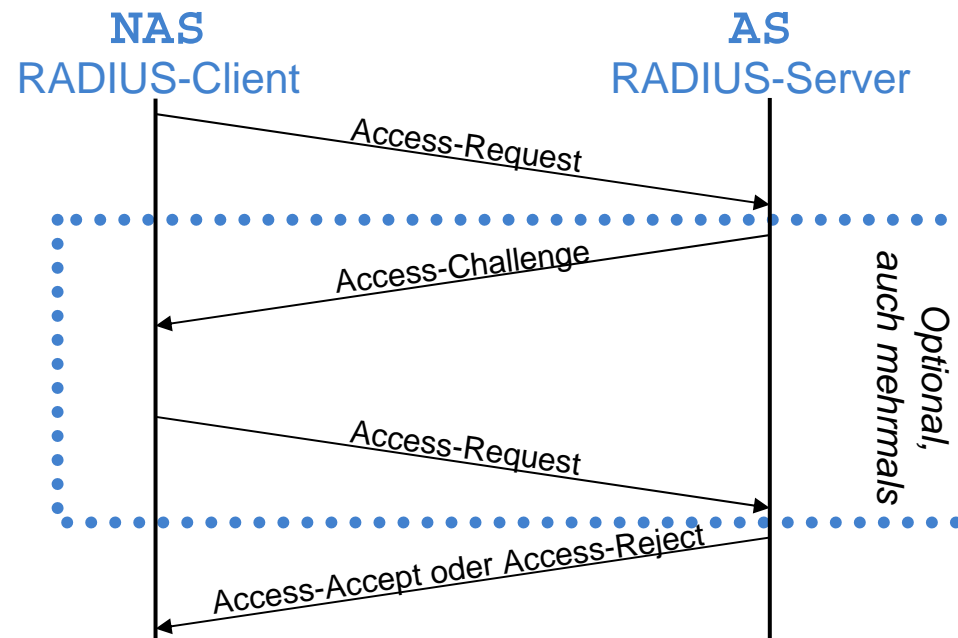
- **Backend-Protokoll** zum Transport von Daten zur
 - Authentifikation, Autorisation, Konfiguration des Einwahlbenutzers zwischen **NAS** und **AS**
- Einsatz bei
 - Modem-/ISDN-Einwahlserver, DSL-Zugangsserver
 - anderen Servern wie z.B. Netzwerkinfrastruktur
 - *Uni Karlsruhe DUKATH: RADIUS + IPsec*

