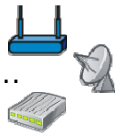
Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

nächste VL

Motivation

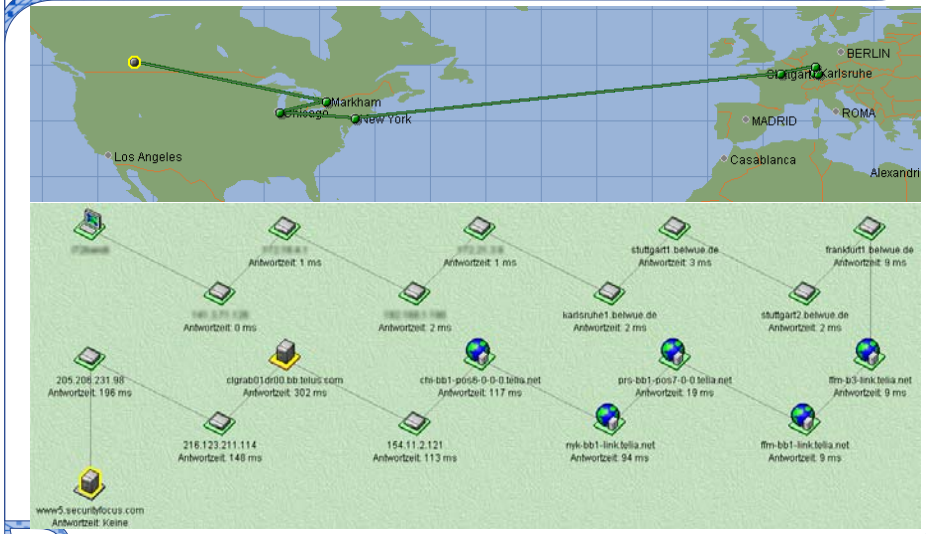
- Welche Zugangsmöglichkeiten zum Internet?
  - DSL, Modem, ISDN, DUKATH, Ethernet, Satellit, …



- 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!?

Motivation – Traceroute



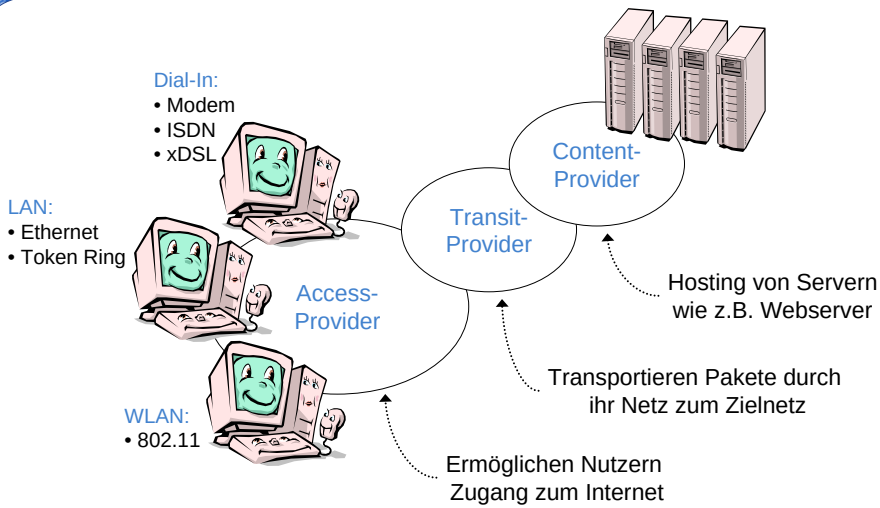
Neotrace von NeoWorx Inc.,

Motivation – Angriffspunkte

- 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
    - wir 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?

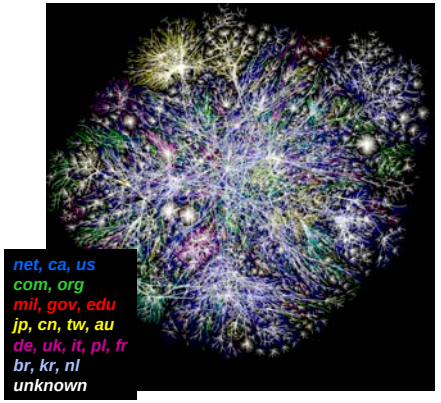
Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

