DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Netzwerktechnologien

Einführung in Computernetzwerke

FH JOANNEUM 08.11. – 09.11.2022

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

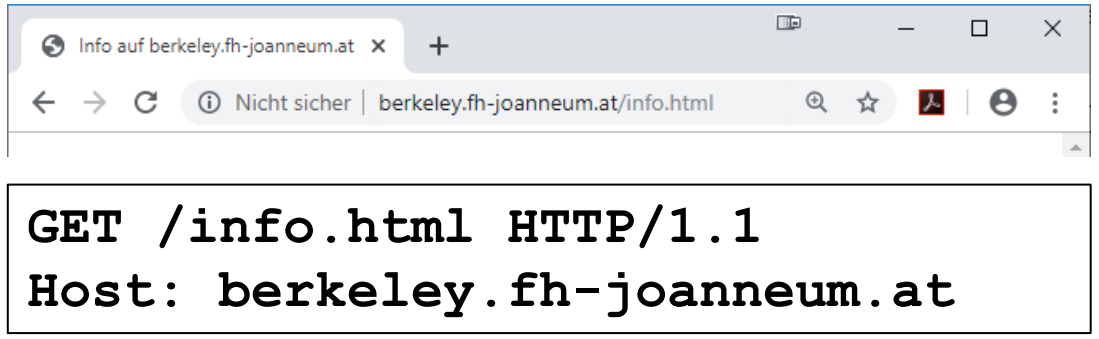
Inhalte:
Einführung Netzwerke
Basistechnologien
OSI Layer, Protokolle und Geräte

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Fallbeispiel: **Client - Server Kommunikation**

- **Client**
  Web Browser
  z.B. Google Chrome)




```
GET /info.html HTTP/1.1
Host: berkeley.fh-joanneum.at
```

- **sendet**
  über das Netzwerk eine
  HTTP*- **Anfrage**

- an den
  Web-**Server**
  z.B. Apache 2

*(*HTTP = Hypertext Transfer Protocol)*

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Fallbeispiel: **Client - Server Kommunikation (2)**

von Client

von
Hardware Adresse
Client PC

an
Hardware Adresse
Gateway

No.	Time	Source	Destination	Protocol	Length	Info
3382	22.991350	10.52.200.132	91.229.57.56	HTTP	698	GET /info.html HTTP/1.1

```
Frame 3382: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits) on interface 0
Ethernet II, Src: 40:b0:76:a2:42:07, Dst: 00:08:e3:ff:fd:2c
Internet Protocol Version 4, Src: 10.52.200.132, Dst: 91.229.57.56
Transmission Control Protocol, Src Port: 53638, Dst Port: 80, Seq: 1, Ack: 1, Len: 644
Hypertext Transfer Protocol
  GET /info.html HTTP/1.1\r\n
  Host: berkeley.fh-joanneum.at\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  Cookie: _ga=GA1.2.1115739603.1574071763; _gid=GA1.2.764581842.1574071763\r\n
  If-None-Match: "9b-5979e1fe538ec-gzip"\r\n
  If-Modified-Since: Mon, 18 Nov 2019 12:31:19 GMT\r\n
```

Port für **HTTP**

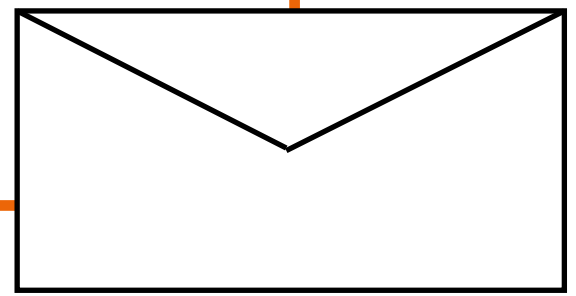
von
Logische Adresse
Client PC

an
Logische Adresse
Webserver

Aus "ipconfig /all"
Netzwerkkarte von Client:
Physische Adresse : 40-B0-76-A2-42-07
IPv4-Adresse . . . . : 10.52.200.132
Standardgateway : **10.52.1.254**

