IT-Sicherheit

- Sicherheit vernetzter Systeme -

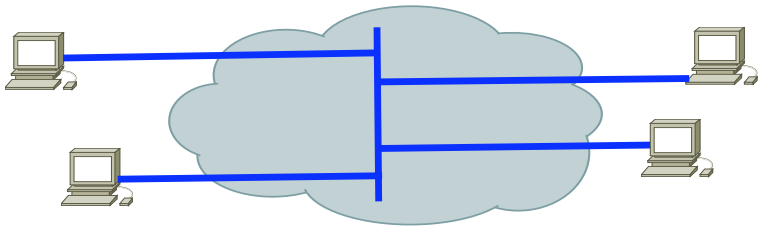
Kapitel 9: Netzsicherheit - Schicht 2: Data Link Layer

Inhalt

- Virtualisierungstechniken
- Point-to-Point Protocol (PPP)
- 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 „Privaten Netztes“) in beliebigen Topologien/ Technologien



- Virtualisierung auf jeder Schicht des OSI-Modells möglich

Virtual Network auf Schicht 1

- Optical Private Link oder Optical Private Network (OPN)
  - Provider betreibt Glasfaserinfrastruktur
  - Kunde erhält eine Wellenlänge (Farbe) in dieser Infrastruktur
  - Kunde kann dies nutzen wie einen Schicht 1 Link

Virtual Network auf Schicht 2/3/4

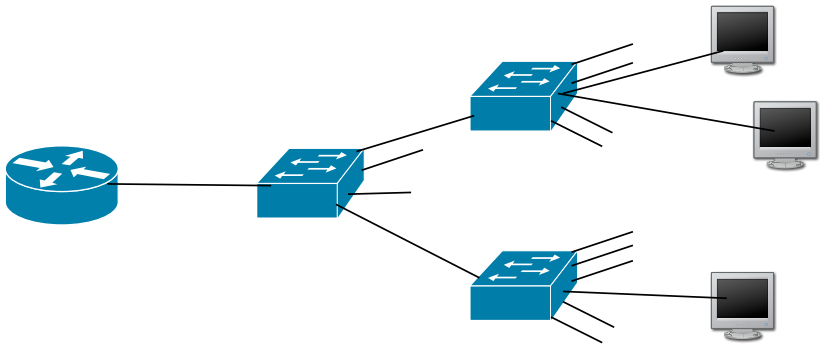
- Schicht 2:
  - Virtual Private Wire (VPWS) und Private Line Services (VPLS)
    - Provider bietet Punkt zu Punkt Verbindung (VPWS)
    - Punkt zu Multipunkt Verbindungen (VPLS)
    - Kunde kann dies nutzen wie einen Schicht 2 Link
  - Virtual LAN (VLAN)
  - Point-to-Point Verbindungen
  - Layer2 Tunneling Protocol
  - ....
- Schicht 3/4:
  - IPSec
  - SSL / TLS
  - OpenVPN
  - ...

Aufgaben der Schicht 2

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

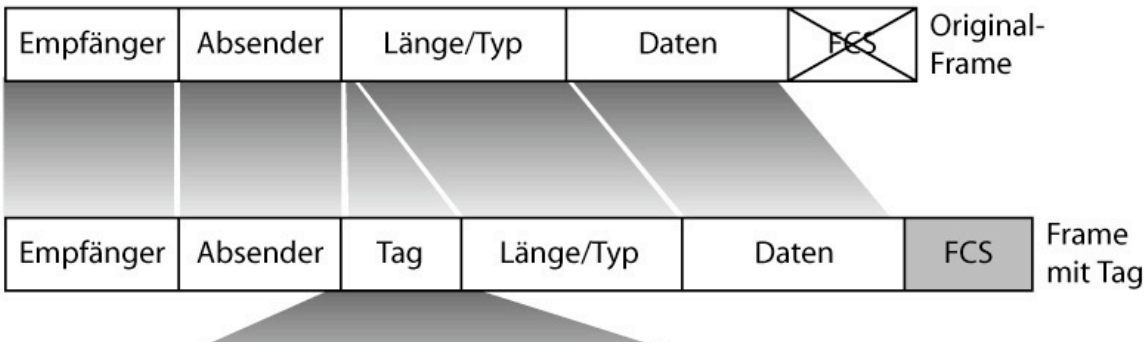
Virtual Private LAN (VLAN)

