

Workshop

---

# Computernetzwerke & Sicherheit

**Achim Friedland**  
<achim.friedland@stud.tu-ilmenau.de>

**Veranstalter:**  
**Technische Universitaet Ilmenau**  
**Fakultät für praktische Informatik und Medieninformatik**  
**Fachgebiet Telematik, Prof. Dr.-Ing. habil. Dietrich Reschke**

**in Zusammenarbeit mit dem URZ Ilmenau**  
**Dipl.-Ing. Joachim Ritschel**

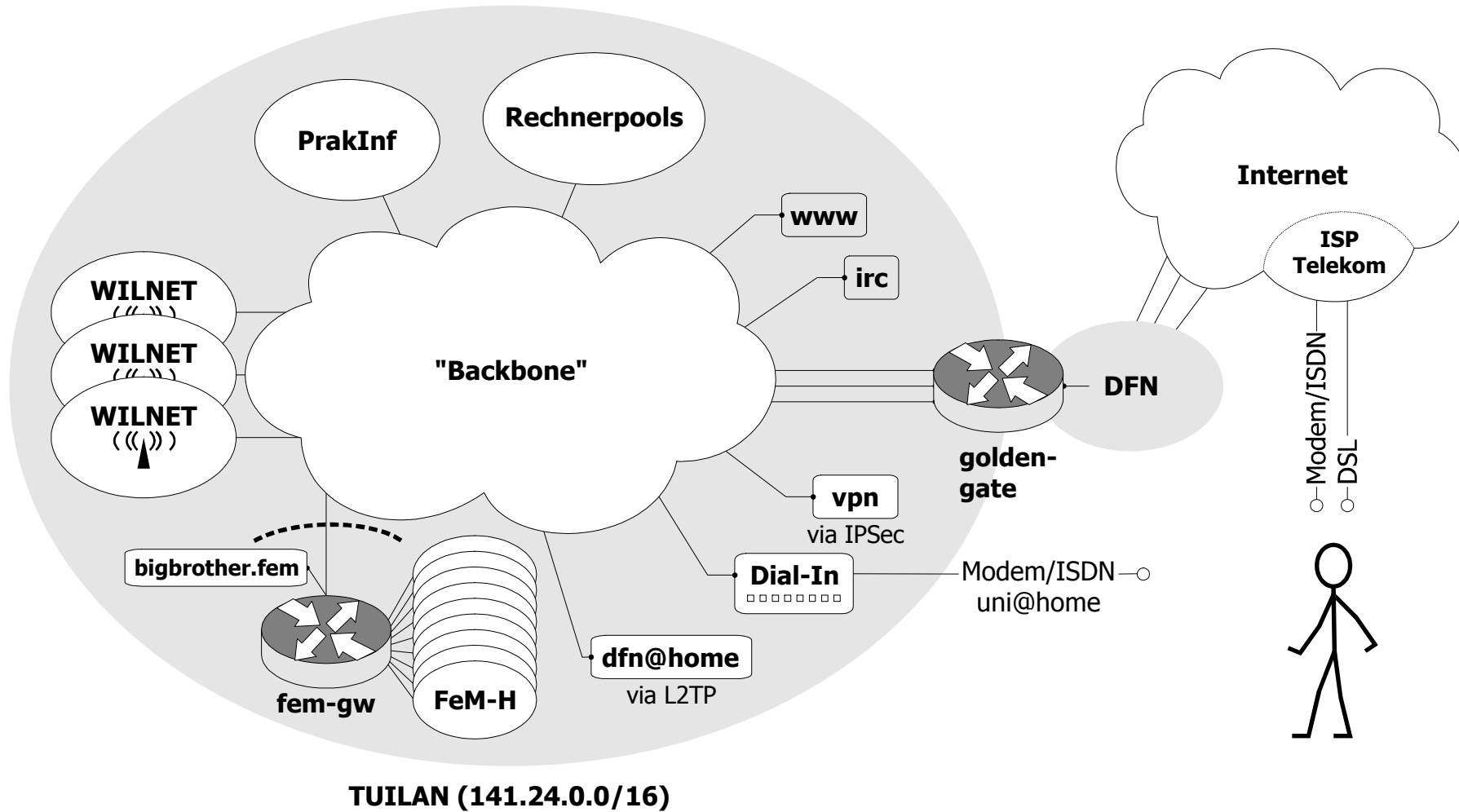
---

# Inhalt

---

- 1. Die Struktur des TUILANs**
- 2. IP-Protokoll und Schicht 4-Protokolle**
- 3. TUILAN intern: Ethernet**
- 4. TUILAN extern: Modem, ISDN, GSM/GPRS und DSL**
- 5. TUILAN mobil: WILNET, IPSec**

# 1. Struktur des TUILANs



# 1. Struktur des TUILANs

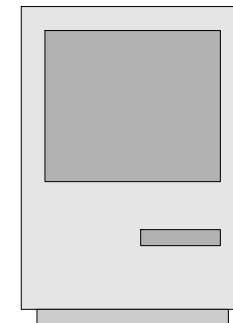
---

- Jeder Rechner im TUILAN ist weltweit durch eine eindeutige IP-Adresse aus dem Netz 141.24.0.0/24 zu erreichen
- Es werden keine Anwendungen bzw. Ports gesperrt
- Die Sicherheit des eigenen Rechners ist Aufgabe jedes einzelnen !

-> Ist das vertretbar?