Aus "arp –a":
Schnittstelle: 10.52.200.132

Internetadresse	Physische Adresse
10.52.1.254	**00-08-e3-ff-fd-2c**



DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

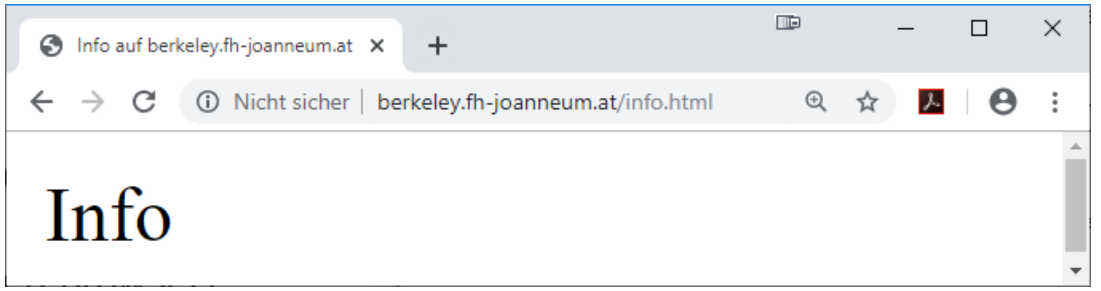
Fallbeispiel: **Server – Client Kommunikation (1)**

- Der **Server** sendet eine (HTTP-) **Antwort** an den **Client** (=Browser) zurück

- und deren Inhalt zeigt ein Browser als (HTML) **Dokument** gerendert an

```
HTTP/1.1 200 OK
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>Info auf berkeley.fh-joanneum.at</title>
  </head>
  <body>
        Info
  </body>
</html>
```



DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Fallbeispiel: Server – Client Kommunikation (1)

von Server

von
Hardware Adresse
Gateway

an
Hardware Adresse
Client PC

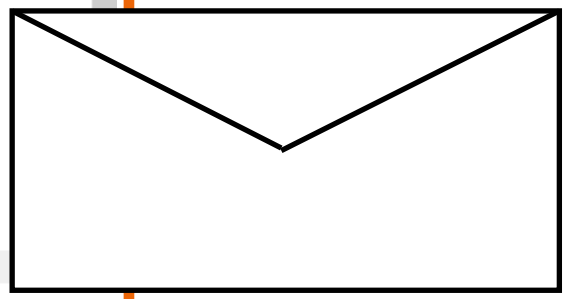
```
No.     Time        Source          Destination     Protocol  Length Info
   3483 13.250701   91.229.57.56    10.52.200.132   HTTP         559 HTTP/1.1 200 OK  (text/html)

Frame 3483: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
Ethernet II, Src: 00:08:e3:ff:fd:2c, Dst: 40:b0:76:a2:42:07
Internet Protocol Version 4, Src: 91.229.57.56, Dst: 10.52.200.132
Transmission Control Protocol, Src Port: 80, Dst Port: 54074, Seq: 1, Ack: 619, Len: 505
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 18 Nov 2019 13:20:42 GMT\r\n
  Server: Apache/2.4.25 (Debian)\r\n
  Last-Modified: Mon, 18 Nov 2019 12:31:19 GMT\r\n
  ETag: "9b-5979e1fe538ec-gzip"\r\n
  Accept-Ranges: bytes\r\n
  Vary: Accept-Encoding\r\n
  Content-Encoding: gzip\r\n
  Access-Control-Allow-Origin: *\r\n
  Content-Length: 137\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.004144000 seconds]
  [Request in frame: 3481]
  [Request URI: http://berkeley.fh-joanneum.at/info.html]
  Content-encoded entity body (gzip): 137 bytes -> 155 bytes
  File Data: 155 bytes
Line-based text data: text/html (11 lines)
```

Port für **HTTP**

von
Logische Adresse
Webserver

an
Logische Adresse
Client PC



Fallbeispiel: **Zusammenfassung**

- Einer sendet eine Anfrage, der andere antwortet → **Client-Server** Model
- HTTP (Hyper Text Transport Protocol) ist die "**Sprache**", das **Protokoll**, die zwischen Server und Browser gesprochen wird.
- "**Protokolle**" bilden die **technische Basis** des Internets.
- Moderne Computernetzwerke unterscheiden genau zwischen **Anwendung**(-sdaten) und **Transport**
- **Jedes Transportmittel** kann genutzt werden, solange bestimmte Voraussetzungen erfüllt werden. (Geschwindigkeit, Latenz, …)

