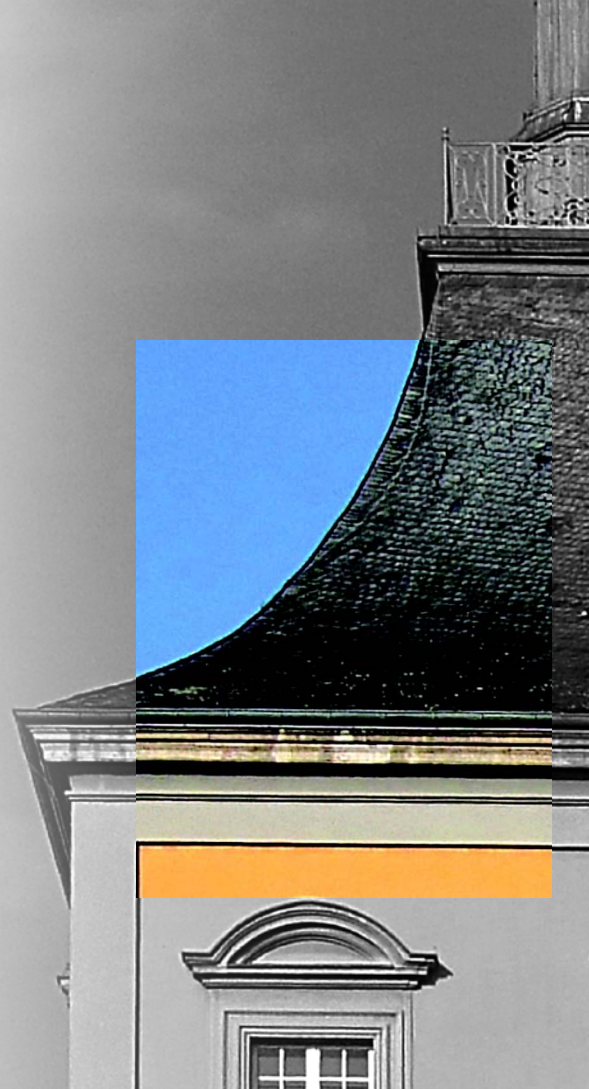
UNIVERSITÄT BONN

VORLESUNG

NETZWERKSICHERHEIT

SOMMERSEMESTER 2023

MO. 14-16 UHR



UNIVERSITÄT BONN

KAPITEL 1

WIEDERHOLUNG OSI-LAYER 1 + 2

NETZWERKE

Lastverbund

- Aufgabenverteilung an unterschiedliche Endpunkte
- (Optimale) Lastverteilung / Ressourcennutzung

Leistungsverbund

- Unterschiedliche spezialisierte Endpunkte
- Zusammengefasst zu einer logischen Einheit

Verfügbarkeitsverbund

- Redundanz / Load-Balancing
- Problem: Datenhaltung oft nicht redundant

UNIVERSITÄT BONN

NETZWERKE (FORTS.)

Funktionsverbund

- Geteilte Ressourcennutzung (Festplattenspeicher, Software, etc.)
- Virtuelle Umgebung (Abstraktion für Benutzer)

Datenverbund

- Zugriff auf gemeinsame Datenbestände (klassische Datenbanken)
- Meist ohne Redundanz und ortsgebunden

Nachrichtenverbund

- Austausch von Nachrichten / Kommunikation
- Ortsübergreifende Erreichbarkeit von Kommunikationspartnern