Der Weg ins Internet

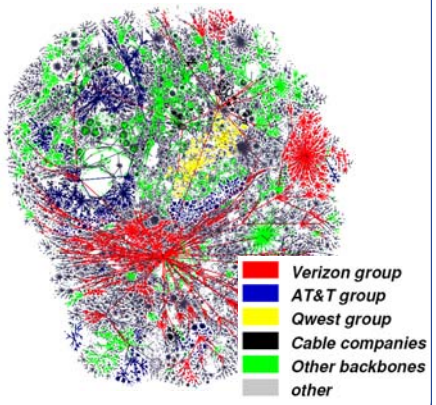


Der Weg ins Internet

- Viele Zugänge, viele Provider, viele Netze, …
  → überall Sicherheitsmechanismen notwendig



http://www.opte.org/maps

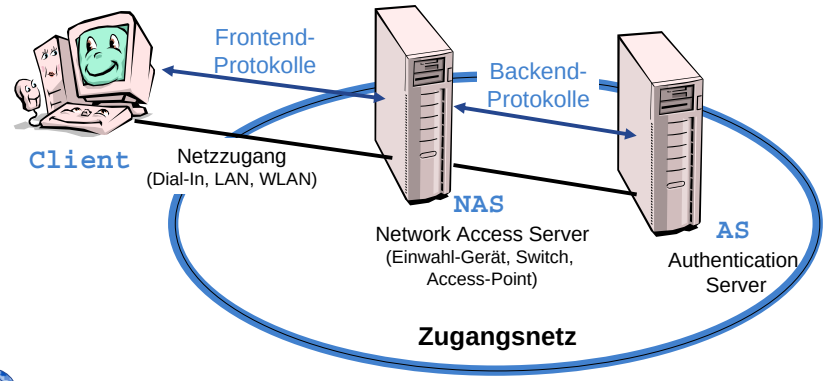


http://advice.cio.com/themes/CIO.com/cache/Internet_map_labels_0.pdf

Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

Überblick

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



Überblick

- 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)

Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

1. Motivation
2. Der Weg ins Internet
3. Überblick
4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung

Netzzugang – Übersicht

- 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

Netzzugang – Übersicht

- 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

RADIUS

- 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

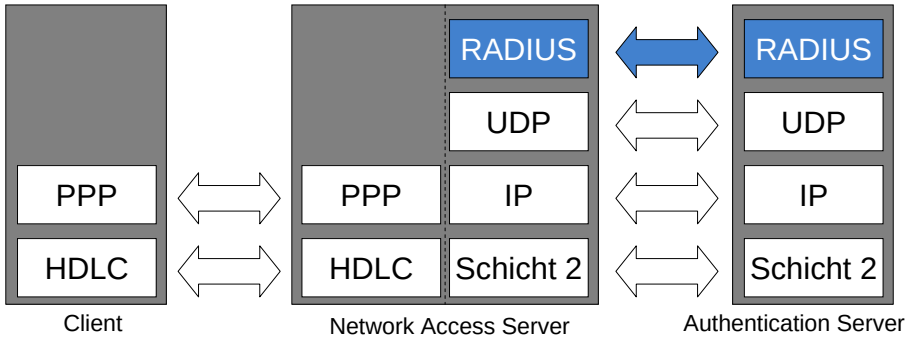
RADIUS: *Remote Authentication Dial In User Service*

- 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 im Protokollstack

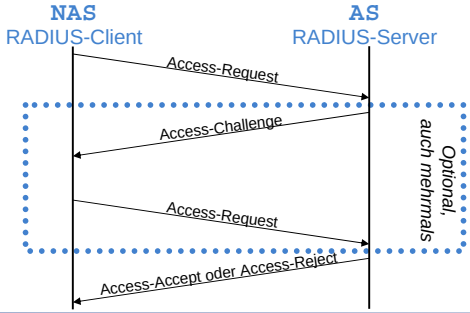
- Radius
  - arbeitet auf Anwendungsschicht über UDP
  - nur zwischen NAS und AS, Client nicht beteiligt



Rollen und Protokollablauf

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*)



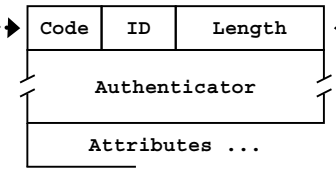
Paketformat

Art des RADIUS Pakets

```
1 Access-Request
2 Access-Accept
3 Access-Reject
11 Access-Challenge
...
```

Identifikator zum Matching von Reply auf Request

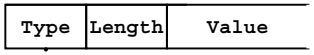
Länge des Paktes incl. Attributen



Authentifizierung von Paketen

Beliebige Anzahl an Attributen der Form:

```
1 User-Name
2 User-Password
3 CHAP-Password
...
```



Authenticator-Feld und hidden attributes

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

```
MD5(  Code + ID + Length      +
      RequestAuthenticator    +
      Attribute + Schlüssel   )
```