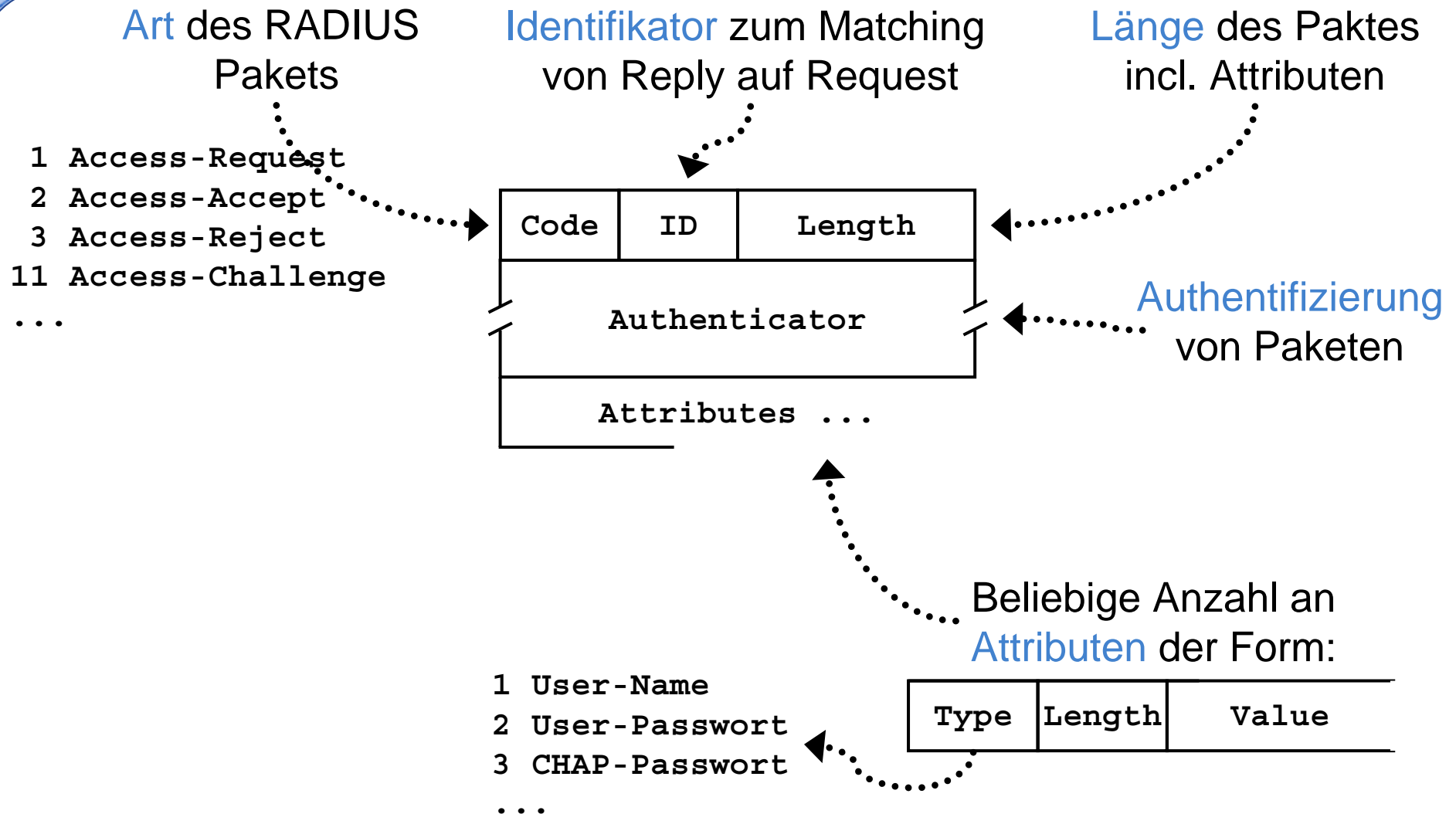
- Radius
 - arbeitet auf Anwendungsschicht über UDP
 - nur zwischen NAS und AS, Client nicht beteiligt



Rollen bei RADIUS

- **NAS** ist Client
 - transportiert Authentifikationsdaten aus Frontend-Protokoll zwischen Einwahlbenutzer und **AS**
- **AS** ist Server
 - authentifiziert Benutzer direkt oder
 - leitet Daten als Proxy zu einem anderen **AS** weiter (→ *Roaming*)





Schutz der Integrität von Nachrichten

- Request-Authenticator
 - Pakete mit Code **Access-Request**
 - Client wählt 16 Byte lange Zufallszahl
- Response-Authenticator
 - Pakete mit Code **Access-Challenge**, **Access-Accept** und **Access-Reject**
 - Anwendung von **MD5 auf Paket und Schlüssel**
$$\text{MD5 (Code + ID + Length + RequestAuthenticator + Attribute + Schlüssel)}$$

- Geschützte Übertragung von Attributen
→ z.B. Benutzerpasswort (Typ 2 User-Password)
- Verschlüsselung von Attributen
 - Partitionierung d. Attributs in 16-Byte-Blöcke p_1, \dots, p_n
 - 16 Byte langer Schlüssel S
 - Berechnung: Stromchiffre mit MD5 als PRF

$$\begin{aligned}
 c_1 &= p_1 \text{ xor MD5}(S + \text{RequestAuth}) \\
 c_2 &= p_2 \text{ xor MD5}(S + c_1) \\
 &\dots \\
 c_i &= p_i \text{ xor MD5}(S + c_{i-1})
 \end{aligned}$$

- Übertragung von c_1, \dots, c_i an Stelle von p_1, \dots, p_i

Zusammenfassung RADIUS

Angriffspunkte? Was muss geschützt werden? Wie wurde dies realisiert?