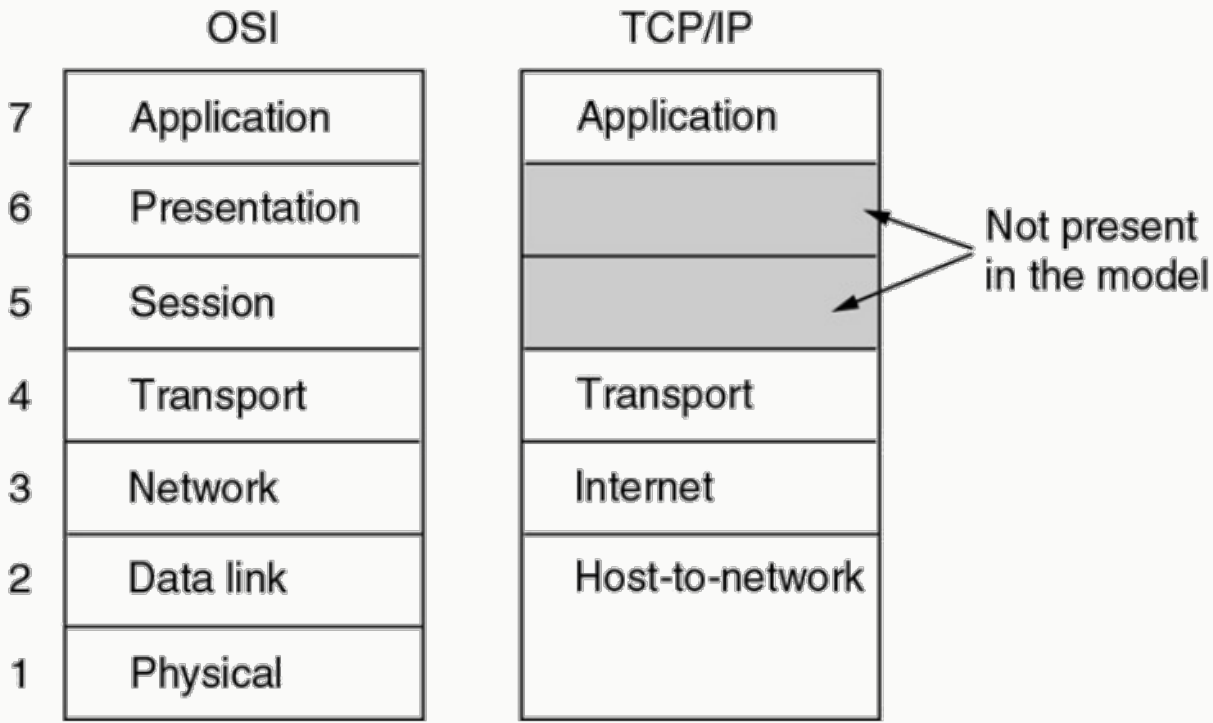
UNIVERSITÄT BONN

NETZWERKE (FORTS.)

Achtung!

- Das World Wide Web ist nicht das Internet!
  - Vielmehr bietet das Internet eine technische Basis für das WWW und weitere Dienste
- Das Internet ist nicht das einzige Netzwerk!
  - GAN – Global Area Network
  - WAN – Wide Area Network
  - MAN – Metropolitan Area Network
  - LAN – Local Area Network
  - PAN – Personal Area Network

NETZWERK-PROTOKOLLE



UNIVERSITÄT BONN

LOKALE NETZWERKE

IEEE 802.X

- Standards für die OSI-Layer 1 + 2 (lokale Netzwerke / Netzzugang)
- Layer 1 (Bitübertragung)
- Layer 2 (Sicherungsschicht / Ethernet)
  - Layer 2a (Media Access Control)
  - Layer 2b (Logical Link Layer)

} so nicht im ISO/OSI-Schichtenmodell

LAYER 1 – BITÜBERTRAGUNGSSCHICHT

Übertragene Einheiten

- Bits / Symbole (z.B. mittels Manchesterkodierung)

Protokolle

- ARCNET
- TokenRing
- 1000Base-T

Geräte / Hardware

- Netzwerkkabel
- Repeater / Hub

amiga.resource.cx
Commodore A560

Pixabay.com - 494654

UNIVERSITÄT BONN

LAYER 2A – MEDIA ACCESS CONTROL

Übertragene Einheiten

- Frames

Protokolle

- 802.3 – Ethernet
- 802.11 – WLAN
- 802.15.1 – Bluetooth

Geräte / Hardware

- Kontrolle der verwendeten Geräte (z.B. Duplex-Settings)
- Zugang zum Übertragungsmedium (z.B. CSMA/CD)