lorrian.rz.tu-ilmenau.de  
141.24.190.38

Port 22 / SSH

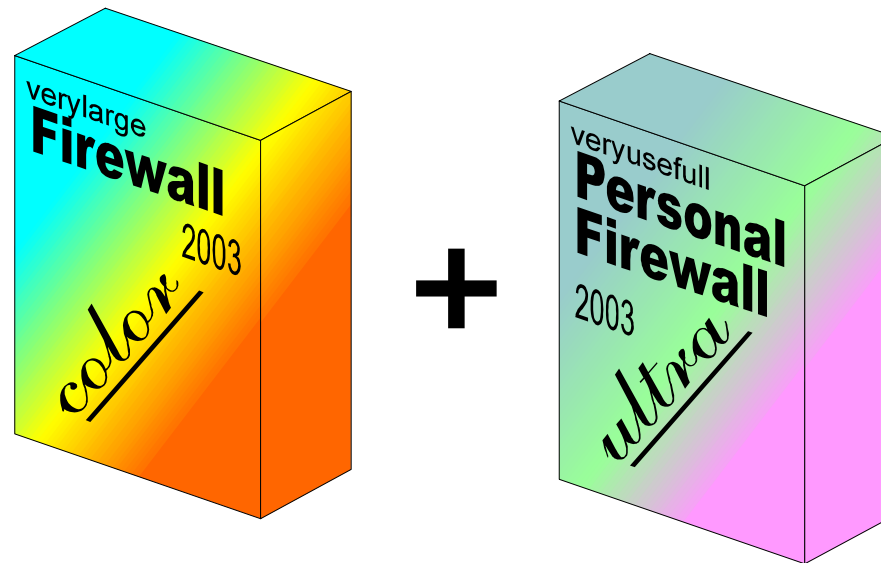


Socket

# 1. Struktur des TUILANs

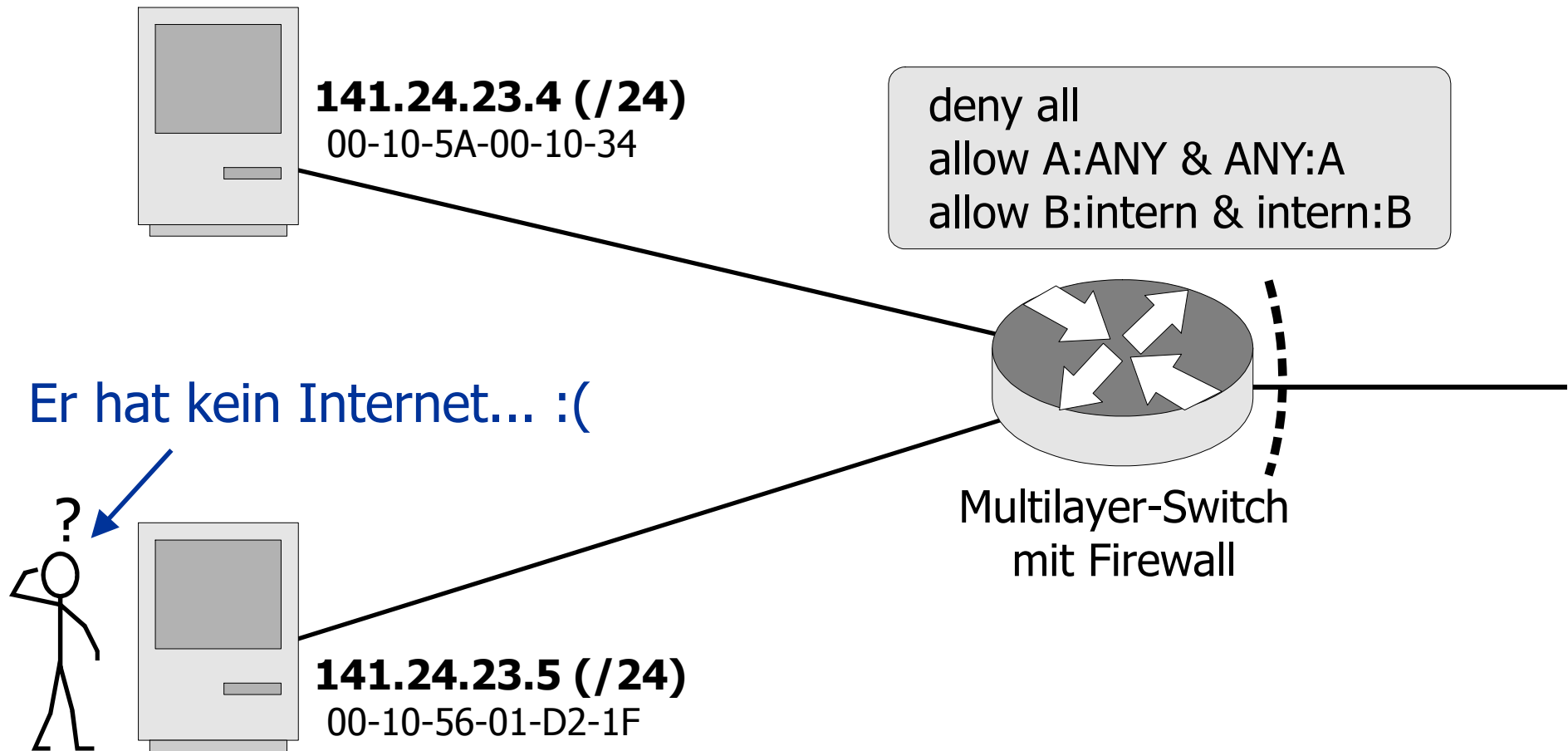
---

**Kaufen wir also:**

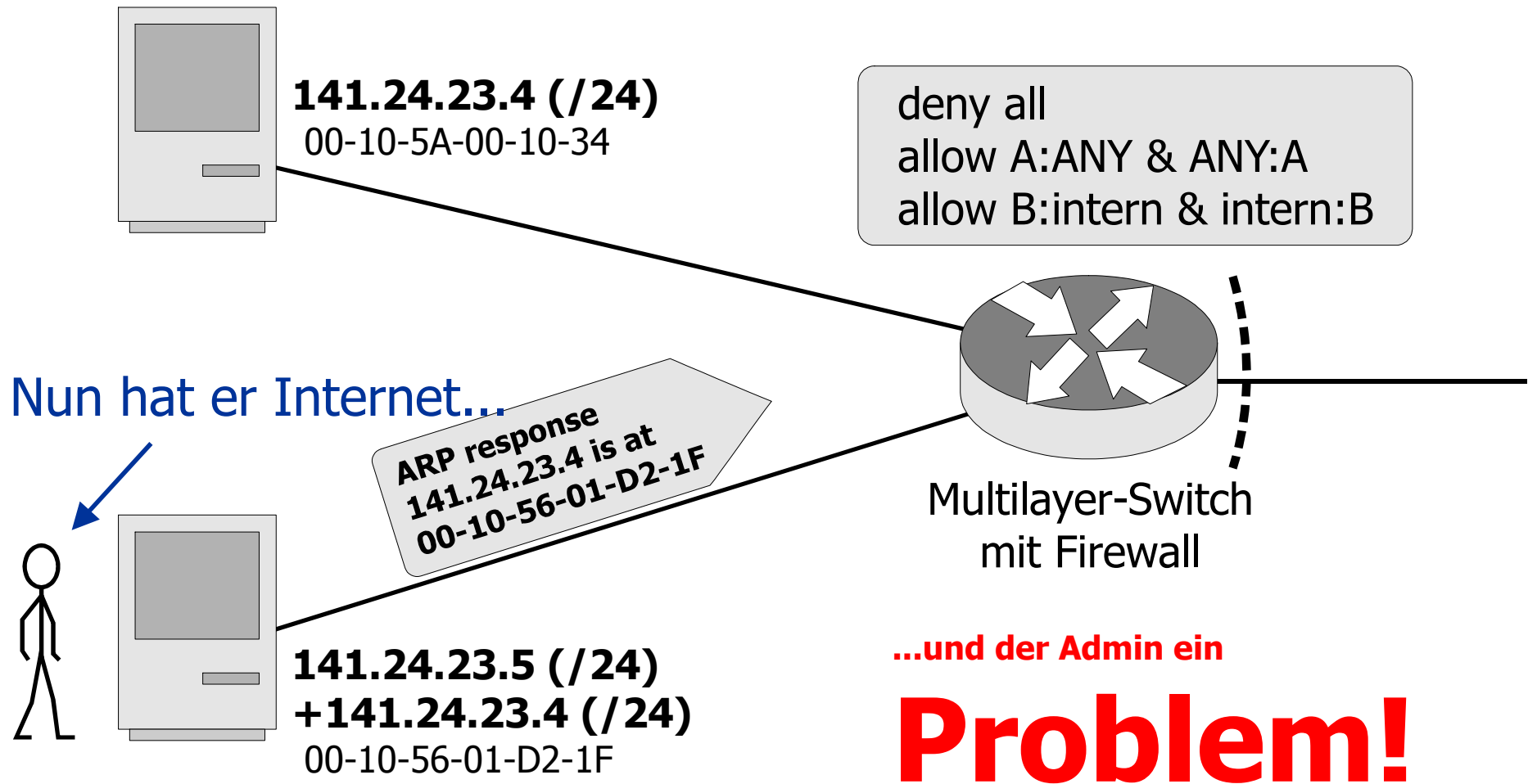


**...und alles wird gut?**

# 1. Struktur des TUILANs



# 1. Struktur des TUILANs



# 1. Struktur des TUILANs

---

Sicherheit ist **kein Produkt...**

Sicherheit ist **ein Konzept !**

- **Firewallsysteme stellen ein Grundgerüst da, aber sind nur ein kleiner Teil eines Konzeptes**
- **Sie arbeiten hauptsächlich auf Schicht 3-4 des ISO/OSI-Modells**
- **Sowohl die Schichten darunter als auch die darüber werden meist vergessen**
- **Vorallem die Schichten 1, 2 und ihre Zusammenarbeit mit der Netzwerkschicht (3), sollen genauer betrachtet werden.**

# 1. Struktur des TUILANs

---

- **Security-Policy: Was soll überhaupt geschützt werden**
- **Meist Unterscheidung in: trusted host, unknown, untrusted**
- **Häufige Angriffsmuster:**
  - + **Paket-Sniffer**
  - + **Replay-Attack**
  - + **Man-in-the-Middle**
  - + **Adress-Spoofing**
  - + **Denial-of-Service (DOS, DDOS)**
  - + **Application Layer-Attack**

## 2. Das IPv4-Protokoll

---

### IPv4-Adressen / IP-Routing

141.24.44.23:53

└──────────┬──────────┘ └──────────┬──────────┘  
Netzanteil Hostanteil

→ golden-gate

└──────────┬──────────┘ └──────────┘  
Netzanteil Hostanteil

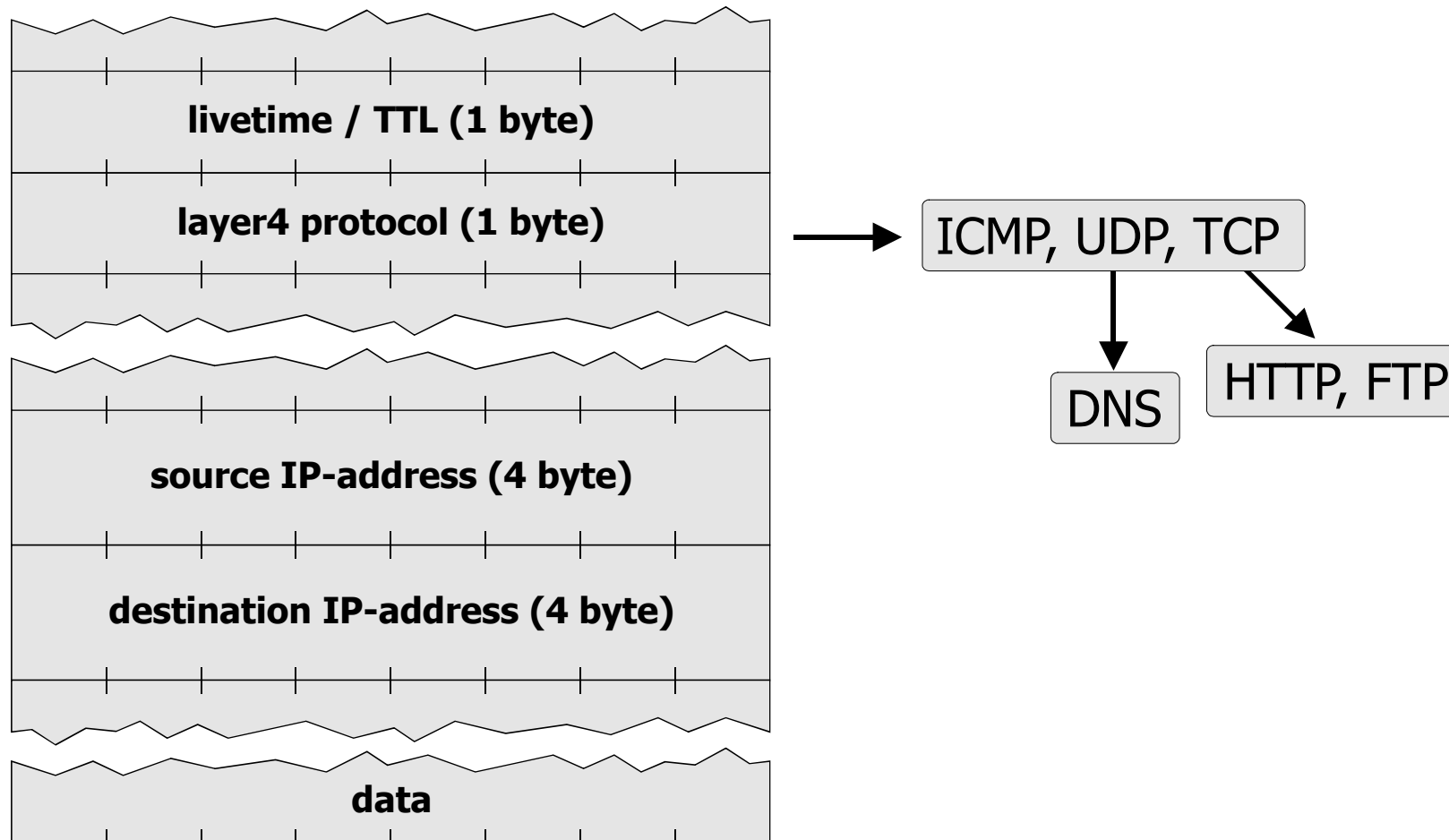
→ fem-gw

└──────────┬──────────┘  
Hostanteil

→ RechnerXYZ

## 2.1 Das IPv4-Protokoll

### IPv4-Header (rfc 791)



## 2.2 Schicht 4-Protokolle

---

141.24.44.23:53

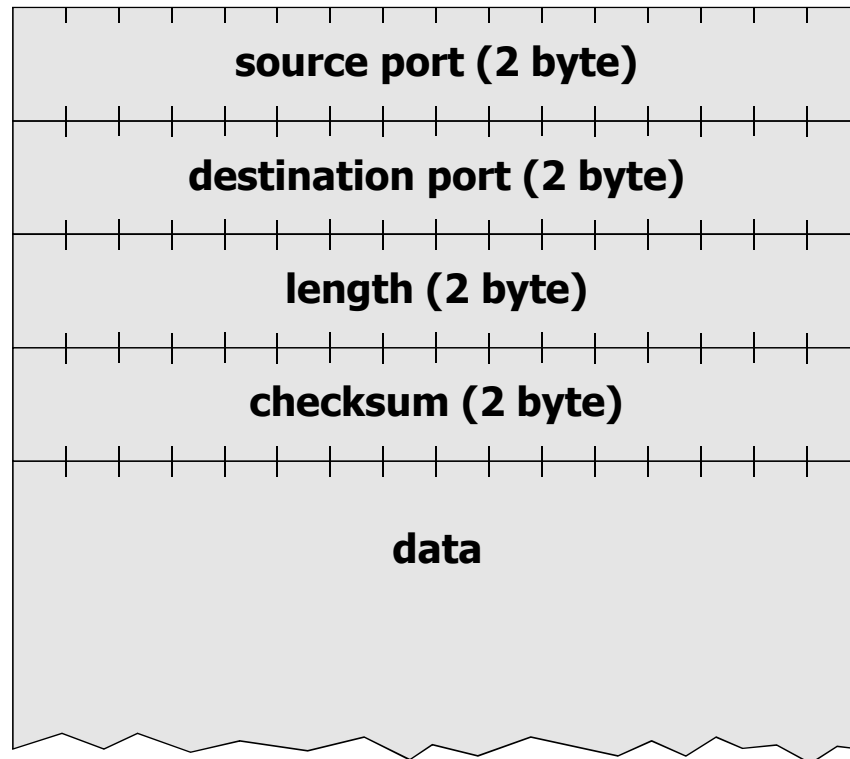
Hostanteil

Port

→ Programm  
XYZ

## 2.2 Schicht 4-Protokolle

### z.B. UDP-Paketformat



**UDP für ungesicherte Datagramme  
(rfc 768)**

**TCP für alles wo es auf Reihenfolge,  
verlorene, doppelte Pakete und eine  
automatische Anpassung der Daten-  
rate ankommt. (rfc 793)**