- **Authentizität** des Kommunikationspartners
 - Preshared Keys und MD5
 - **Authenticator**-Feld im RADIUS-Paket
- **Vertraulichkeit** der Authentifikationsdaten
 - Verschlüsselung sensibler Daten
 - *hidden attributes* mit Hilfe des Preshared Keys und MD5
- Schutz vor **Wiederholungsangriffen**
 - Verwendung von Zufallszahlen
 - **ID**-Feld im RADIUS-Paket

- **RADIUS**

- Zugriffsschutz für Netzwerkressourcen
- Authentication, Authorization, Accounting (AAA)

- **PPP**

- Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
- **PAP, CHAP**: Einfache Authentifizierung
- **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung

- **PPPoE**

- Ethernet Verbindungen über xDSL

- **802.1x**

- Port-basierte Authentifizierung von Endgeräten

Backend

Frontend

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication. Authorization. Accounting (AAA)
- **PPP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP:** Einfache Authentifizierung
 - **EAP, EAP-OTP:** Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

- Punkt-zu-Punkt-Verbindungen (**Point-to-Point**, PtP)
 - **Frontend-Protokolle** zum Verbinden von zwei Geräten
 - Übertragen Daten meist seriell
 - Übertragungsrichtungen parallel nutzbar (full duplex)
- Zwei typische Anwendungsszenarien
 - Dynamisch: **Einwahl** (z.B. ISDN, DSL)
 - Statisch: **WAN-Verbindungen** zwischen Routern (z.B. PDH/SDH)

Point-to-Point Protokoll (PPP) – Protokoll für PtP-Verbindungen

Erweiterungen

- Compression Control Protocol (CCP)
- Encryption Control Protocol (ECP)

Schicht 3-Konfiguration

- Initialisierung und Konfiguration von Schicht-3-Protokollen
- Network Configuration Protocol (**NCP**)

Protokollmultiplexing

- Multiplexing von Schicht-3-Protokollen

Schicht 2-Konfiguration

- Aufbau u. Test von Schicht-2-Verbindungen
- Link Configuration Protocol (**LCP**)

Optionsaushandlung: Kern von PPP

- Erweiterbarer Mechanismus zur Aushandlung von Optionen
- Aushandlung in beide Richtungen individuell

Eingliederung von PPP in das ISO/OSI-Schichtenmodell

Schicht 3 *Netzwerkschicht*

Schicht-3-Instanz 1
z.B. IP

...

Schicht-3-Instanz n
z.B. IPX

NCPs: Initialisierung und Konfiguration

PPP

NCP

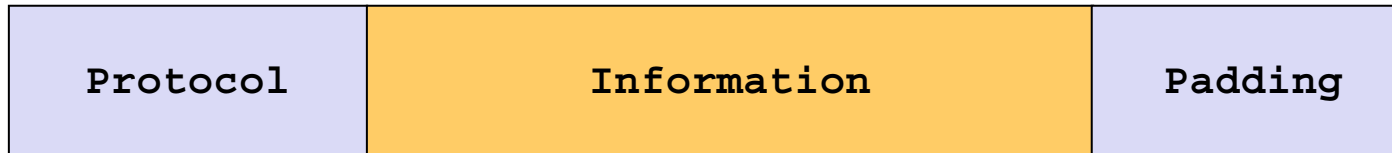
Weitere Protokolle z.B. EAP

LCP

LCP: Verbindungsaufbau,
Test und Überwachung

Schicht 2 *Sicherungsschicht*

Schicht-2-Instanz
z.B. HDLC, Ethernet, AAL5



- **Protocol:**
 - 8 oder 16 Bit: Mechanismus für erweiterbare Adressfelder
 - **Identifiziert den Inhalt des Rahmens**, ermöglicht somit (De)-Multiplexing
- **Information:**
 - **Enthält Daten** des durch Protocol identifizierten Protokolls
 - Maximum Receive Unit (MRU): maximale Länge inkl. Padding (Default 1500 Bytes, andere Längen verhandelbar)
- **Padding:**
 - Optional beliebige Anzahl von Padding-Bytes (bis zur MRU)

- Transport von PPP über Link-Layer-Protokolle
 - HDLC (z.B. ISDN, SDH/SONET)
 - Ethernet
 - Frame-Relay
 - ATM-Adaption-Layer (AAL2, AAL5)

PPP in HDLC, z.B. PPP over SDH/SONET

Flag 01111110	Address 11111111	Protocol 00000011	PPP-Rahmen	FCS 16/32 Bits	Flag 01111110
------------------	---------------------	----------------------	------------	-------------------	------------------

PPP over Ethernet (PPPoE)

Destination	Source	EtherType =0x8864	PPP-Rahmen	FCS
-------------	--------	----------------------	------------	-----

AAL5, z.B. LLC encapsulated PPP

LLC-Header	NLPID =0xCF	PPP-Rahmen	Padding	CPCS-PDU Trailer
------------	----------------	------------	---------	---------------------