UNIVERSITÄT BONN

LAYER 2B – LOGICAL LINK CONTROL (LLC)

Übertragene Einheiten

- UFrames (unnumbered) – Link control (Disconnect Mode, etc.)
- SFrames (supervisory) – Management (Receiver ready, R. not ready, Reject)
- IFrames (information) – Sequenziell (Payload-Übertragung)

Unterschiedliche Dienstklassen / Protokoll-Multiplexing

- LLC1 (unbestätigt, verbindungslos)
- LLC2 (bestätigt, verbindungsorientiert)
- LLC3 (bestätigt, verbindungslos)
- LLC4 (Vollduplex Punkt-zu-Punkt)

UNIVERSITÄT BONN

ZUGANGSNETZE

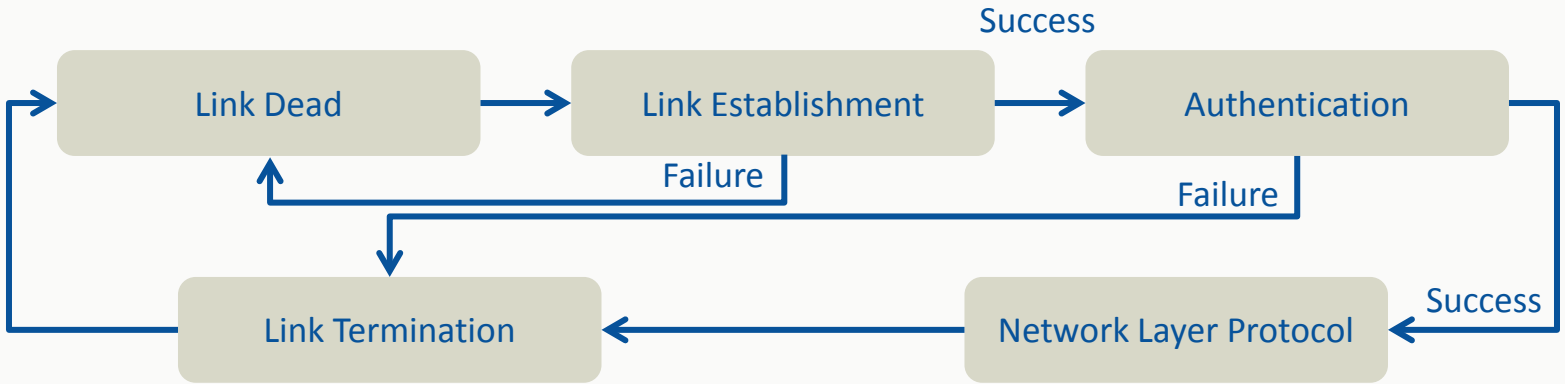
Standards für den (entfernten) Netzwerkzugang

- Modem/ISDN/DSL (PPP)
  - Über die Telefonleitung (häufig asynchrones DSL)
- Ethernet (PPPoE)
  - Kabelanschluss (PPPoE)
  - WLAN (Eduroam)
  - Root-/V-Server im Rechenzentrum
- Mobiler Zugang
  - GSM/UMTS/LTE
  - 5G