- LAN Infrastruktur über mehrere Switches (Gebäude) hinweg
- Verschiedene LANs auf einer Netzkomponenten
- Verkehrsseparierung

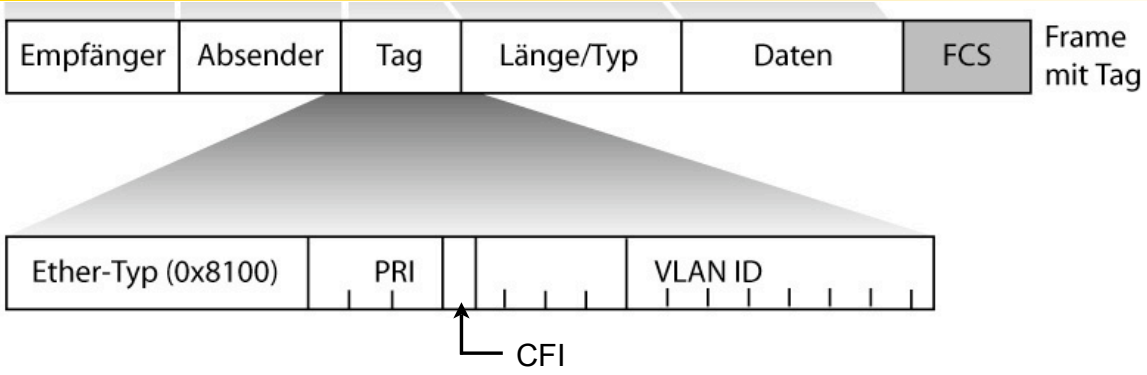


VLAN

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



VLAN: Tag Format



- Erweiterung des Ethernet-Frame:
  - TPID (Tag Protocol Identifier): 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)

PPP: Grundlagen

- Punkt-zu-Punkt Protokoll; Entwickelt für Verbindungsaufbau über Wählleitungen
  - DSL, ISDN, Modem, Mobilfunk, Funk, serielle Leitungen,....
  - WAN-Verbindungen zwischen Routern
  - Angelehnt an HDLC (High-Level Link Control); Schicht 2 Prot.
- Spezifiziert in RFC 1661, 1662 und 2153
  - Frame Format mit Begrenzungssymbolen (Delimiter) und Prüfsumme
  - Link Control Protocol (LCP) für:
    - Verbindungsauf- und -abbau
    - Test
    - Aushandlung der Konfiguration
  - Network Control Protocol (NCP) :
    - Aushandlung 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

- Authentisierung optional
- Im Rahmen der LCP Aushandlung der Konfiguration kann jeder Partner Authentifizierung fordern
- Definierte Authentisierungsprotokolle:
  - Password Authentication Protocoll (PAP)
  - Challange-Handshake Authentication Protocol (CHAP)
  - Extensible Authentication Protocol (EAP)

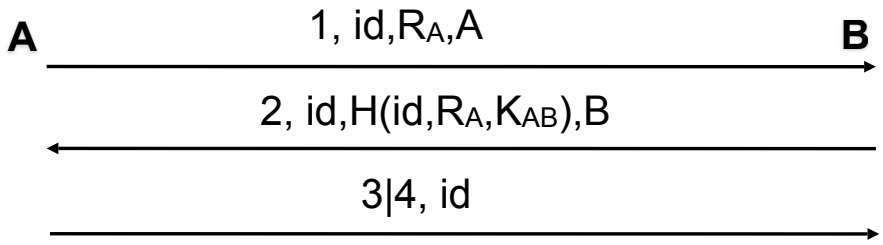
Password Authentication Protocol (PAP)