Link Configuration Protocol (LCP)

- Auf- und Abbau von Schicht-2-Verbindungen
 - Aushandlung von Optionen (Rahmenformat, max. Paketgröße)
 - Erkennung von Fehlern
 - ▶ z.B. Loop-back: gesendete Pakete werden wieder empfangen
- LCP verhandelt optional
 - Protokoll für Authentifikation des Kommunikationspartners
 - ▶ *Password Authentication Protocol* (PAP)
 - ▶ *Challenge Handshake Authentication Protocol* (CHAP)
 - ▶ *Extensible Authentication Protocol* (EAP)
 - Protokoll für Test und Überwachung der Qualität der Verbindung
 - ▶ *PPP Link Quality Monitoring*
 - Kompression

Behandelte Authentifikationsprotokolle für PPP

- Grundmechanismen (*diese VL*)
 - PAP: *Password Authentication Protocol*
 - CHAP: *Challenge Handshake Authentication Protocol*
 - EAP: *Extensible Authentication Protocol*
- für WLAN: EAP-Erweiterungen auf TLS (*nächste VL*)
 - EAP-TLS: *EAP Transport Layer Security*
 - PEAP: *Protected EAP*
 - EAP-TTLS: *EAP Tunneled TLS*

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP, LCP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP:** Einfache Authentifizierung
 - **EAP, EAP-OTP:** Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

Password Authentication Protocol (PAP)

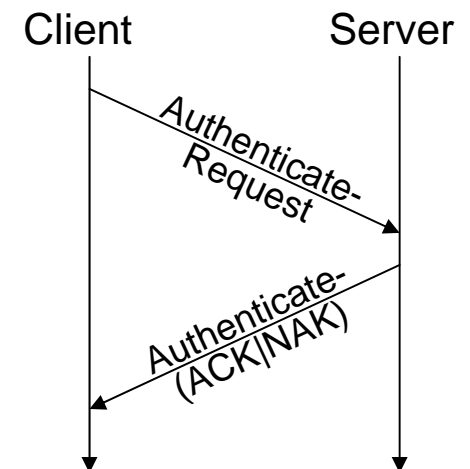
- Ablauf

- Client schickt ID/Passwort-Paar
- Server bestätigt oder beendet Verbindung

- Schwächen

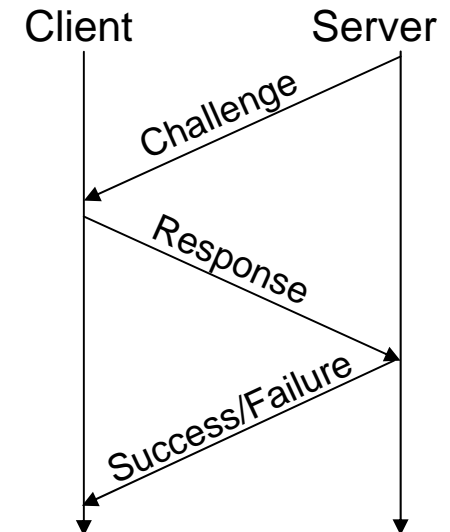
- Übertragung des Passwort im Klartext
 - ▶ Replay-Angriffe möglich
- Client ist Initiator
 - ▶ kann Anfrage-Frequenz bestimmen
 - ▶ dadurch DoS-Angriffe möglich
- beide Teilnehmer müssen das Passwort in Klartext kennen

- PAP nur **Notlösung**, wenn kein anderes Protokoll verhandelt werden konnte



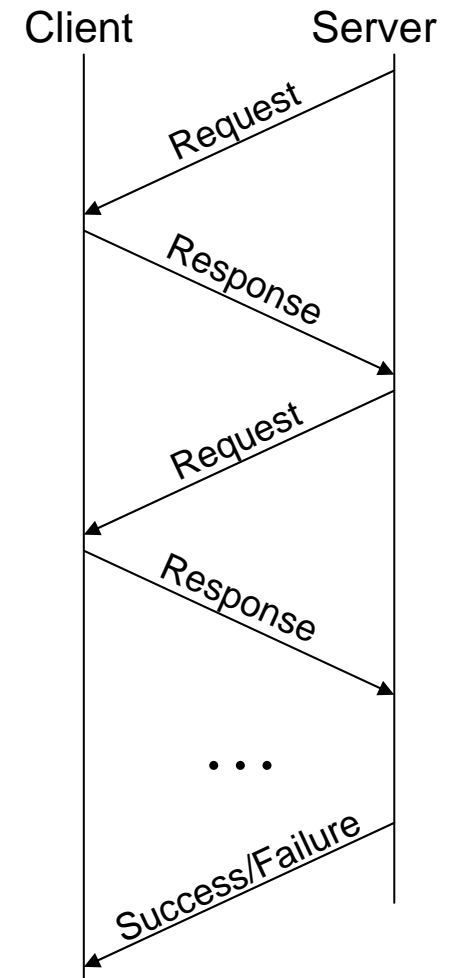
Challenge Handshake Authentication Protocol (CHAP)