ZUGANGSNETZE

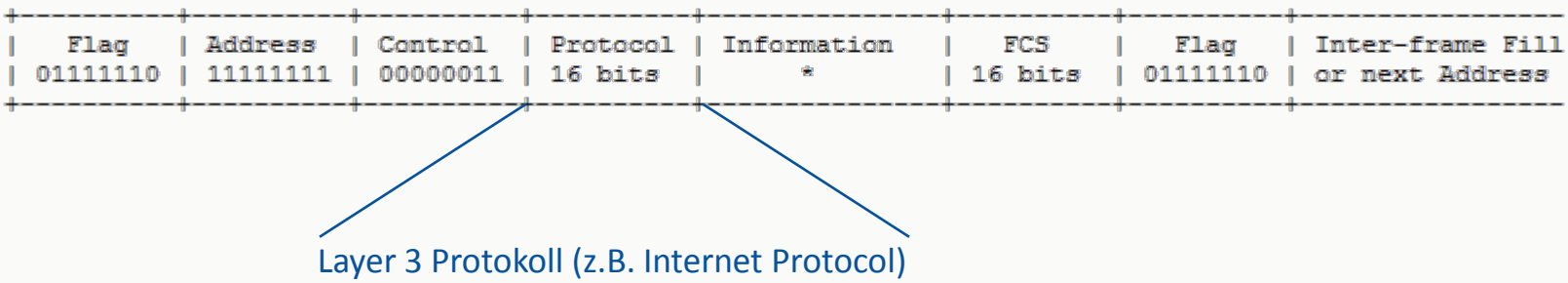
PPP (urspr. RFC 1331)

- basiert heute häufig auf HDLC (High-Level Data Link Control; RFC 1662)



ZUGANGSNETZE

PPP (urspr. RFC 1331)



- Authentifikation über zusätzliches Authentication Protocol (z.B. PAP, CHAP, ...)

PPPoE (RFC 2516) – Basiert auf Ethernet-Frames

GLEICH MEHR

PPTP (RFC 2637) – „Microsoft“-Tunnel (z.B. über IP-Netze)

- Microsoft Point-to-Point-Encryption (MPPE)
- Microsoft Point-to-Point Compression (MPPC)

UNIVERSITÄT BONN

KAPITEL 1

WIEDERHOLUNG: OSI-LAYER 1 + 2 SICHERHEIT

UNIVERSITÄT BONN

LAYER 1 - SICHERHEITSASPEKTE

Einziges Angriffsszenario: Physikalischer Zugriff

- Rechenzentrum
- Dark-Fiber
- WLAN
- IMSI-Catcher

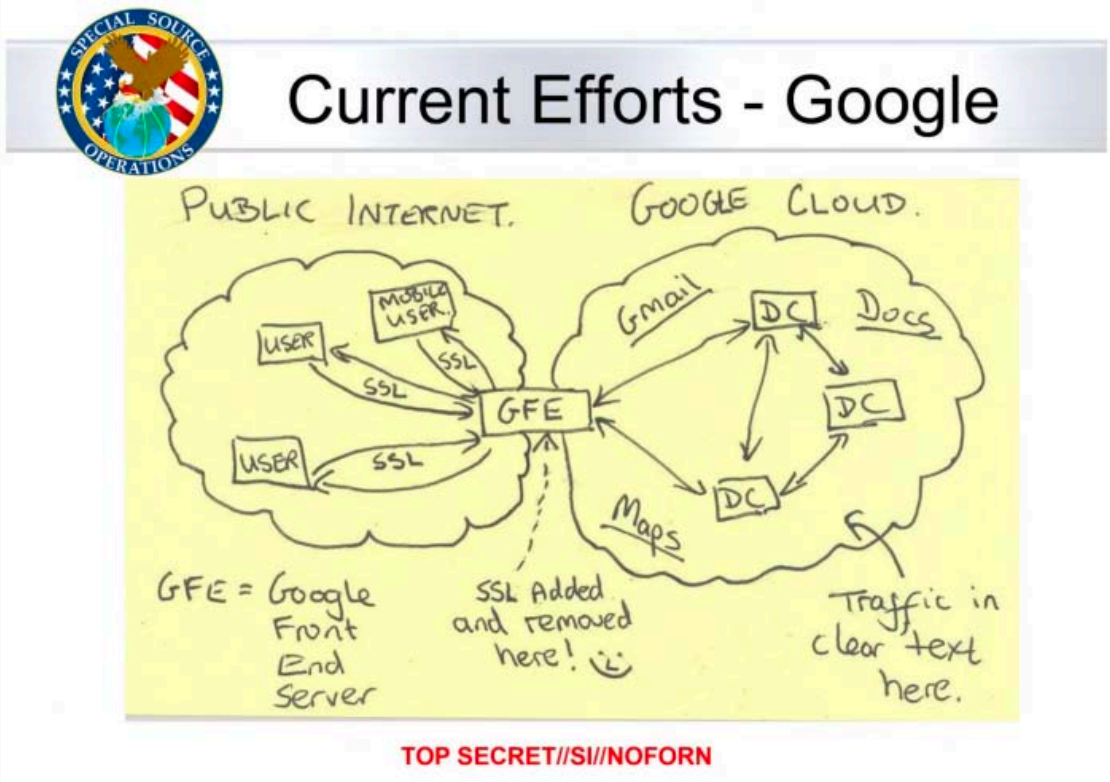
Mögliche Angreifer (realistisch?)