- 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

Challenge-Handshake Authentication Protocol: CHAP

- 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 zur Identifikation des Challange/Response Prot. (jedesmal wechseln)
  - H Hash Verfahren, im Standard MD5
  - 3 = success; 4 = failure
- Auth-Request kann später beliebig neu geschickt werden

Extensible Authentication Protocol (EAP)

- RFC3748 und RFC5247
- Authentisierungs-Framework, bietet gemeinsame Funktionen und Aushandlungsmechanismen für konkretes Verfahren (Method)
- 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) Lightwight 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
  - Nutzbar für verschiedenste Autentisierungs-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)

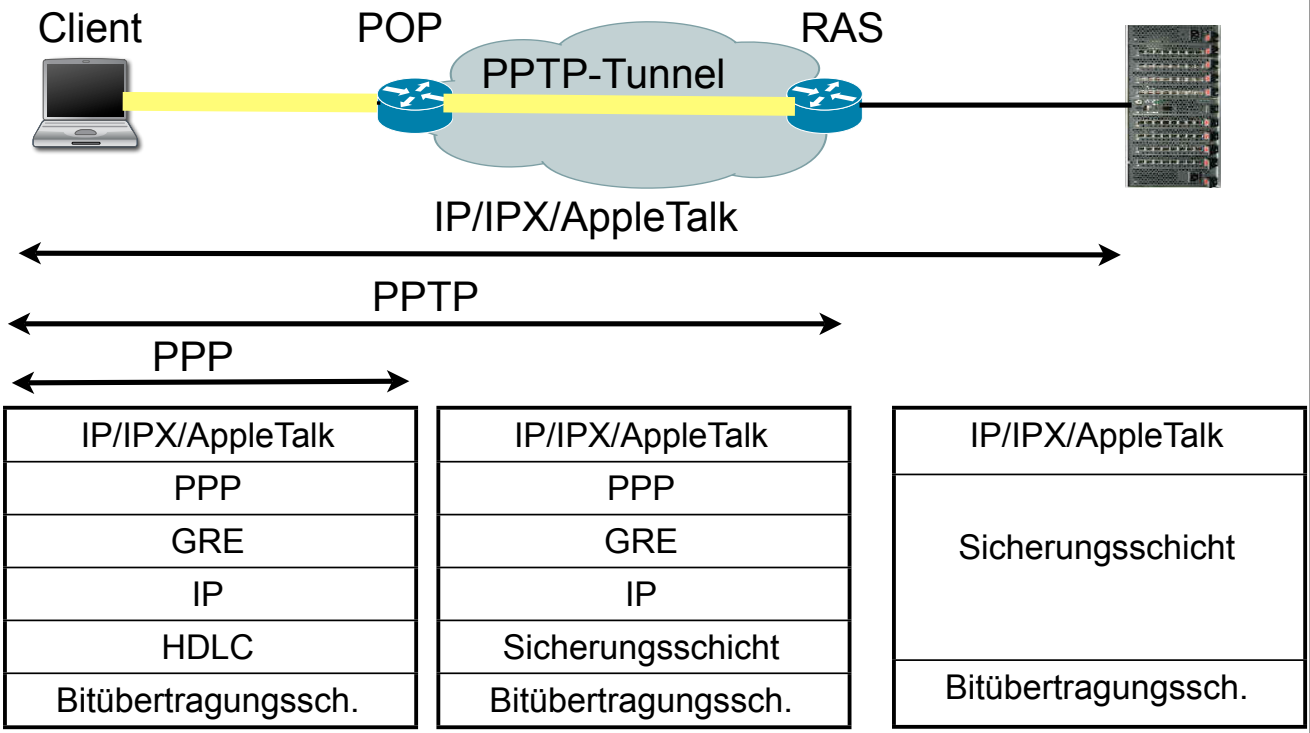
- PPP wurde für „direkt“ verbundene Systeme entwickelt
- Idee von PPTP:
  - Ausdehnung von PPP über Internet
  - PPTP realisiert Tunnel durch Internet
  - Transport von PPP PDUs in IP Paketen
  - Dazu werden PPP PDUs mit Generic Router Encapsulation Protocol (GRE) gekapselt
  - GRE ist ein Schicht 4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