- 3-way Handshake
 - Server schickt Challenge (Zufallszahl)
 - Client sendet errechnete Response
 - ▶ z.B. MD5 (Challenge, Passwort)
 - Server prüft Ergebnis, antwortet entsprechend
- Vorteile von CHAP gegenüber PAP
 - Passwort nicht im Klartext
 - Replay-Angriff nicht möglich (bei guter Challenge)
 - Server ist Initiator
 - ▶ kann Zeitpunkt und Frequenz der Anfragen bestimmen
 - ▶ legt bei Misserfolg Wiederholung fest
 - Algorithmen wählbar: MD5, SHA-1, MS-CHAP
- Nachteil: auch hier muss **Passwort auf dem Server in Klartext** gespeichert werden



Extensible Authentication Protocol (EAP)

- **Generisches Protokoll zur Authentifizierung**
 - von LCP wie PAP/CHAP ausgehandelt
 - tatsächlich verwendeter Mechanismus erst während der EAP-Protokoll-Phase ermittelt
 - ermöglicht Einholen von weiteren Daten vor der Entscheidung für Mechanismus
- **Ablauf**
 - Server (eine oder mehrere) Anfragen an Client
 - ▶ z.B. Frage nach ID, Senden einer Challenge
 - Client sendet angeforderte Daten zurück oder lehnt Anfrage ab (mit Gegenvorschlag)
 - Server antwortet mit Erfolg/Misserfolg, wenn keine weiteren Fragen anstehen bzw. wenn Ergebnis der Authentifikation feststeht



EAP standardisierte Request/Response-Typen

- **Identity**
 - Ermittlung der ID des zu authentifizierenden Clients
 - meist erster Protokoll-Austausch
- **Notification**
 - Übertragung einer Nachricht an den Client, die bestätigt werden muss
 - z.B. Warnungen, dass Passwort bald erneuert werden muss
- **NAK** (nur als Antwort verwendbar)
 - Ablehnung einer Anfrage
- **MD5-Challenge** (wie CHAP aber mit folgenden Unterschieden)
 - enthält Gegenvorschlag
 - Client kann Mechanismus ablehnen (NAK), Gegenvorschlag machen
- **Generic Token Card**
 - wie CHAP, nur Hardware-basiert
- **One-Time Password** (OTP)
 - siehe nächste Folien



- Code: Typ des Pakets
 - 1 Request
 - 2 Response
 - 3 Success
 - 4 Failure
- ID: ermöglicht Zuordnung von Antworten auf Anfragen
- Typ: Request/Response-Typ an
 - z.B. 1=Identity

- One-Time Password (OTP)
 - Verhindern von Replay-Angriffen durch Einmal-Passwörter
 - Mechanismus erstmals von Leslie Lamport veröffentlicht (1981)
 - Implementierung S/KEY diente als Grundlage für OTP
- Initialisierung
 - Client vereinbart mit Server Passphrase, Seed, Hash-Algorithmus
 - Client berechnet Einmal-Passwörter
$$S_0 = \text{hash}(\text{Passphrase} + \text{Seed})$$
$$S_1 = \text{hash}(S_0)$$
$$\dots$$
$$S_{n-1} = \text{hash}(S_{n-2})$$
 - Server berechnet S_n , speichert Paar $\{n, S_n\}$ und vergisst dann die Passphrase (!)