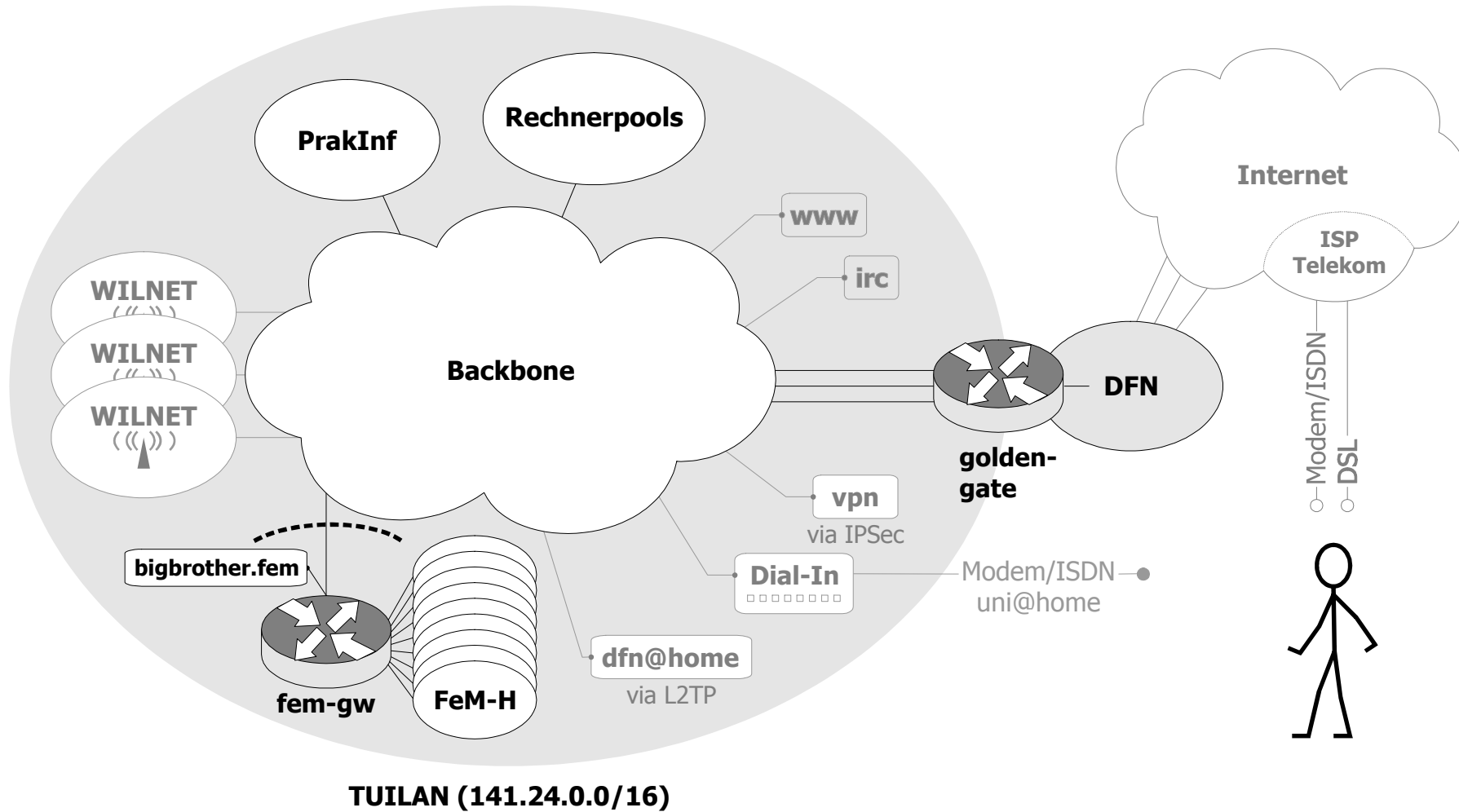
**ICMP als Steuer-/Regelprotokoll  
für das "darunterliegende" IP.  
(rfc 792)**

## 2.3 Schicht 1 und 2 Protokolle

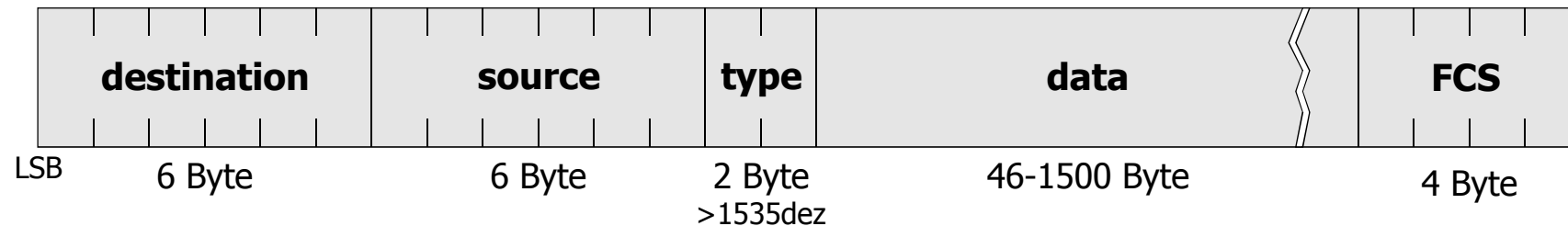
---

- **IP ist ein rein logisches Netzwerkprotokoll**
- **Daher und aus Effizienzgründen werden IP-Pakete nicht direkt über ein Medium versendet, sondern es wird noch ein weiteres Protokoll dazwischengelegt.**
- **z.B. Transmission of IP Datagrams over Ethernet Networks (rfc 894)**
- **Damit dies alles reibungslos zusammenarbeitet braucht man (meist) noch ein Protokoll welches die physikalischen Adressen mit denen der Netzwerkschicht verbindet... ARP...**

# 3. TUILAN intern: Ethernet



## 3.1 Ethernet Frame (nach Xerox (Intel, Digital))



- Jeder "Netzwerk Port" hat seine eigene MAC-Adresse
- MAC-Adressen sind 6 Byte lang, werden vom Hersteller festgelegt und sind weltweit einmalig
- Sie sind aber softwaremässig änderbar und deshalb nicht wirklich zum Authentifizieren geeignet
- Multicastadressen werden durch das erste Bit markiert

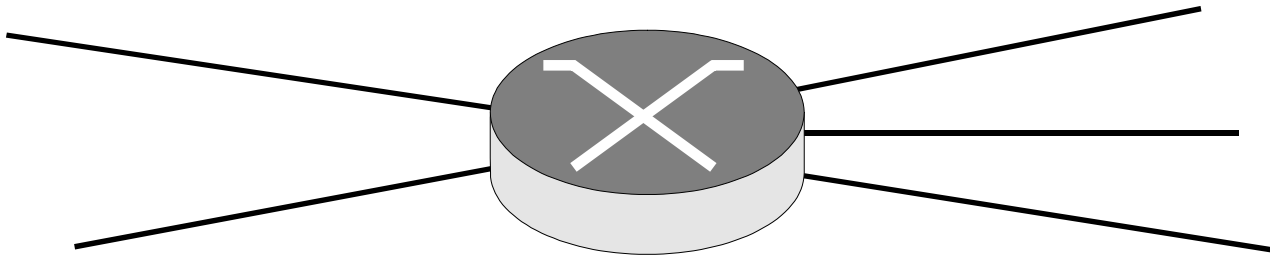
## **3.2 Address Resolution Protocol (ARP) (z.B. rfc 826)**

---

- **Löst Schicht-3-Adressen (z.B. IP) zu Schicht-2-Adressen (z.B. Ethernet) und umgekehrt auf**
- **Verbindungsloser Transport in Schicht 2-Rahmen**
- **ARP Request (who-has) via Broadcast an alle**
- **ARP Response (is-at) via Unicast**
- **Es wird nur der Inhalt des ARP-Paketes ausgewertet**
- **Antworten werden lokal für ca. 60 Sek. gecached**
- **Manuelle Einträge in den ARP-Cache sind möglich**
- **Reverse ARP (RARP) zur automatischen Vergabe von Schicht-3-Adressen (besser: BOOTP, DHCP)**
- **ARP als Mittel zur Trafficanalyse ("Wer mit Wem")**

## 3.3 Ethernet Switches (transparent bridging IEEE 802.1)

---



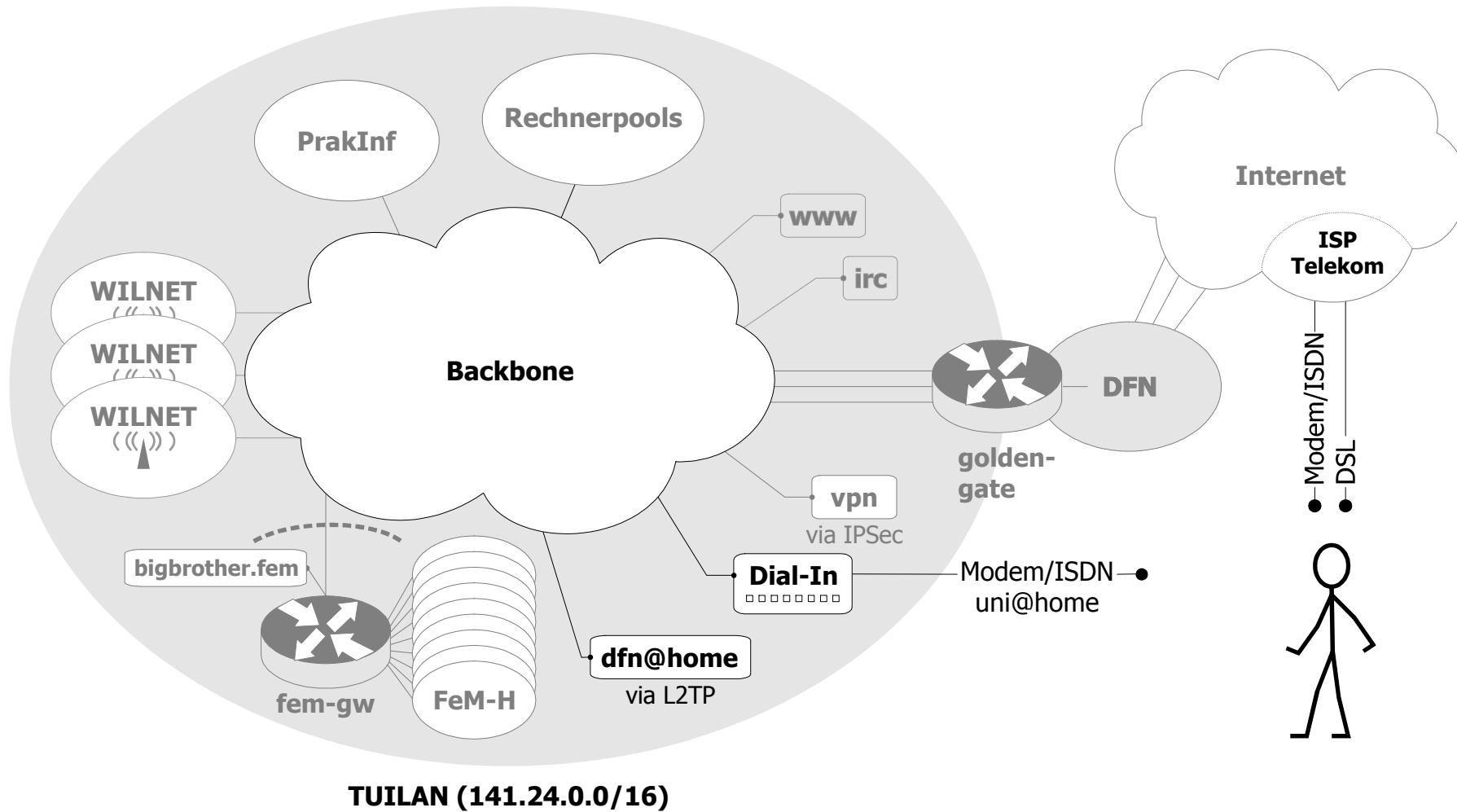
- **Dienen zum sternförmigen Zusammenschluss von Rechnern zu Netzwerken**
- **Arbeiten auf Schicht 2 (vgl. Hub -> Schicht 1)**
- **"Lernen" die MAC-Adressen der angeschlossenen Rechner an einem Port und stellen dadurch die Ethernetpakete gezielt zu**
- **Um fremde Daten mitzulesen, kann der Lernprozess allerdings recht einfach überlistet werden**
- **Bieten Netzwerkmanagement und QoS-Möglichkeiten**