PPP Protocol Data Unit (PPP PDU)
GRE
IP
Sicherungsschicht
Bitübertragungsschicht (Physical Layer)

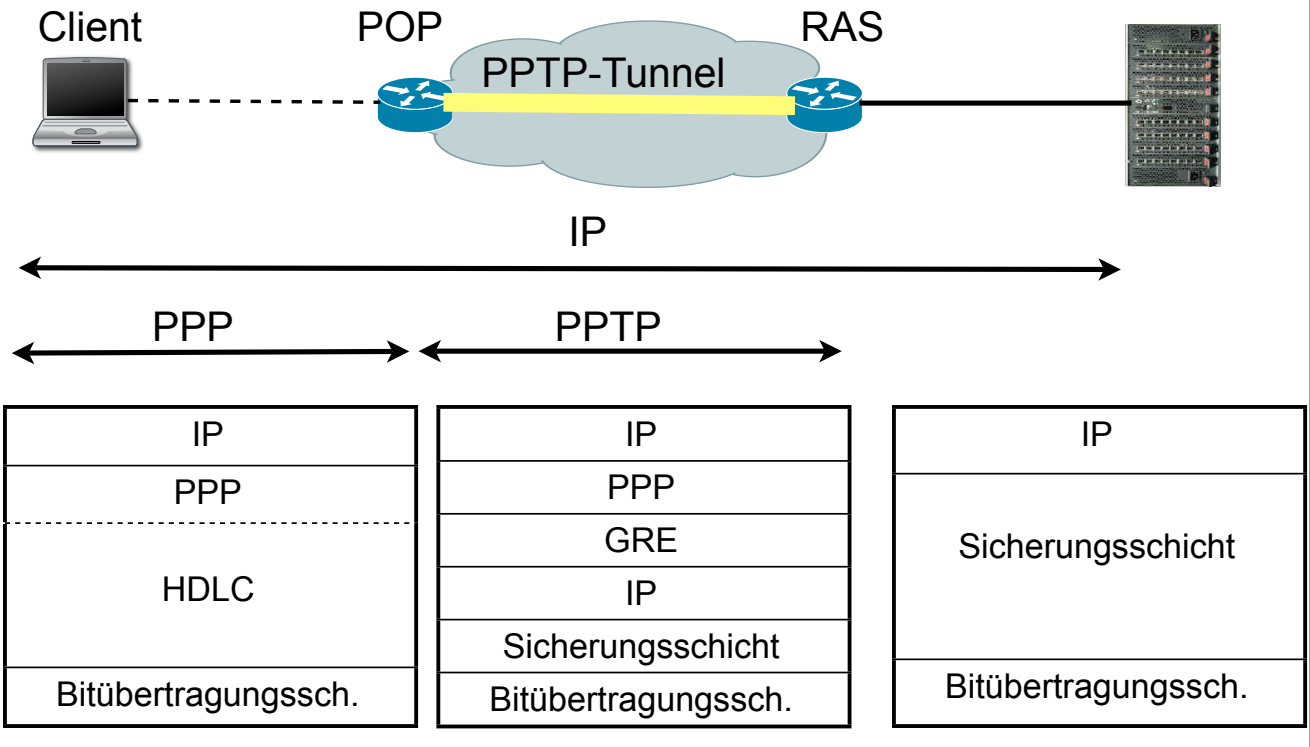
PPTP: Anwendungsfälle

- 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 Client

PPTP: Voluntary Tunneling



PPTP: Compulsory Tunneling

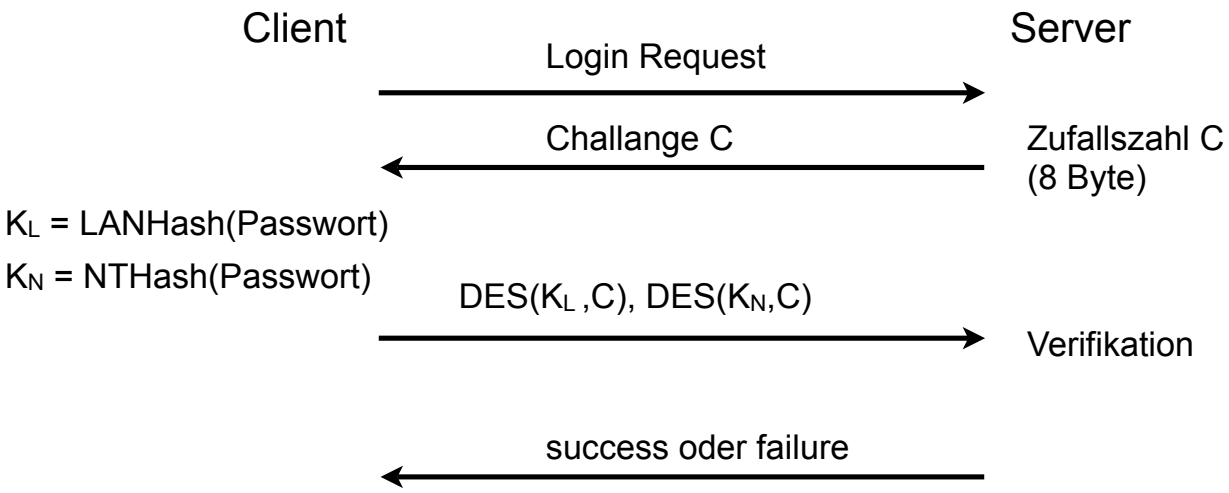


PPTP Sicherheit

- Von Microsoft entwickelt [RFC 2637]
- Teil des Remote Access Service (RAS)
- Microsoft proprietäre 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 (Stichwort: LAN Manager Passwort und L0ptCrack)
  - Challenge/Respose Protokol erlaubt Maskerade Angriff auf RAS Server (keine zweiseitige Authentisierung)
  - Verschlüsselung: Implementierungsfehler erlaubt Dekodierung
  - Verschlüsselung: geratenes Passwort erlaubt Entschlüsselung
  - Kontrollkanal: Unautorisierte Nachrichten erlauben DoS (Crash des Servers)
- Microsoft bessert nach PPTP v2 und MS-CHAPv2 [RFC 2759]