Ablauf der Authentifikation

- Server schickt Client Challenge
 - $\{\text{Seed}, \text{Hash-Funktion}, n-1\}$
- Client sendet S_{n-1} zurück
- Server
 - Verifiziert $\text{hash}(S_{n-1}) \stackrel{?}{=} S_n$
 - Speichert Paar $\{n-1, S_{n-1}\}$ für nächste Authentifikation
 - wenn letztes Passwort S_0 benutzt wurde, neue Initialisierung

Darstellung des Einmal-Passworts

- Hexadezimal-kodiert (schwer zu merken)
- Six-Word-Format
 - 64 Bit durch Prüfbits auf 66 Bit erweitert und in 6x11 Bit unterteilt
 - 11 Bit dienen als Schlüssel in Wörterbuch mit 2048 Einträgen
 - Ergebnis-Beispiel: OUST COAT FOAL MUG BEAK TOTE

- | | |
|--|---|
| 0 RESERVED | 25 PEAP |
| 1 Identity | 26 MS-EAP-Authentication] |
| 2 Notification | 27 Mutual Authentication w/Key Exchange (MAKE) |
| 3 Legacy Nak | 28 CRYPTOCARD |
| 4 MD5-Challenge | 29 EAP-MSCHAP-V2 |
| 5 One-Time Password (OTP) | 30 DynamID |
| 6 Generic Token Card (GTC) | 31 Rob EAP] |
| 7 Allocated | 32 Protected One-Time Password |
| 8 Allocated | 33 MS-Authentication-TLV |
| 9 RSA Public Key Authentication | 34 SentiNET |
| 10 DSS Unilateral | 35 EAP-Actiontec Wireless |
| 11 KEA | 36 Cogent Systems Biometrics Authentication EAP |
| 12 KEA-VALIDATE | 37 AirFortress EAP |
| 13 EAP-TLS | 38 EAP-HTTP Digest |
| 14 Defender Token (AXENT) | 39 SecureSuite EAP |
| 15 RSA Security SecurID EAP | 40 DeviceConnect EAP |
| 16 Arcot Systems EAP | 41 EAP-SPEKE |
| 17 EAP-Cisco Wireless | 42 EAP-MOBAC |
| 18 GSM Subscriber Identity Modules (EAP-SIM) | 43 EAP-FAST |
| 19 SRP-SHA1 | 44 ZoneLabs EAP (ZLXEAP) |
| 20 AVAILABLE | 45 EAP-Link |
| 21 EAP-TTLS | 46 EAP-PAX |
| 22 Remote Access Service | 47 EAP-PSK |
| 23 EAP-AKA Authentication | |
| 24 EAP-3Com Wireless | |

- Problem bei **RADIUS mit EAP**
 - **NAS** authentifiziert Client meist über PPP/EAP oder 802.1x/EAPoL
 - muss Daten zwischen EAP-Paketen und Radius-Attributen kopieren
- **RADIUS-Erweiterung**
 - neues RADIUS-Attribut
 - ▶ **EAP-Message**: Transport von EAP-Paketen zwischen Client und Server
 - EAP-Pakete können direkt zwischen PPP und RADIUS kopiert werden

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP, LCP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP**: Einfache Authentifizierung
 - **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

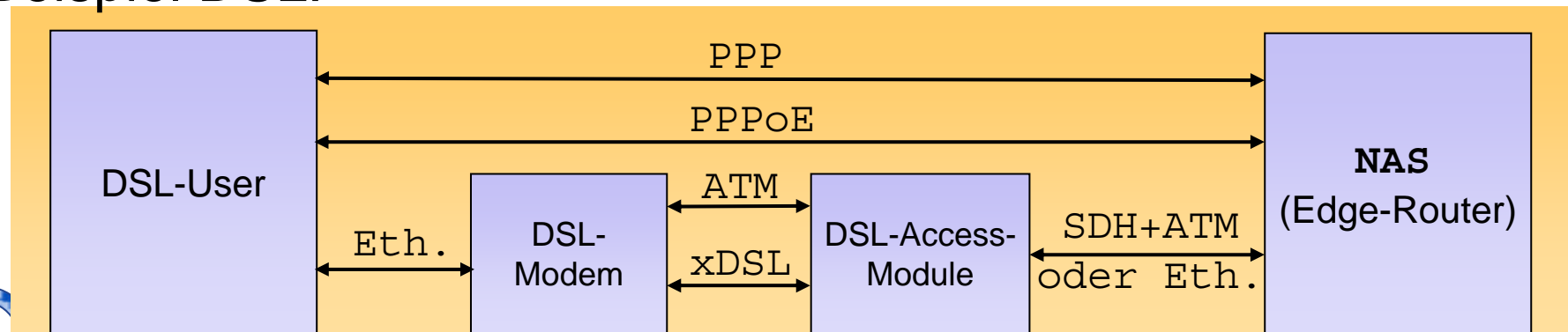
Problem

- Ethernet als Anschlusstechnologie für Kundengeräte (*Customer Premises Equipment*) attraktiv
- aber: **fehlende Funktionalität in Ethernet**
 - ▶ Authentifikation, Aushandlung von Optionen, Accounting