Authenticator-Feld und hidden attributes

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

$$c_1 = p_1 \text{ xor } MD5(S + RequestAuth)$$
$$c_2 = p_2 \text{ xor } MD5(S + c_1)$$
$$\ldots$$
$$c_i = p_i \text{ xor } MD5(S + c_{i-1})$$

- Übertragung von $c_1,\ldots,c_i$ an Stelle von $p_1,\ldots,p_i$

Sicherheitsmechanismen

Zusammenfassung RADIUS

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

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

Netzzugang – Übersicht

- 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

Netzzugang – Übersicht

- 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

- 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

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

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

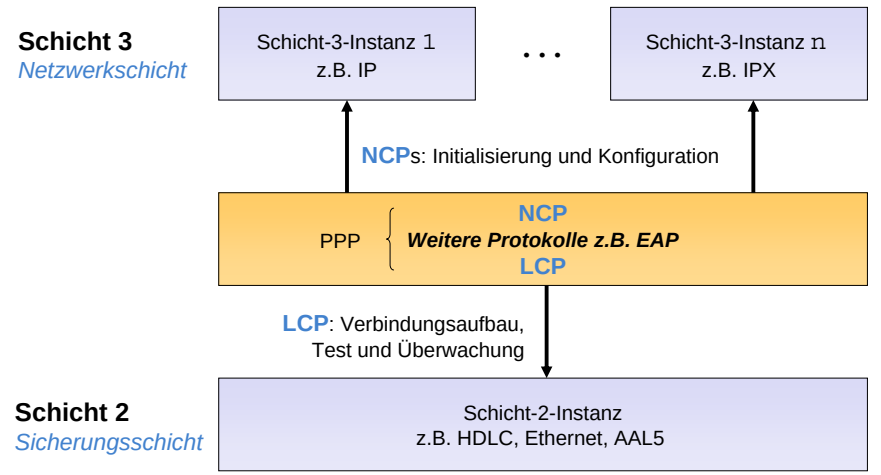
Schicht 3-Konfiguration
- Initialisierung und Konfiguration von Schicht-3-Protokollen
- Network Configuration Protocol (**NCP**)

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



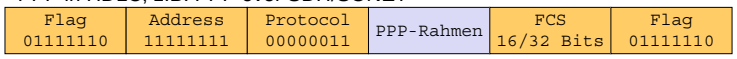
PPP-Rahmen

- **`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)

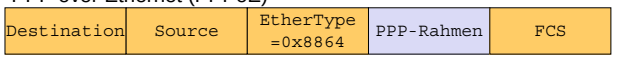
Einbettung in Schicht 2

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

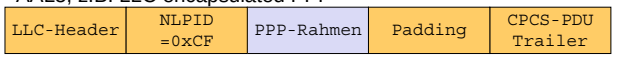
PPP in HDLC, z.B. PPP over SDH/SONET



PPP over Ethernet (PPPoE)



AAL5, z.B. LLC encapsulated PPP



Link Configuration Protocol

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

PPP-Authentifikationsmechanismen

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*

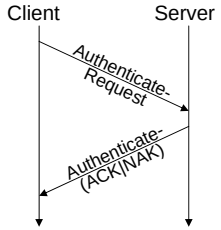
Netzzugang – Übersicht

- 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

Password Authentication Protocol (PAP)

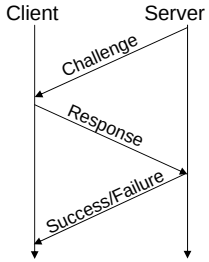
- Ablauf
  - Client schickt ID/Passwort-Paar
  - Server bestätigt oder beendet Verbindung



- Schwächen
  - Übertragung des Passwort im Klartext
    - Replay-Angriffe möglich
  - Client ist Initiator
    - kann Anfrage-Frequenz bestimmten
    - 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

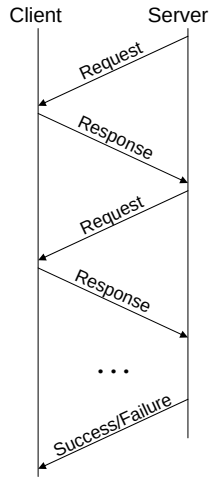
Challenge Handshake Authentication Protocol (CHAP)



- 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

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

Grundmechanismen von EAP

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

EAP-Rahmen

- `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`

EAP-Modul: One-Time Password

- 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 = hash(Passphrase+Seed)

    S_1 = hash(S_0)

    ...

    S_{n-1} = hash(S_{n-2})
  - Server berechnet S_n, speichert Paar $\{n, S_n\}$ und vergisst dann die Passphrase (!)