## 3.4 TUILAN intern

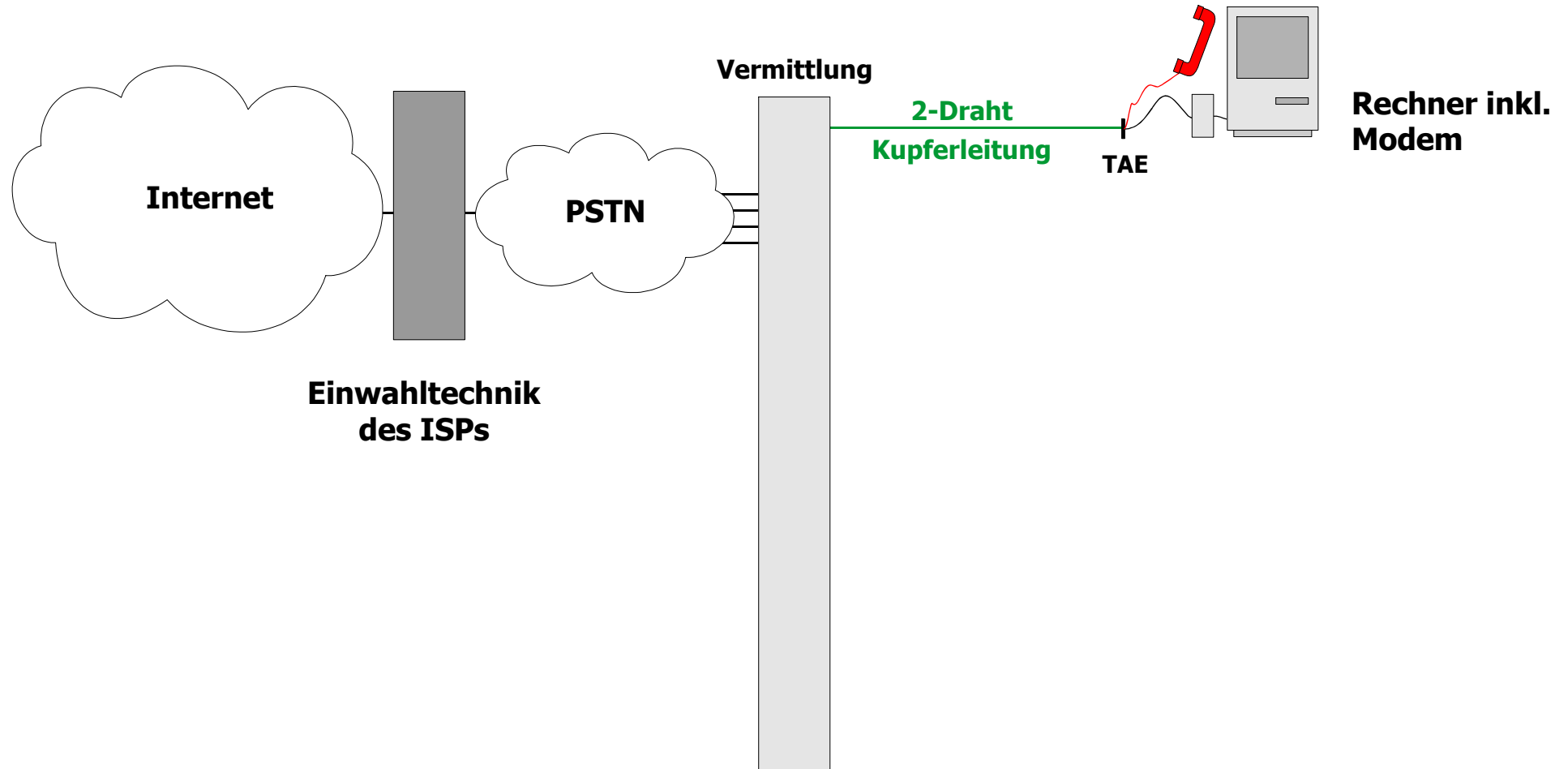
---

- **Firewallsysteme können viele Angriffe aus dem Internet schon am Eingangsrouter filtern**
- **Firewallsysteme bieten auch die Möglichkeit der Rechervergabe beim Zugriff auf das Internet**
- **Aber eine Firewall bietet nicht den Schutz der versprochen wird**
- **Angriffe auf Schichten die durch eine Firewall nicht geschützt werden können ihren Schutz komplett umgehen**
- **Ohne umfassende Security-Policy kann man sich die Firewall auch sparen**

## 4. TUILAN extern: Modem, ISDN, GSM/GPRS und DSL



## 4.1 TUILAN extern: Modem

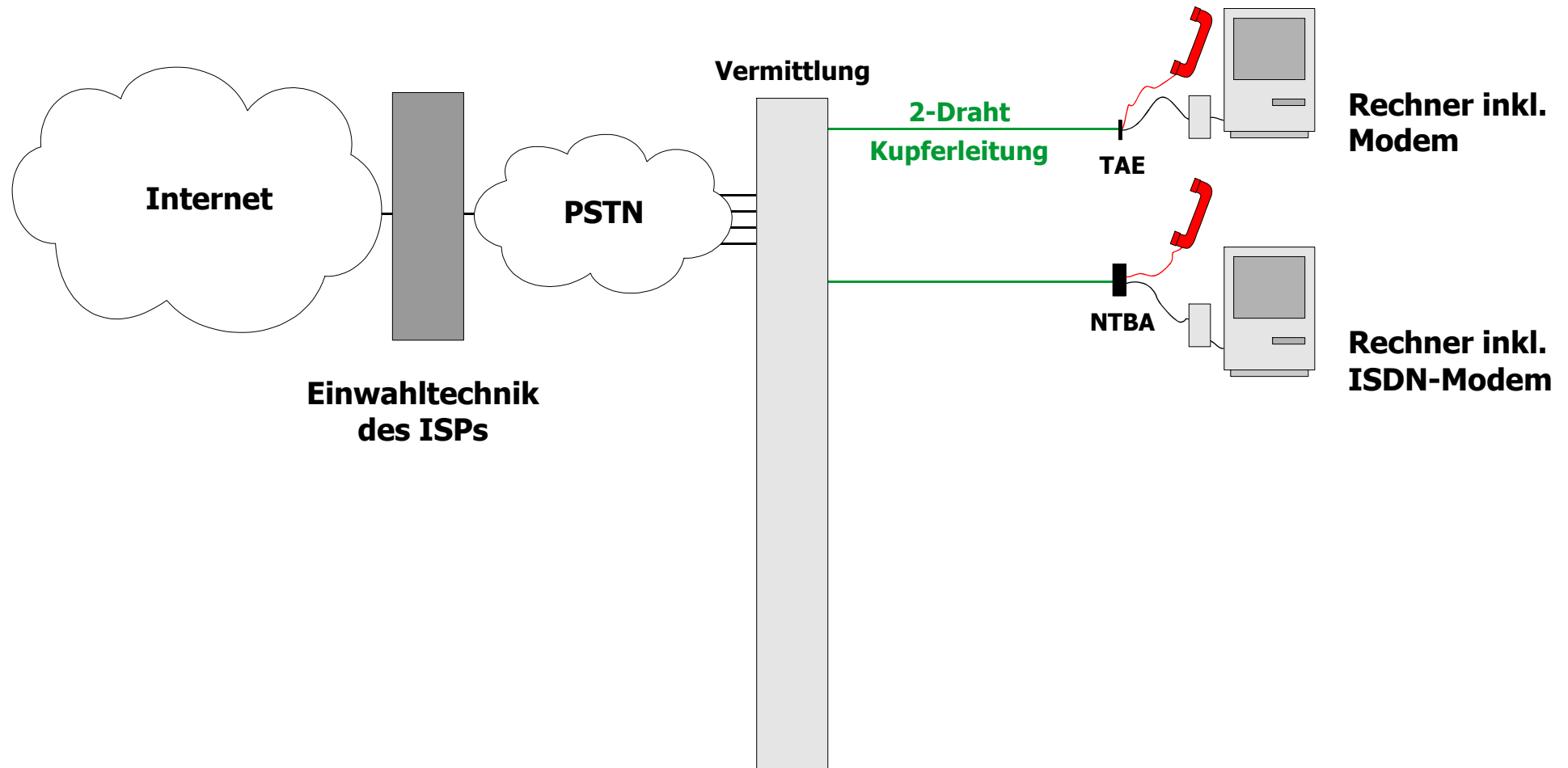


## 4.1 Datensicherheit & Modems

---

- **Daten via Telefonsystem, Bits -> "Tönen"**
- **Belauschen von Telefonleitungen ist reine "Fingerübung"**
- **Demodulation fremder Daten einigermaßen trivial**
- **Weder Verschlüsselung des "Gesprächs" noch der Daten**
- **Authentifizierung nur auf Nutzerebene**

## 4.2 TUILAN extern: ISDN



## 4.2.1 Datensicherheit im ISDN

---

- **Am ISDN Bus (S0) kommen sämtliche Daten bei allen Teilnehmern an**
- **Aber die wenigsten Karten unterstützen einen "promisc mode"**
- **Kommunikation ist nur zw. Teilnehmer und Vermittlungsstelle definiert. Dadurch ist ein Man-in-the-Middle Angriff kaum realisierbar.**
- **keine Verschlüsselung der Daten (aber TRON, CCC)**
- **Authentifizierung nur auf Nutzerebene, Rufnummernübermittlung ist KEINE Sicherheit**