Lösung: **PPP over Ethernet** (PPPoE)

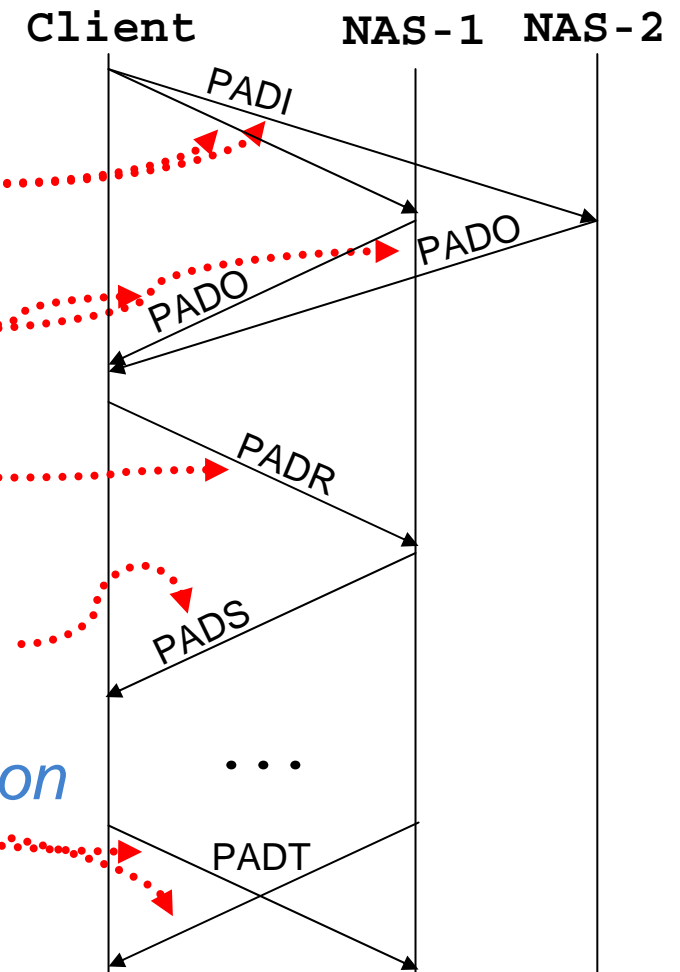
- **Discovery Stage**
 - ▶ Client lokalisiert NAS und handelt mit NAS Session aus
 - ▶ Client oder Server können jeder Zeit Session terminieren
- **PPP Session Stage**
 - ▶ PPP-Rahmen werden in Ethernet-Rahmen übertragen

Beispiel DSL:

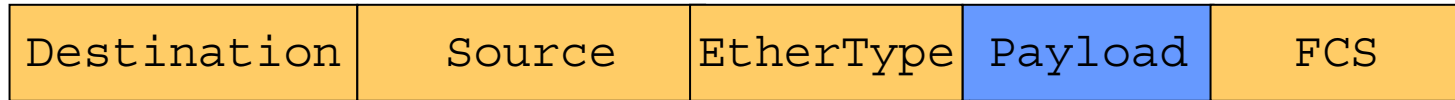


- Sitzungsaushandlung

- *PPPoE Active Discovery* **Initiation** (PADI)
- *PPPoE Active Discovery* **Offer** (PADO)
- *PPPoE Active Discovery* **Request** (PADR)
- *PPPoE Active Discovery* **Session-Confirmation** (PADS)
- *PPPoE Active Discovery* **Termination** (PADT)

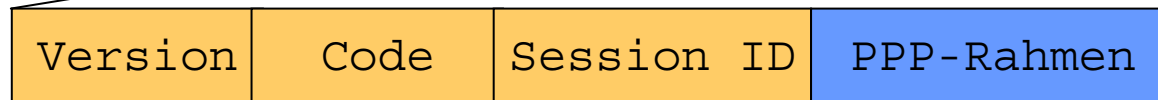


Ethernet-Rahmen
(Client-Server)



wobei EtherType=0x8864

PPPoE-Rahmen



- Fazit
 - Nutzung von PPP Mechanismen wie Authentifikation und Accounting
 - einheitlicher Mechanismus beim Access-Provider für Einwahl und erleichtertes Management
 - Aber:
 - nicht sinnvoll im großen Stil
 - ▶ z.B. jeder Rechner in LAN-Segment baut PPPoE-Verbindung zu Gateway auf
- Portbasierte Authentifizierung: 802.1x