Kommunikations-Schichten

- Daten, als **HTML** kodiert
- Anwendungsprotokoll ist **HTTP** (das WWW)
- Transportprotokolle (logisch) sind **TCP / IP**
- Transportprotokoll (physisch)ist das kabelgebundene **Ethernet II.**
  (Es könnten aber auch Funk, Kabel, Briefträger oder gar Brieftauben verwendet werden …)*

(* RFC 1149: IP Protocol implemented over Avian Carriers (IPoAC))

Technische Termini

https://tools.ietf.org/html/rfc1122

IP Datagram

- Einheit der End-zu-End Verbindung im IP
- besteht aus IP Header und Segmentdaten

Segment

- Einheit der End-zu-End Verbindung im TCP
- besteht aus TCP Header und Daten
- ist in einem IP Datagramm eingekapselt

Frame | Rahmen

- Einheit der Verbindungsschicht
- besteht aus Header der Verbindungsschicht und einem Paket

Packet | Paket

- Datenpaket, das zwischen Internet- und Verbindungsschicht gesendet wird. Kann ein ganzes oder das Fragment eines Datagrams sein

Message | Nachricht

- Daten, die zwischen Transport- und Internetschicht gesendet werden. Kann ein Segment sein

Maximale Größen von

Datagram

- 576 Oktette

Segment | Maximum Segment Size (mss)

- 536 Oktette
- Maximale Datagramgröße – 40 Oktette (Header)

MTU | Maximum Transfer Unit

- maximal zulässige Größe eines Pakets

Begriffe: **Daten**

- **Bit** (kommt vom engl. „binary digit“)
  - Maßeinheit für digitale Daten mit den Zuständen 0 oder 1
  - Einheit: b (1 Mb = 1 Megabit = 1.000.000 Bit; 1Gb = i Gigabit = 1.000.000.000 Bit)

- **Byte** (kommt vom engl. „bit“ und „bite“)
  - Maßeinheit für digitale Daten. Besteht in der Regel aus 8 Bit.
  - Einheit: B (1 KB = 1 Kilobyte = 1.000 Byte = 8.000 Bit)

- **Taktrate** (Hz)
  - Um digitale Signale zu übertragen werden in der Netzwerktechnik konstante Taktintervalle verwendet. 1 Intervall pro Sekunde entspricht 1 Hz.
  - Einheit: Hz
  - Beispiele: 1.000 Hz = 1 KHz, 1.000.000 Hz = 1 MHz

Übertragungstypen 1/2

- **Punkt zu Punkt** (Direktverbindung)
  - Verbindung zwischen zwei Punkten/Orten/Systemen
  - Wenn andere Systeme dazwischen liegen spricht man von **End zu End** Verbindung
  - Redundanz durch mehrere Routen
  - „Packet Switching“