## 4.2.2 ISDN als Personal Area Network

---

### **PRO:**

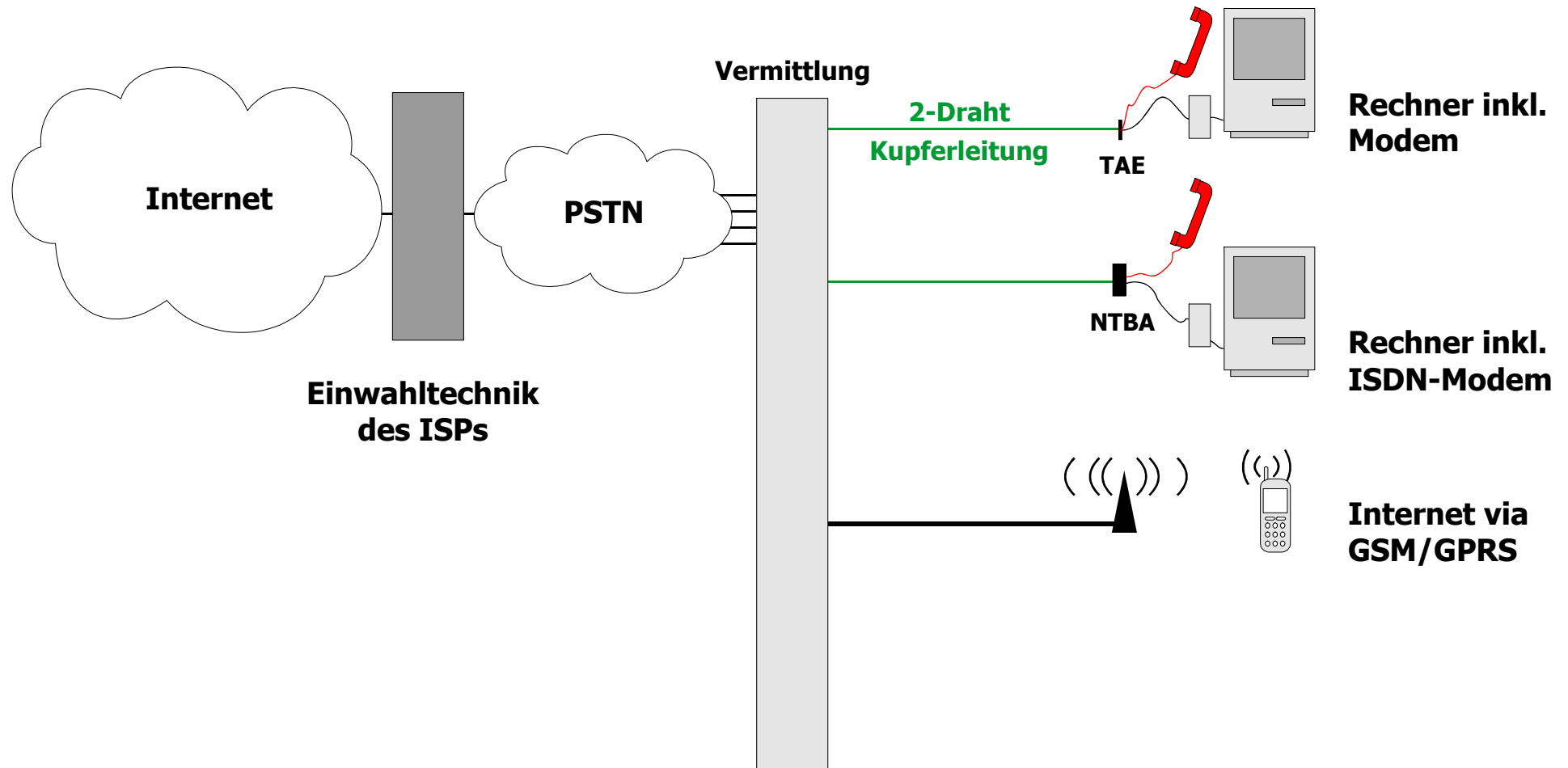
- **kollisionsfreie Bus Topologie**
- **billiges Kabel (cat.3)**
- **Vermittlung kann Hardwareadressen vergeben ("AutoConf")**
- **QoS Merkmale**

### **CONTRA:**

- **festgelegt auf 2x 64k Bit**
- **Kommunikation zw. Teilnehmern nur via Zusatzhardware**

**=> Heutzutage für PANs unbrauchbar...**

## 4.3 TUILAN extern: GSM/GPRS

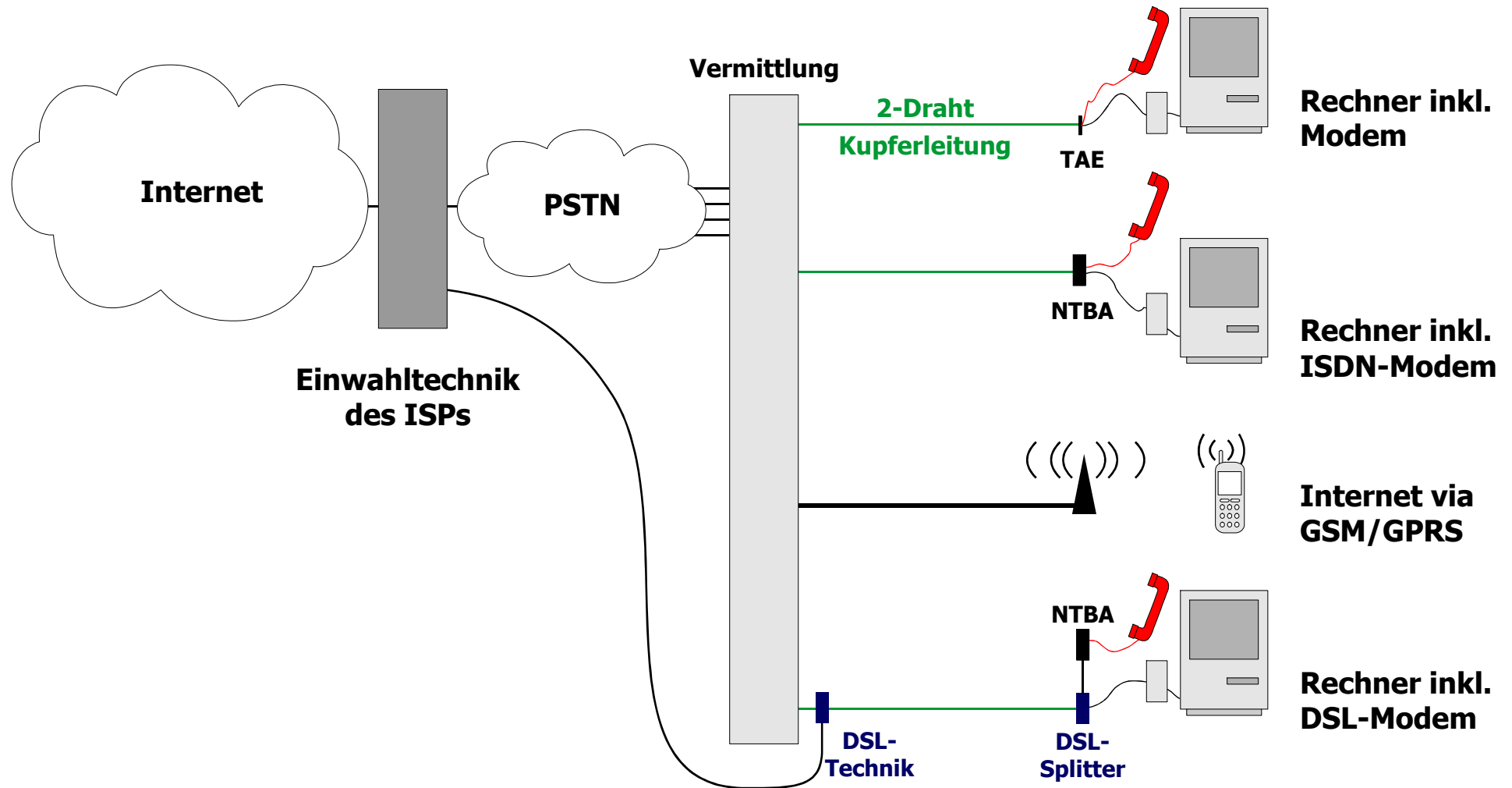


## 4.3.1 Datensicherheit mit GSM/GPRS

---

- **Die mobile Kommunikation zwischen Base Transceiver Station und Mobile Station ist verschlüsselt (A5), der Schlüssel aber schon länger gebrochen.**
- **Restliches Mobilnetz komplett unverschlüsselt**
- **Man-in-the-Middle nennt sich hier: IMSI-Catcher**
- **Egal ob Internet via Dial-In oder GPRS, die Daten sind defacto unverschlüsselt**

## 2.3 TUILAN extern: Digital Subscriber Line (DSL)

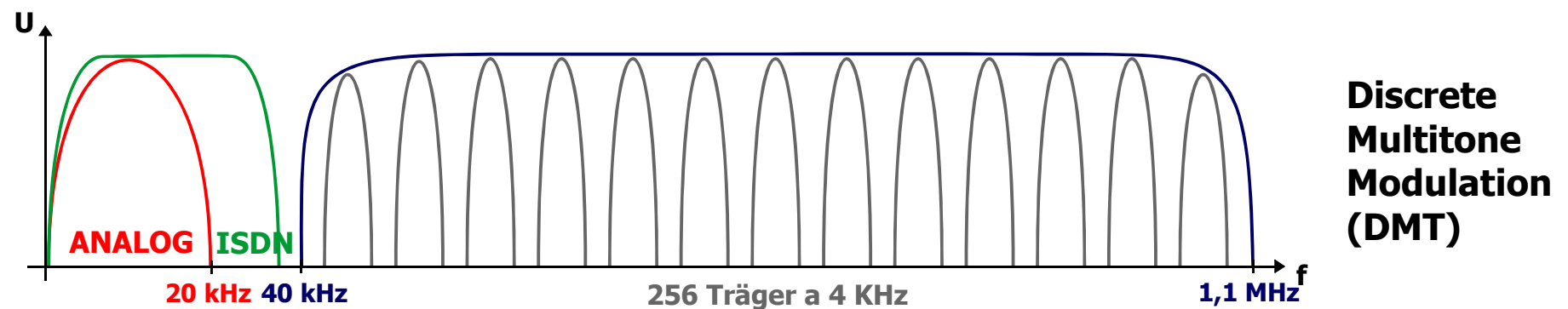
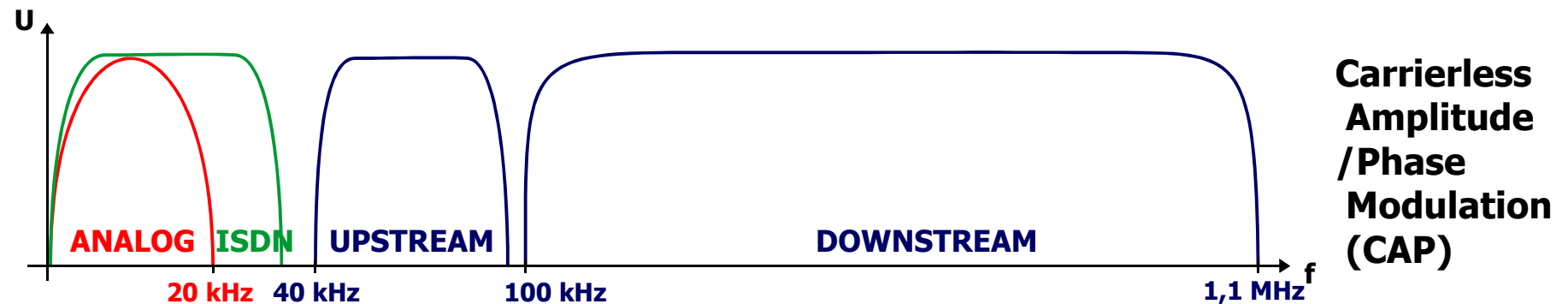