- RZ-Betreiber / Angestellte / Reinigungskraft
- WLAN-Wardriver
- Strafverfolger / Geheimdienste

LAYER 1 – SICHERHEITSASPEKTE (FORTS.)

Exkurs in die Realität

- NSA belauscht unverschlüsselten Google-Traffic (Dark-Fiber)



LAYER 1 – SICHERHEITSASPEKTE (FORTS.)

Exkurs in die Realität

- NSA belauscht unverschlüsselten Google-Traffic (Dark-Fiber)
- IMSI-Catcher in Gefängnissen oder bei Ermittlungen

UNIVERSITÄT BONN

LAYER 2 - SICHERHEITSASPEKTE

IEEE 802 – MAC-Schicht

- 802.3ab (1000Base-T)
  - Authentifikation verwendeter Hardware (z.B. auf Basis der MAC-Adresse)
    - Einfach zu fälschen (Spoofing)
  - Zertifikatbasierte Authentifikation (802.1X „Port-based Authentication“)
    - Zertifikate zur Authentifikation

LAYER 2 - SICHERHEITSASPEKTE

IEEE 802 – MAC-Schicht

- 802.3ab (1000Base-T)
  - Authentifikation verwendeter Hardware (z.B. auf Basis der MAC-Adresse)
    - Einfach zu fälschen (Spoofing)
  - Zertifikatbasierte Authentifikation (802.1X „Port-based Authentication“)
    - Zertifikate zur Authentifikation
- 802.11 (WLAN)
  - WEP (Wired equivalent privacy) **UNSICHER!**
  - WPA/WPA2/WPA3 (WiFi Protected Access)
  - Verschlüsselung und Authentifikation

KEINE VERSCHLÜSSELUNG

LAYER 2 – SICHERHEITSASPEKTE (FORTS.)

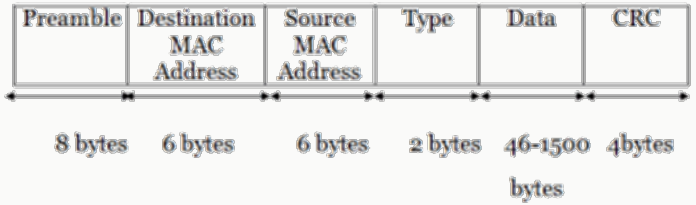
PPP/PPTP/PPPoE

- PAP (Password Authentication Protocol)
  - Unverschlüsselte Übertragung von Benutzername : Passwort
- CHAP (Challenge Handshake Authentication Protocol)
  - Zufallszahl des Servers mit Benutzerpasswort gehashed
  - MS-CHAPv2 mit MD4/DES mit Bruteforce zu knacken
- EAP (Extensible Authentication Protocol)
  - 2-Phasen-Authentifikation (z.B. mit RADIUS)
  - Erlaubt Verwendung von Authentication-Protokollen (z.B. Kerberos)
  - >40 konkrete Verfahren (z.B. EAP-TLS, EAP-MD5, EAP-TTLS, …)

LAYER 2 – SICHERHEITSASPEKTE (FORTS.)