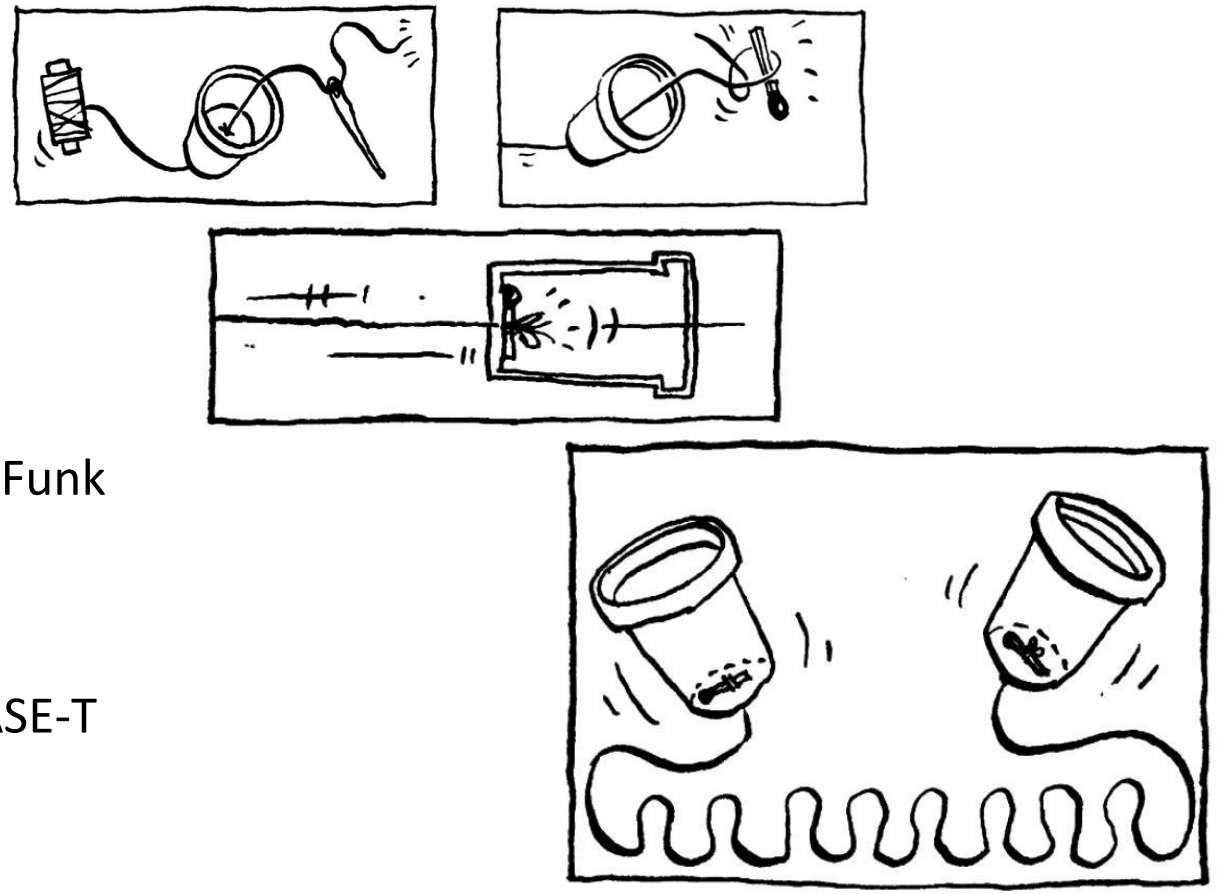
Größere Netzwerke (geographische Verteilung) haben üblicherweise eine "Point-To-Point" Verbindung
Kleinere Netzwerke arbeiten effizienter mit Broadcast Technologien.

- **Broadcast**
  - Überträgt eine Nachricht von einem System auf alle anderen Systeme
  - Alle hören die Nachricht und müssen relevante Daten herausfiltern
- **Multicast**

  Überträgt eine Nachricht von einem System auf eine Gruppe von Systemen

Übertragungsrichtung

- **Simplex** (SX) - Richtungsbetrieb
  - **Unidirektionaler** Kanal - Broadcast
  - Beispiele: Radio, Fernsehen
- **Halbduplex** (HX) - Wechselbetrieb
  - **Bidirektional abwechselnd**
  - Beispiele: Walkie-Talkie, Relaisstationen, CB-Funk
- **(Voll-)Duplex** (DX) - Gegenbetrieb
  - **Bidirektional gleichzeitig**
  - Beispiel: Telefon, mobile Endgeräte, 1000BASE-T Kabel, High Level Data Link Control (HDLC)



https://kinderuni.at/forsche-und-staune/experimente/kannst-du-mit-joghurtbechern-telefonieren/

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Übung: **Welcher Typ, welche Richtung?**

Beschreibung	Übertragungstyp (Punkt zu Punkt, Broadcast)	Übertragungsrichtung (Simplex, Half oder Full Duplex)
Türglocke		
Radio		
Händehaltendes Pärchen mit eigenem Code für das Drücken der Hand		
„A capella“ Gruppe (beim Üben)		
Pistolenduell		
Teamspeak		
Diskussionen		






DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Netzwerkgeräte im Überblick