EAP-Modul: One-Time Password (2)

Ablauf der Authentifikation

- Server schickt Client Challenge
  - {Seed,Hash-Funktion,n-1}
- Client sendet S_{n-1} zurück
- Server
  - Verifiziert hash(S_{n-1}) $=^?$ 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

Weitere registrierte EAP-Mechanismen

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

Quelle: http://www.iana.org/assignments/eap-numbers

Einschub: RADIUS und EAP

- 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

Netzzugang – Übersicht

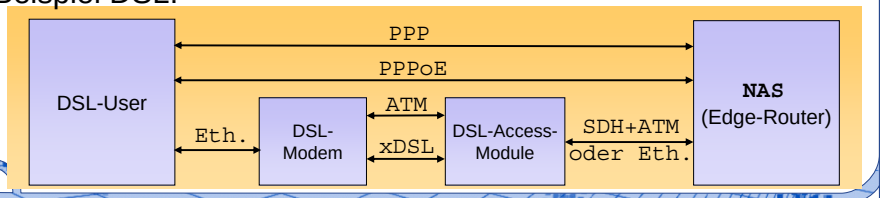
- RADIUS
  - Zugriffsschutz für Netzwerkressourcen
  - Authentication, Authorization, Accounting (AAA)
- PPP, LCP
  - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
  - PAP, CHAP: Einfache Authentifizierung
  - EAP, EAP-OTP: Generisches Protokoll zur Authentifizierung
- PPPoE
  - Ethernet Verbindungen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

PPP over Ethernet

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

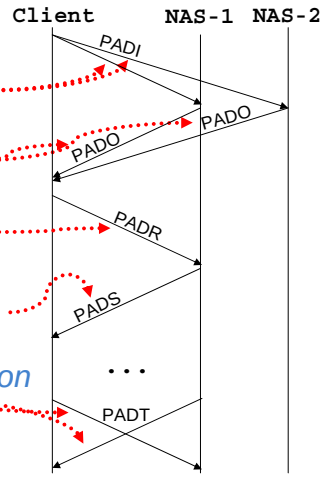
Lösung: PPP over Ethernet (PPPoE)
- **`Discovery Stage`**
  - Client lokalisiert `NAS` und handelt mit `NAS` Session aus
  - Client oder Server können jeder Zeit Session terminieren
- **`PPP Session Stage`**
  - PPP-Rahmen werden in Ethernet-Rahmen übertragen

Beispiel DSL:

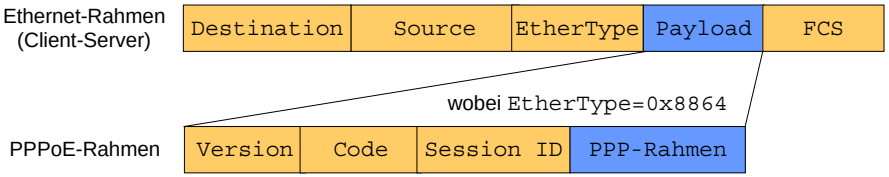


PPPoE: Discovery Stage

- 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)



PPPoE Fazit



- 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

Netzzugang – Übersicht

- 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

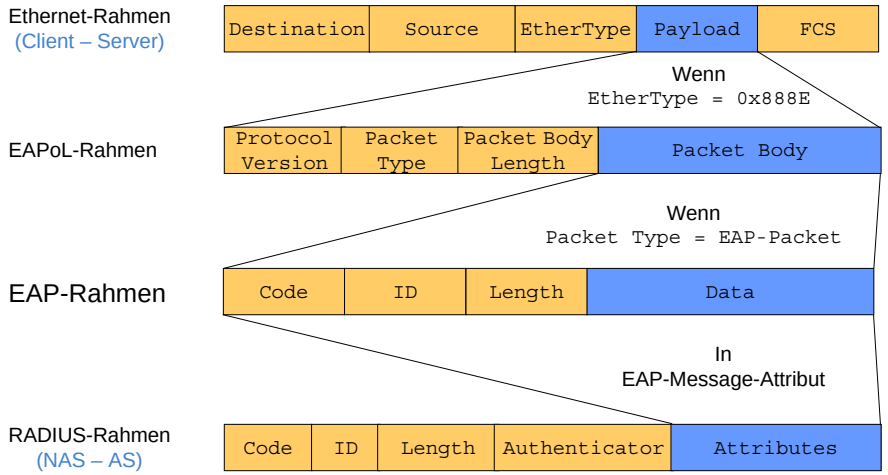
IEEE 802.1x - Ethernet

- Probleme
  - unautorisierte Nutzung ungenutzer 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)

Funktionsprinzip

- 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



Protokoll-Ablauf