## 4.3.1 Datensicherheit mit DSL

---

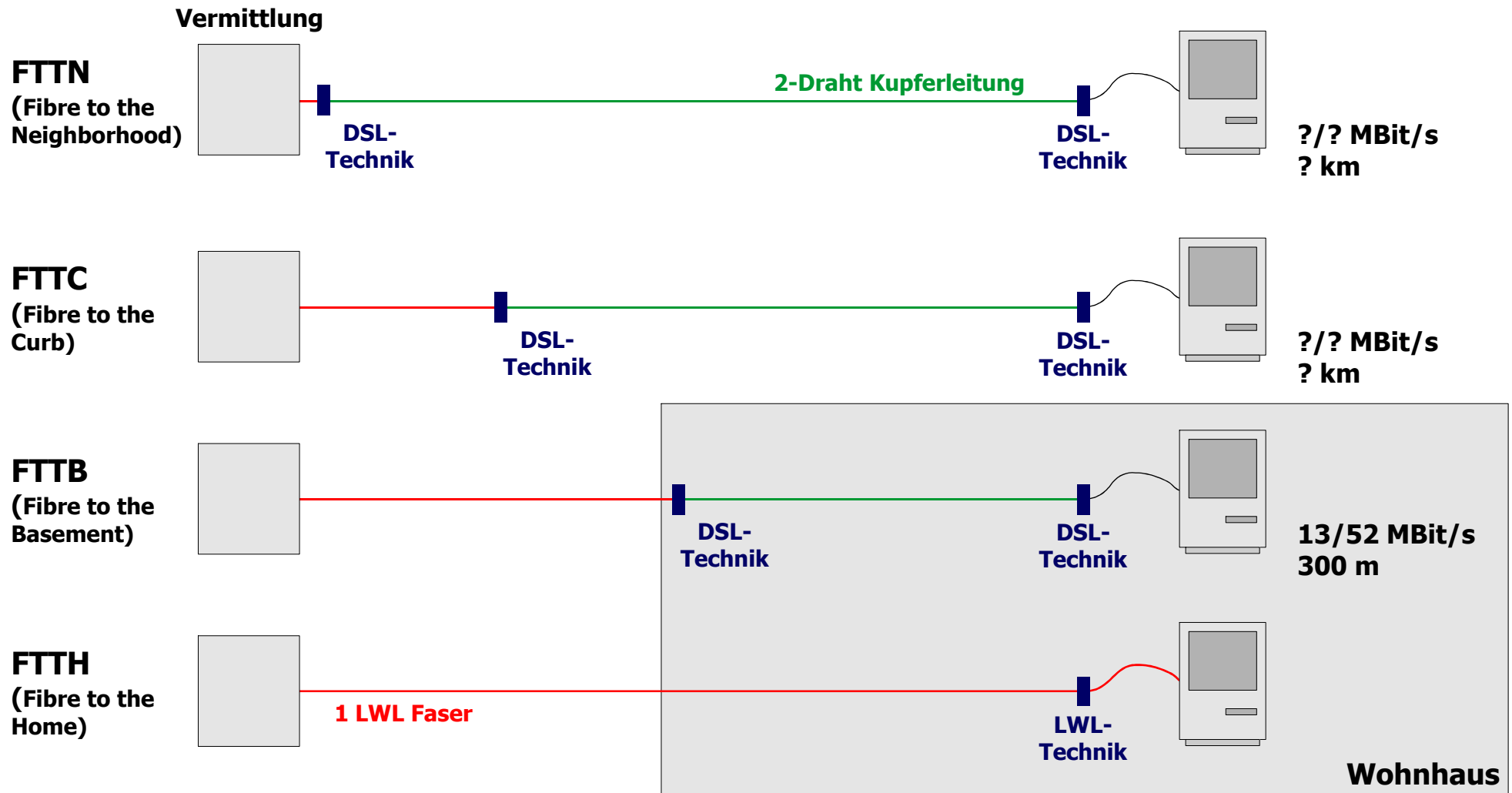
- **Verschiedene DSL Varianten für dezidierte Punkt-zu-Punkt Netzwerkverbindungen über 2-Draht Twisted-Pair (z.B. Telefonleitungen)**
- **Meist asymmetrisches Verhältnis von Up- zu Downstream**
- **64/384 kBit/s bis 13/52 MBit/s je nach Leitungsquerschnitt/-länge und anderen Störgrößen**

## 4.3.2 Frequenznutzung bei DSL



- Beide Verfahren jeweils mit und ohne Analog Telefon/ISDN im Band

## 4.3.3 "DSL über OPAL" (Optische Anschlußleitung)



## **4.4 Point-to-Point Protocol (PPP) (rfc 1547 und rfc 1661)**

---

**Das Point-to-Point Protocol (PPP) bietet ein standardisiertes Framework zum Transport von Schicht 3 Datagrammen über Punkt-zu-Punkt Verbindungen. Es beinhaltet...**

- Eine Methode zum Kapseln von Multi-Protokoll Datagrammen via HDLC**
- Ein Link Control Protocol (LCP) zum Aufbau, Konfiguration und Testen der Schicht 2 Verbindung**
- Eine Sammlung von Network Control Protocols (NCPs) zur Konfiguration und Transport verschiedener Protokolle der Netzwerkschicht (IP control protocol rfc 1332)**
- Defacto-Standard für Internet Dial-up Services (früher SLIP)**
- Multilink PPP/Kanalbündelung (rfc 1990)**

## 4.4.1 PPP Authentication Protocols (rfc 1334)

---

### 1. Password Authentication Protocol (PAP)

- Wiederholtes unverschlüsseltes Senden von Login+Passwort
- Playback Angriff

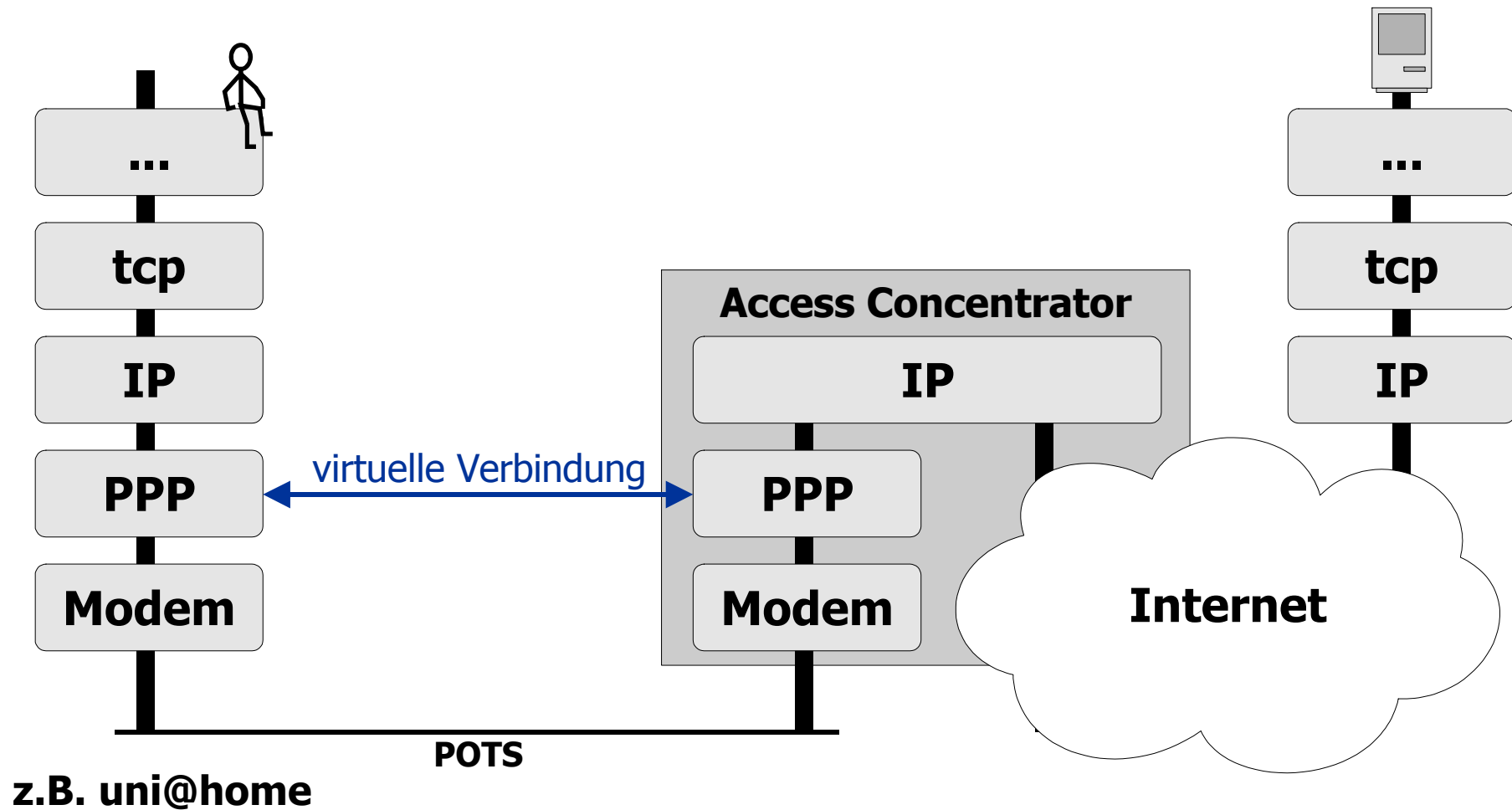
### 2. Challenge Handshake Authentication Protocol (CHAP) (rfc 1994)

- Der AC sendet eine "Challenge" die via "One-Way Hash" Funktion und shared-secret berechnet wird (MD5, SHA-1).
- Client sendet nur das Ergebnis. Stimmt es nicht mit der Berechnung der Gegenstelle überein, so wird die Verbindung abgebaut.

### 3. PPP Extensible Authentication Protocol (EAP) (rfc 2284)

- Beide Seiten können sich eine Methode aussuchen
- Authentifizierung kann auch verzögert und/oder ausgelagert werden (z.B. AAA, Radius-Server)

## 4.4.2 Point-to-Point Protocol (PPP) (rfc 1547 und rfc 1661)



## 4.5 Point-to-Point over Ethernet (PPPoE) (rfc 2516)

---

**Standardverfahren um PPP Merkmale über DSL nutzen zu können**

**Discovery Stage** (ether\_type 0x8863)

- **PPPoE Pakete enthalten type-length-value encodierte TAGs (z.B. 0x0102 AC-Name)**
- **Finden geeigneter Access Concentratoren via PADI an Broadcast (PPPoE Active Discovery Initiation) (Schwachstelle für Angreifer?)**
- **Unicast Antwort PADO (PPPoE Active Discovery Offer)**
- **Client sendet an einen davon PADR (PPPoE Active Discovery Request)**
- **AC antwortet mit PADS (PPPoE Active Discovery Session-confirmation)**  
**Dies Paket beinhaltet u.a. die PPPoE Session ID, die nur für diesen Client und den gewünschten Service gültig ist**