- Ein **Modem** dient der Einwahl ins Netzwerk des Internet Service Providers (z.B. Telekom)
- Verschiedene **Kabel** aus Kupfer, Glasfasern (Lichtwellenleiter), etc. verbinden Netzwerkkomponenten
- Eine **NIC** (Network Interface Card) – die **Netzwerkkarte**
  - nimmt im „**promiscous“ Modus** alle Pakete an.
  - Ansonsten nur Pakete, welche als Ziel die Hardware-Adresse der Karte haben!
- **Repeater** verstärken/verbessern Signale (Damit kann man ein Kabel verlängern)
- **Hubs** kopieren/verstärken/verbessern ein Signal/Paket auf mehrere Ausgänge (Multiport-Repeater)
- **Switches** leiten Signale/Pakete zielgerichtet weiter und Speichern dazu an welche Hardware Adresse Pakete gesendet werden Der Vorteil: Keine Überflutung mit Paketen
- **Router** entscheiden, in welches Netzwerk ein Signal/Paket kommt
- **Firewalls** überprüfen Pakete nach verschiedenen Regeln

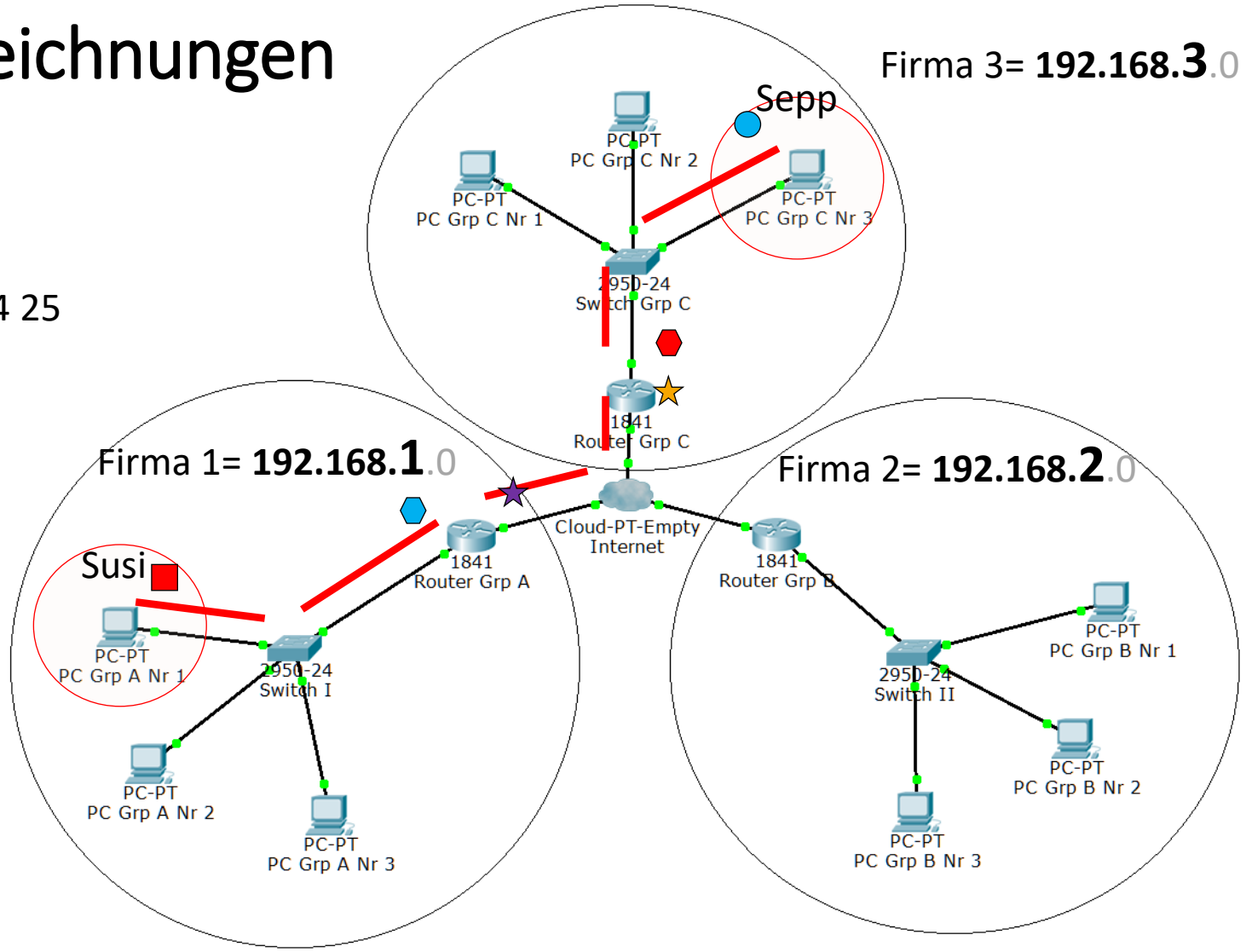
DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Netzwerkbezeichnungen