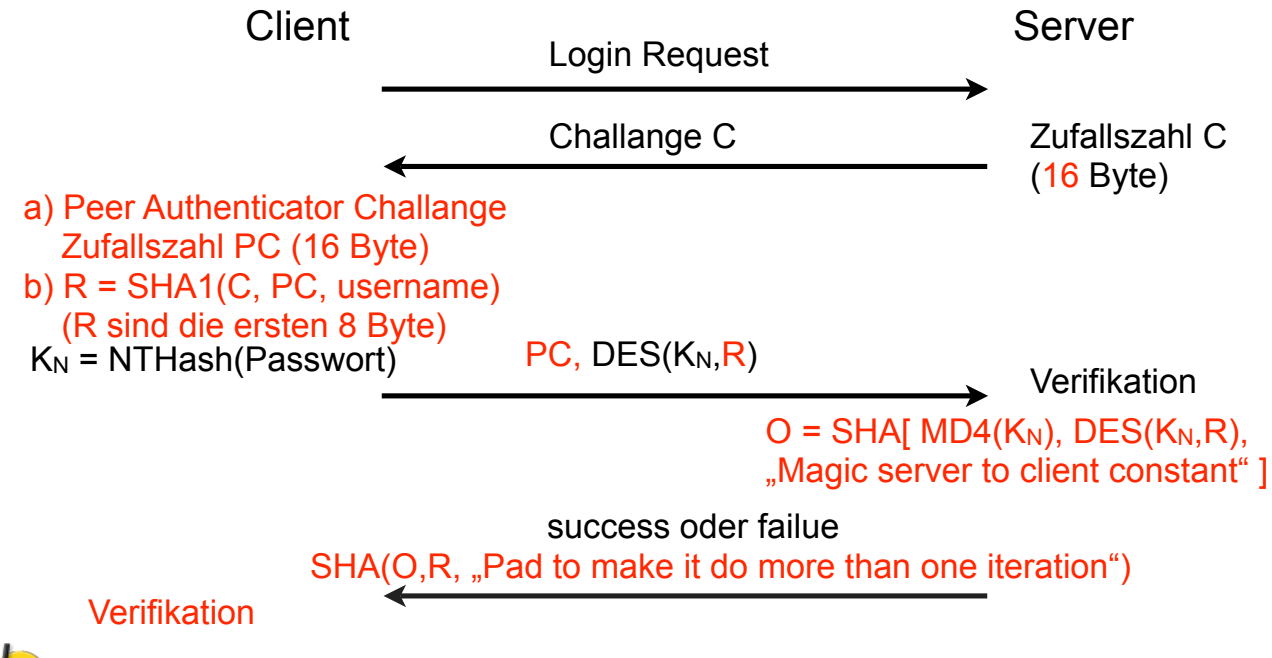
Vergleich MS-CHAP v1 und v2

- Im folgenden Version 1



Vergleich MS-CHAP v1 und v2

- Änderungen in der Version 2



Sicherheit MS-CHAP v2

- Protokoll komplizierter als nötig
- Nutzen von Peer Authenticator Challenge PC nicht klar
- Version Rollback Attack möglich:
  Mallet „überzeugt“ Client und Server MS-CHAP v1 zu verwenden

Layer 2 Tunneling Protocol (L2TP)

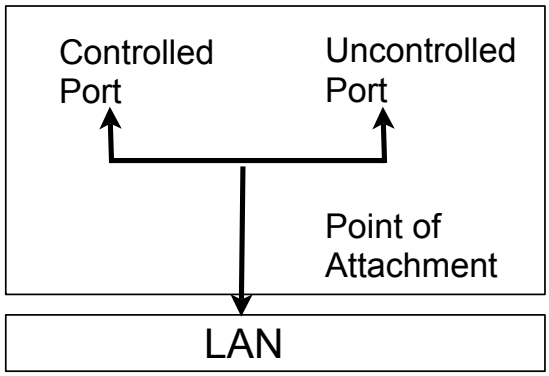
- L2TP [RFC 2661] entwickelt für Tunneling von PPP Paketen
- Unterstützt verschiedene unterliegende Protokolle:
  UDP, ATM, FrameRelay
- Tunnel-ID erlaubt Multiplexing von Verbindungen/Tunneln
- Authentisierung mittels CHAP oder PAP
- Vertraulichkeit über IPSec möglich [RFC 3193]
  (IPSec später in der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

IEEE 802.1X

- Institute of Electrical and Electronics Engineers (IEEE)
- 802 Standards für Local Area Networks (LAN), insebsondere 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
  - meist genutzt in WLAN und (V)LAN
  - Port basierte Network Access Control

802.1X Grundlagen

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

- Möglicher Ablauf:
  1. Supplicant fordert Controlled Port
  2. Authenticator fordert Authentisierung
  3. Nach erfolgreicher Authentisierung wird 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 nur Vermittler der Nachrichten