ARP (Address Resolution Protocol, RFC826)

- Kommunikation auf L2 über MAC-Adressen der Netzwerk-Hardware



- Zuordnung übergeordneter Adressen (z.B. IP-Adressen) zu MAC-Adressen
- Keine Sicherheitsmechanismen (Broadcast request; Broadcast/Unicast response)
- ARP findet meist vom Benutzer unbemerkt statt

LAYER 2 – SICHERHEITSASPEKTE (FORTS.)

ARP (Address Resolution Protocol, RFC826)

- Rechner pflegt einen ARP-Cache

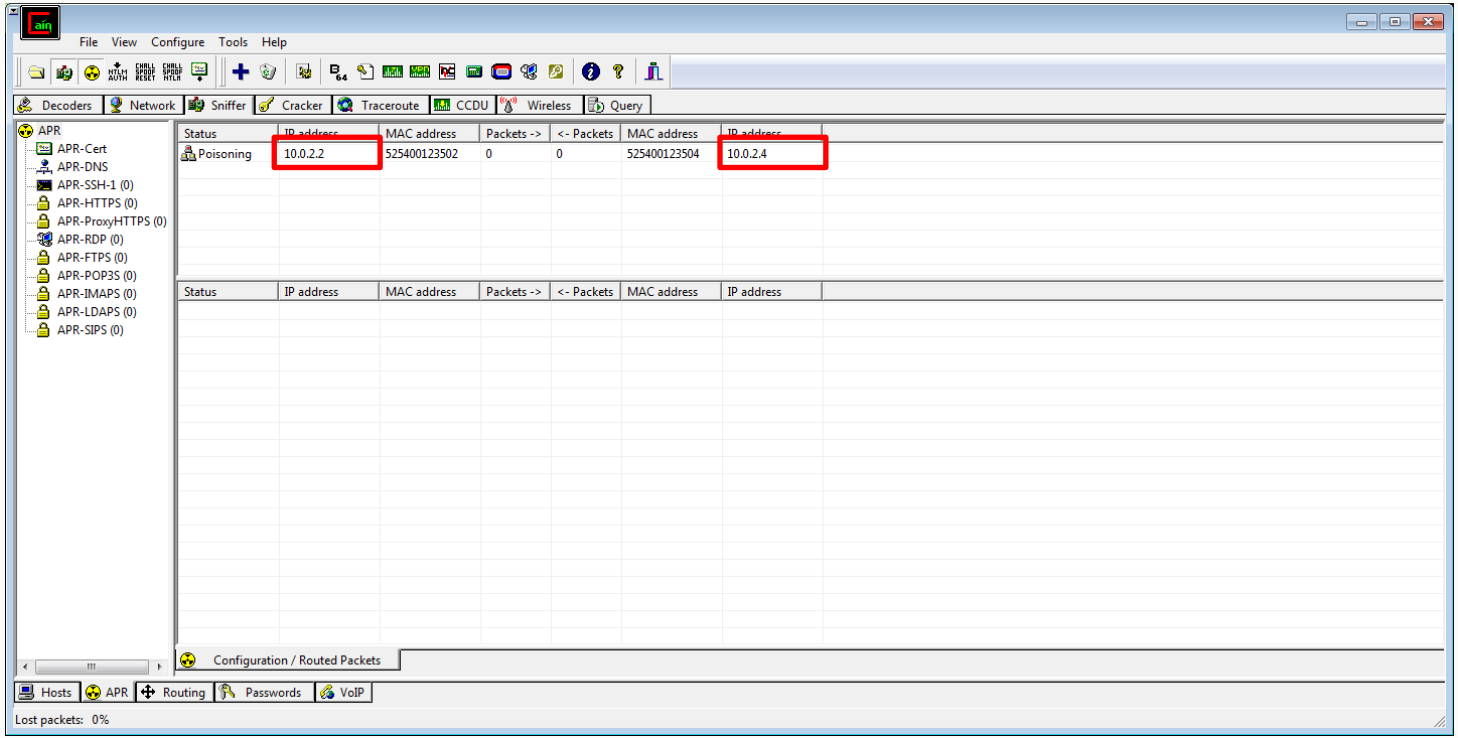
```
[matze@tschita] ~ $ arp -an
(192.168.2.108) auf fc:a1:83:63:76:19 [ether] auf wlan0
(192.168.2.128) auf ac:6f:bb:84:61:5a [ether] auf wlan0
(192.168.2.115) auf f8:cf:c5:cd:e2:e8 [ether] auf wlan0
(192.168.49.1) auf fc:a1:83:63:76:19 [ether] auf wlan0
(192.168.2.121) auf ac:6f:bb:7a:9b:f7 [ether] auf wlan0
(192.168.2.10) auf 60:e3:27:f5:3e:70 [ether] auf wlan0
(192.168.2.104) auf 6c:ad:f8:72:0f:14 [ether] auf wlan0
(192.168.2.22) auf 30:05:5c:e8:f8:3d [ether] auf wlan0
(192.168.2.30) auf 60:e3:27:f5:3e:70 [ether] auf wlan0
(192.168.2.1) auf 38:10:d5:3b:ee:3c [ether] auf wlan0
(192.168.2.21) auf ec:9a:74:9a:bc:60 [ether] auf wlan0
```