## 4.5 Point-to-Point over Ethernet (PPPoE) (rfc 2516)

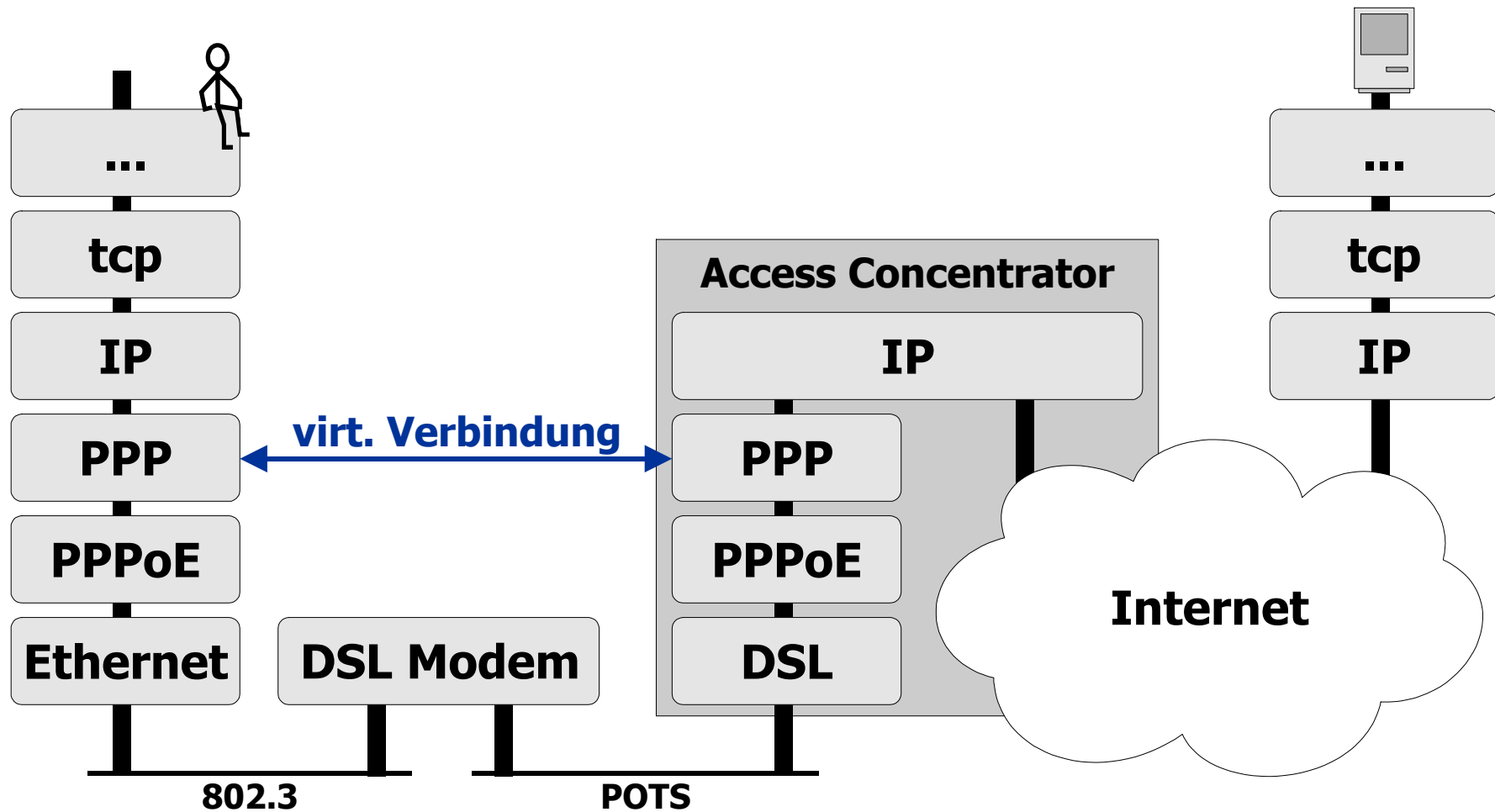
---

### PPP Session Stage (ether\_type 0x8864)

- **Aufbau der eigentlichen PPP-Verbindung**
- **MTU schrumpft um mind. 8 Byte PPPoE Headerdaten**
- **Unplanmässiger Verbindungsabbau via PADT (PPPoE Active Discovery Terminate)**
- **Durch AC-Cookie TAG und HMAC (rfc 2104) kein DOS der DSL-Konzentratoren möglich**

HMAC: Keyed-Hashing for Message Authentication", RFC 2104

## 4.5 Point-to-Point over Ethernet (PPPoE) (rfc 2516)

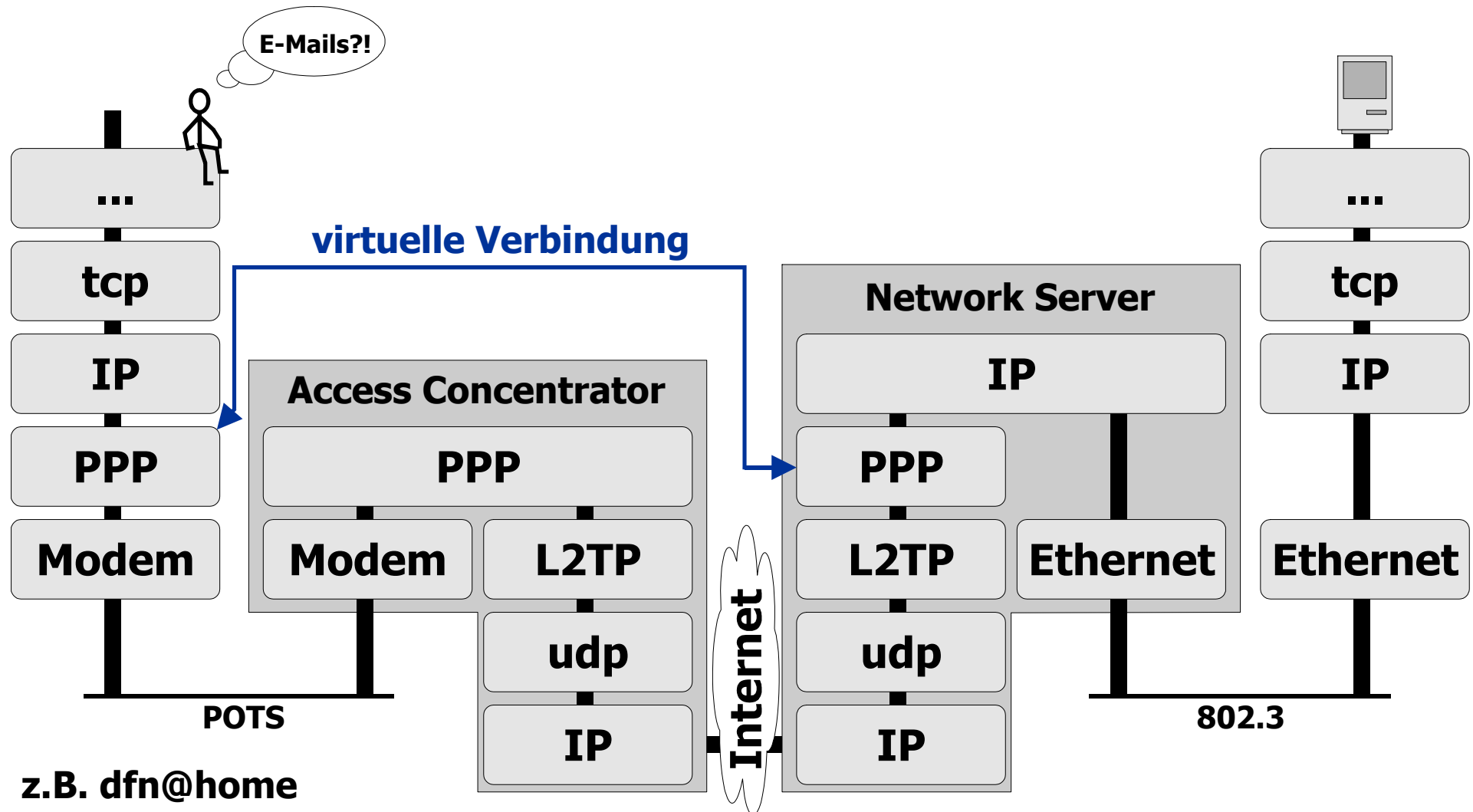


## 4.6 Layer Two Tunneling Protocol (L2TP) (rfc 2661)

---

- **Entstanden aus den Protokollen Point-to-Point Tunneling Protocol (PPTP) (u.a. Microsoft) und Layer-2-Forwarding (u.a. Cisco)**
- **Nutzt PPP zum Transport unterschiedlicher Schicht 3 Protokolle über paketorientierte Netzwerke (IP, ATM, X. 25, ...)**
- **L2TP Access Concentrator (LAC)**
- **L2TP Network Server (LNS)**
- **Verschlüsselung nicht definiert, aber Transport der IP-Daten via IPSec vorgesehen (rfc 3193)**

## 4.6 Layer Two Tunneling Protocol (L2TP) (rfc 2661)

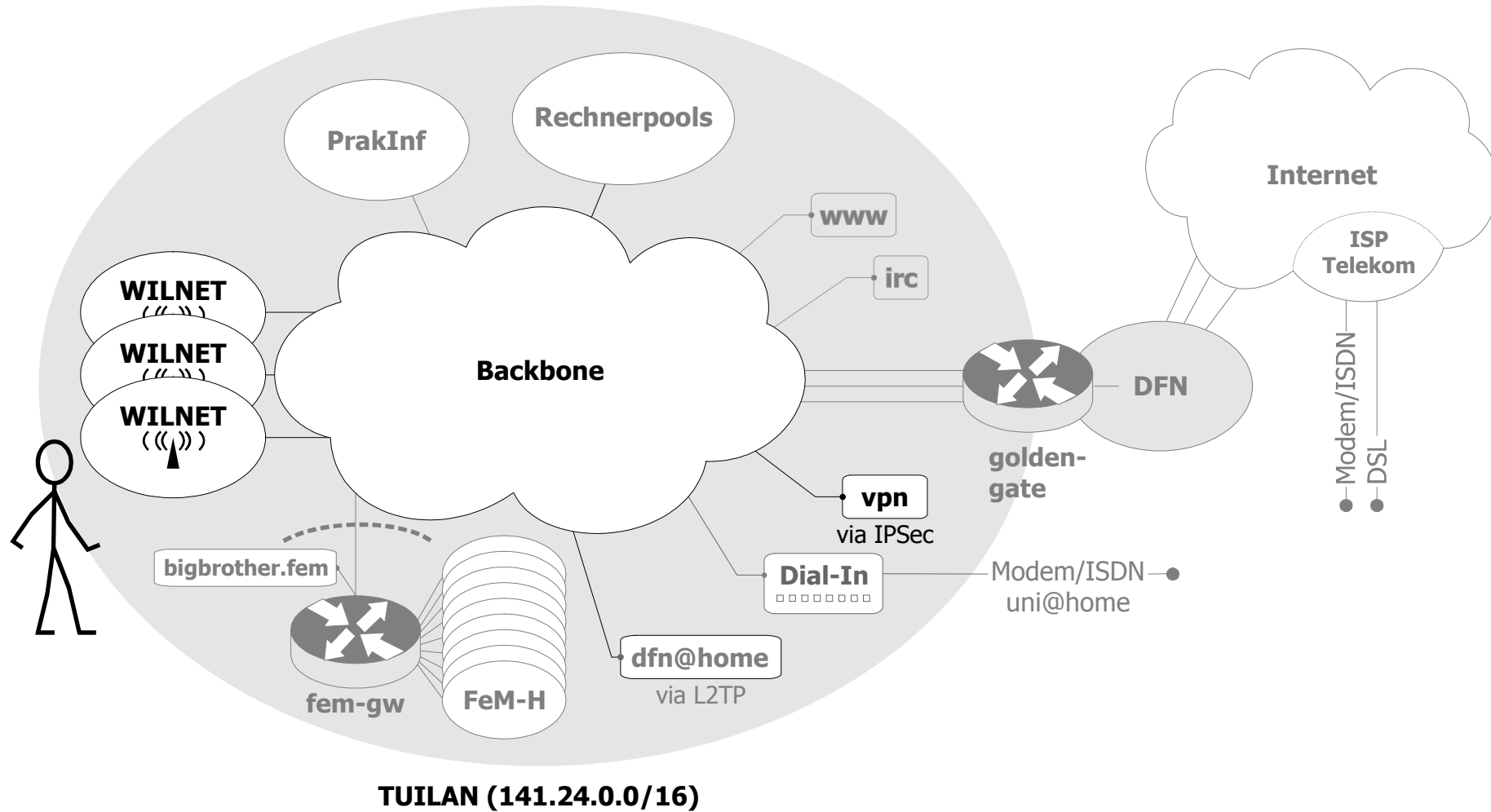


## 4.7 TUILAN extern

---

- **Sämtliche Lösungen haben bislang keine zufriedenstellende Sicherheit geboten**
- **Angreifer könnte durch bestehende Datenverbindungen meinen Computer angreifen**
- **Personal Firewalls helfen mir hierbei nicht weiter**
- **So weit wie möglich Software die verschlüsselt verwenden (SSH, telnet/SSL, IMAPS, HTTPS, ...)**
- **Besserer Ansatz: VPNs auf Basis von IPSec**