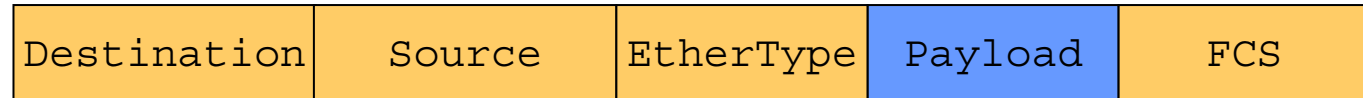
- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP, LCP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP**: Einfache Authentifizierung
 - **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

- Probleme
 - unautorisierte Nutzung ungenutzter Switch-Ports
 - Missbrauch schon genutzter Ports
- 802.1x: IEEE Standard for Local and metropolitan area networks – Port based Access Control
 - Authentifizierung von Geräten, die über PtP-Verbindung angeschlossen werden (z.B. an dedizierten Switch-Port)
 - Freischaltung des Ports nach erfolgreicher Authentifikation
 - ▶ vorher nur Authentifikationsverkehr zugelassen
 - Reauthentifizierung
 - ▶ nach definierter Zeitspanne
 - ▶ wenn Port inaktiv wurde (z.B. durch Abziehen des Kabels)
- 802.1x verwendet EAP-Mechanismen von PPP
 - EAP direkt in Ethernet-Rahmen eingebettet
 - EAP over LANs (EAPoL)

- **Port Access Entities** (PAE, Teilnehmer des PtP-Links) nehmen folgende Rollen an
 - Client, als **Supplicant** bezeichnet, authentifiziert sich
 - NAS, als **Authenticator** bezeichnet, schaltet Port nach erfolgreicher Authentifikation frei
 - Beide Teilnehmer können bei Bedarf beide Rollen annehmen (z.B. Verbindung zwischen zwei Switches)
 - Prüfung der Authentifizierungsdaten durch NAS oder durch AS (z.B. via RADIUS)
- **Authentifizierung durch EAP-Protokoll**
 - Zwischen Client und NAS via Ethernet-Rahmen
 - Zwischen NAS und AS via Backend-Protokoll (z.B. RADIUS mit EAP-Erweiterung)

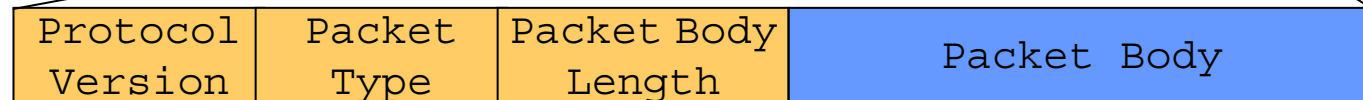
Einbettung von EAP

Ethernet-Rahmen
(Client – Server)



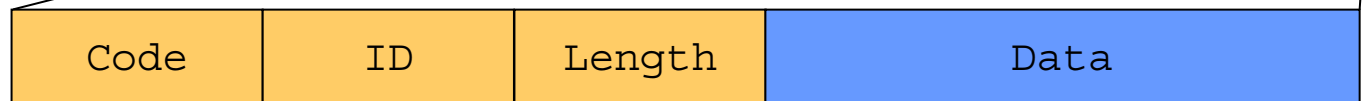
Wenn
EtherType = 0x888E

EAPoL-Rahmen



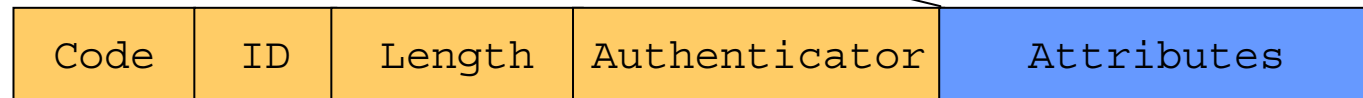
Wenn
Packet Type = EAP-Packet

EAP-Rahmen



In
EAP-Message-Attribut

RADIUS-Rahmen
(NAS – AS)



Protokoll-Ablauf