LAYER 2 – SICHERHEITSASPEKTE (FORTS.)

ARP (Address Resolution Protocol, RFC826)

- Manipulation des ARP-Cache durch gefälschte Antworten
  - ARP-Cache poisoning / ARP-Spoofing
  - Ermöglicht Man-in-the-middle
  - Nur in lokalen Netzen möglich (Layer 2!)
  - Angriff ist ohne technisches Verständnis möglich
    - Linux: z.B. Ettercap
    - Windows: z.B. Cain&Abel (oxid.it)

LAYER 2 – SICHERHEITSASPEKTE (FORTS.)



UNIVERSITÄT BONN

LAYER 2 – SICHERHEITSASPEKTE (FORTS.)

Denial of Service

- Flooding
  - Unicast Flooding eines Hosts (auch mit Hilfe von ARP möglich)
  - Flooding eines Switches mit ARP-Paketen / gefälschten Ethernet Frames

Zusammenfassend:

- Layer-2-Sicherheitsprobleme sind nur bedingt durch Sicherheitsmechanismen auf höheren Schichten zu kompensieren

UNIVERSITÄT BONN

OSI LAYER 1 + 2: FAZIT

Rückblick

- ISO/OSI-Layer 1 und 2 (MAC & LLC nach IEEE 802)
- Unterschiedliche Protokolle auf beiden Schichten
  - 1000Base-T / ARCNET / Ethernet
  - CSMA/CD
  - Ethernet / WLAN / Bluetooth
- Sicherheitsaspekte
  - ARP-Spoofing / -Cache-Poisoning
  - Denial-of-Service

UNIVERSITÄT BONN

AUSGABE ÜBUNGSZETTEL

Immer dienstags (vor der Übung) auf der Vorlesungswebseite

- 1 Woche Bearbeitungszeit
- Abgabe in Gruppen

Morgen ist noch keine Übung!

UNIVERSITÄT BONN

ENDE

Vielen Dank für die Aufmerksamkeit!

Fragen?

Nächste Vorlesung:

- Montag, 17. April 2023

Nächste Übung:

- Dienstag, 18. April 2023 – 16 Uhr
- Abgabe des Übungszettels 1 bis zum 18. – 16 Uhr