# 5. TUILAN mobil: WILNET, IPSec

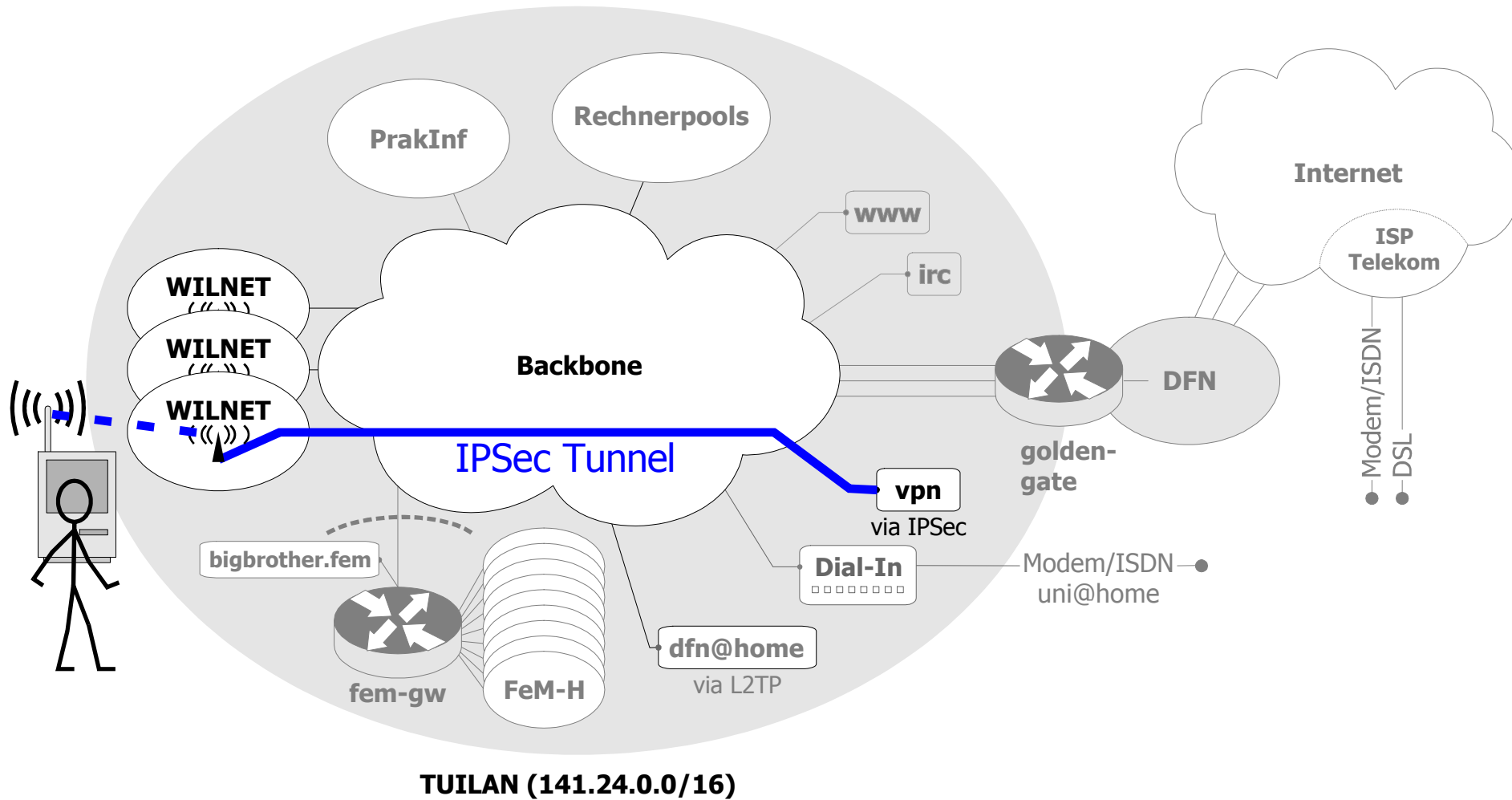


## 5.1 TUILAN mobil: WILNET

---

- **Wireless Ilmenau Network (WILNET)**
- **WLAN auf Basis von IEEE 802.11b, 11 MBit/s, WiFi-Standard**
- **Shared-Medium, jeder sieht den Traffic des anderen**
- **Wired Equivalent Privacy (WEP) bietet keine Sicherheit**
  
- **WILNET bietet auch "öffentliche Netzwerkdosen"**
- **Sicherung der Kommunikation via VPN auf Basis von IPSec (Cisco VPN Client)**

# 5.1 TUILAN mobil: WILNET, IPSec



## 5.2 IPSec (rfc 2411)

---

**Ziel:**

**Authentizität, Integrität und Vertraulichkeit**

**der Kommunikation durch**

**Verschlüsselung und Signaturen**

## 5.2 IPSec (rfc 2411)

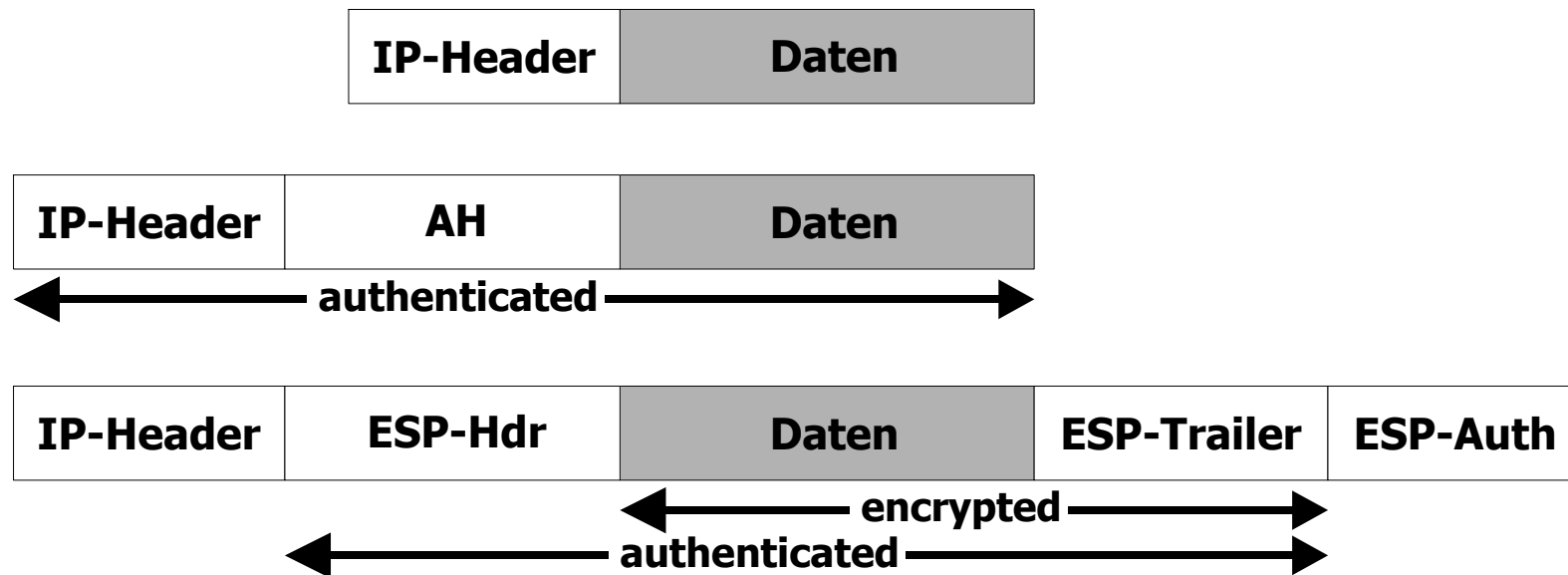
---

### **IPSec = AH + ESP + IPComp + IKE**

- **AH: Authentication Header (rfc 2402)**  
Sichert die Integrität und Authentizität des gesamten IP Paketes durch Signaturen, aber keine Verschlüsselung
- **ESP: Encapsulated Security Payload (rfc 2406)**  
Sichert die Integrität und Authentizität des IP Payloads durch Signaturen, inkl. Verschlüsselung dieser Daten
- **IPComp: IP Compression (rfc 2393)**  
Komprimierung der Daten vor AH/ESP
- **IKE: Internet Key Exchange (rfc 2409)**  
Schlüsselmanagement. Besonders dann wenn die Verbindungspartner sich zu "erstenmal treffen"

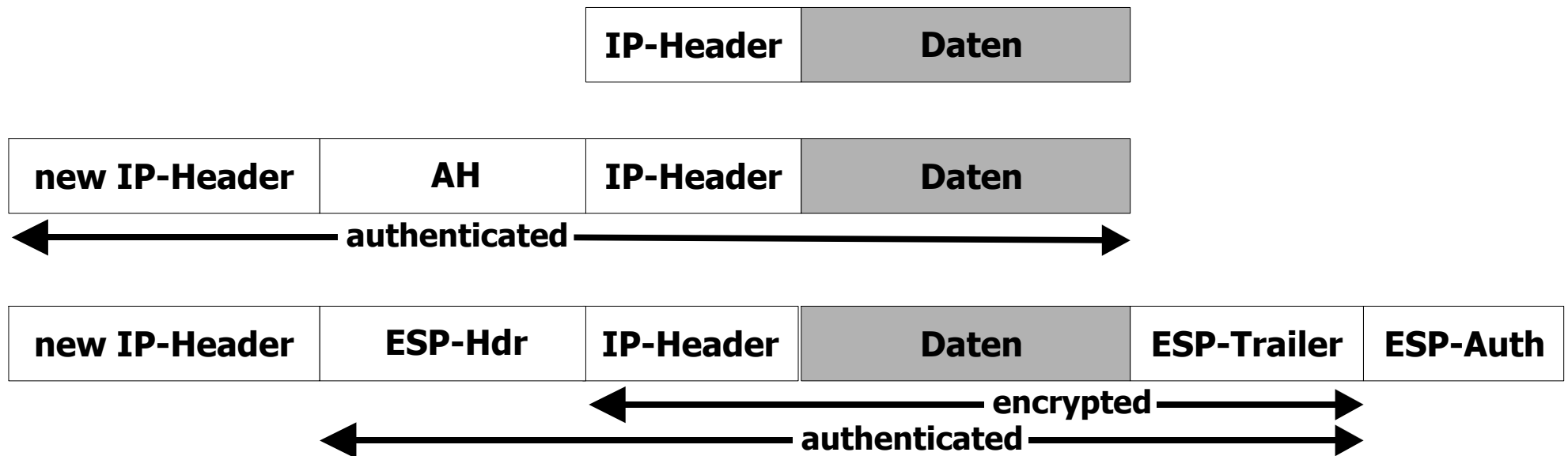
## 5.2 IPSec (rfc 2411)

### Transportmodus



## 5.2 IPSec (rfc 2411)

### Tunnelmodus



## 5.2 IPSec (rfc 2411)

---

- **IPSec bietet einen funktionierenden Ende-zu-Ende Schutz der Kommunikation**
- **IPSec (mit AH) und Network Address Translation (NAT) komplex**
- **IPSec ist ein individueller Sicherheitsansatz und hebt den Sinn von zentralem Sicherheitsmanagement durch Firewalls auf**
  - > **"Lösung": Packet Screen (DFN)**
- **Durch sichere, signierte Daten gäbe es in dem Bereich der persönlichen, wichtigen Kommunikation keine Anonymität mehr.**
- **Signaturen -> Fingerabdrücke, IPSec -> Internet-TCPA?**

**Vielen Dank**

**[http://www.ahzf.de/itsec/TUI-Workshop\\_01.pdf](http://www.ahzf.de/itsec/TUI-Workshop_01.pdf)**