= 00 E0 A3 0D 24 25

Susi = 192.168.1.**1**



Netzwerkbezeichnungen & Reichweiten

- **LAN** (Local)
  Mit einer Reichweite von wenigen Kilometer ideal für Unternehmen und im Privatbereich
- **MAN** (Metropolitan)
  Die Reichweite nimmt Stadtgröße mit bis ca 100 Kilometer ein. Für große Unternehmen, die Stadtverwaltung und ISPs.
- **WAN** (Wide) In einem Lander oder auf einem Kontinent. Das Internet wäre schon ein Beispiel, dessen Architektur eine Verbindung mehrerer Topologien und Teilnetze möglich macht
- **GAN** (Global)
  Ein globales Netzwerk wie das Internet verbindet mehrere WANs International und Interkontinental über Unterwasserkabel und Satelliten

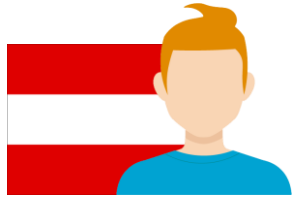
Das "Schichtenmodel"

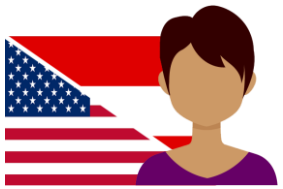
- Ein Schichtenmodel **vereinfacht die Interaktionen zwischen den Operationseinheiten** durch Vereinfachung
- Schichten werden definiert durch …
  - … das, **was sie machen**.
  - … die **Eingabe**, die sie brauchen.
  - … die **Ausgabe**, die sie anbieten.
- Die Funktionalität jeder Schicht kann **unabhängig entwickelt** werden.
- Die Schichten haben **genau definierte Schnittstellen**.
- Solange die **Definition der Schnittstelle** entsprochen wird funktioniert das System: Das nennt man **Kapselung**.
- **Gleiche Schichten auf unterschiedlichen Plattformen** sind **zueinander immer kompatibel**!

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Beispiel – Telefonanruf nach Spanien





Teilnehmer in Österreich

Übersetzer

Telefon

Vermittlung

Kabel

Virtuelle Verbindung
Protokoll

Virtuelle Verbindung
Protokoll

Signale
Physische Verbindung

Schnittstelle

Schnittstelle

Schnittstelle

Schnittstelle

Schnittstelle

Teilnehmer in Spanien

Übersetzer

Telefon

Vermittlung

Kabel

Schnittstelle

Schnittstelle

Schnittstelle

Schnittstelle

Begriffe

- **Schnittstelle**
  - Übergang zwischen 2 übereinanderliegenden Schichten
  - Regeln der Kommunikation über die Schnittstellen bilden die Schnittstellendefinition
- **Dienste**
  - Leistungen, die eine Schicht der darüber liegenden zur Verfügung stellt
- **Protokolle**
  - Kommunikationsvorschrift von Partnern der gleichen Schicht.
  - Format der ausgetauschten Daten
- **Virtuelle Verbindung**
  - Kommunikation zwischen 2 Partnern der gleichen Schicht

OSI – Open Systems Interconnect

Kommunikation in **sieben Schichten** mit diesen Zielen:

- Eine **Schicht** soll dort erstellt werden, wo ein neuer **Abstraktionsgrad** nötig ist.
- Jede Schicht soll eine **genaue definierte Funktion** erfüllen.
- Bei Funktionswahl sollen international **genormte** Protokolle berücksichtigt sein.
- Die Grenzen zwischen den Schichten sollen so sein, dass der **Informationsfluss** über sie **möglichst gering** bleibt.
- Die Anzahl der Schichten soll eine **handliche Architektur** mit unterschiedlichen Funktionen in unterschiedlichen Schichten sein.

Die glorreichen Sieben

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

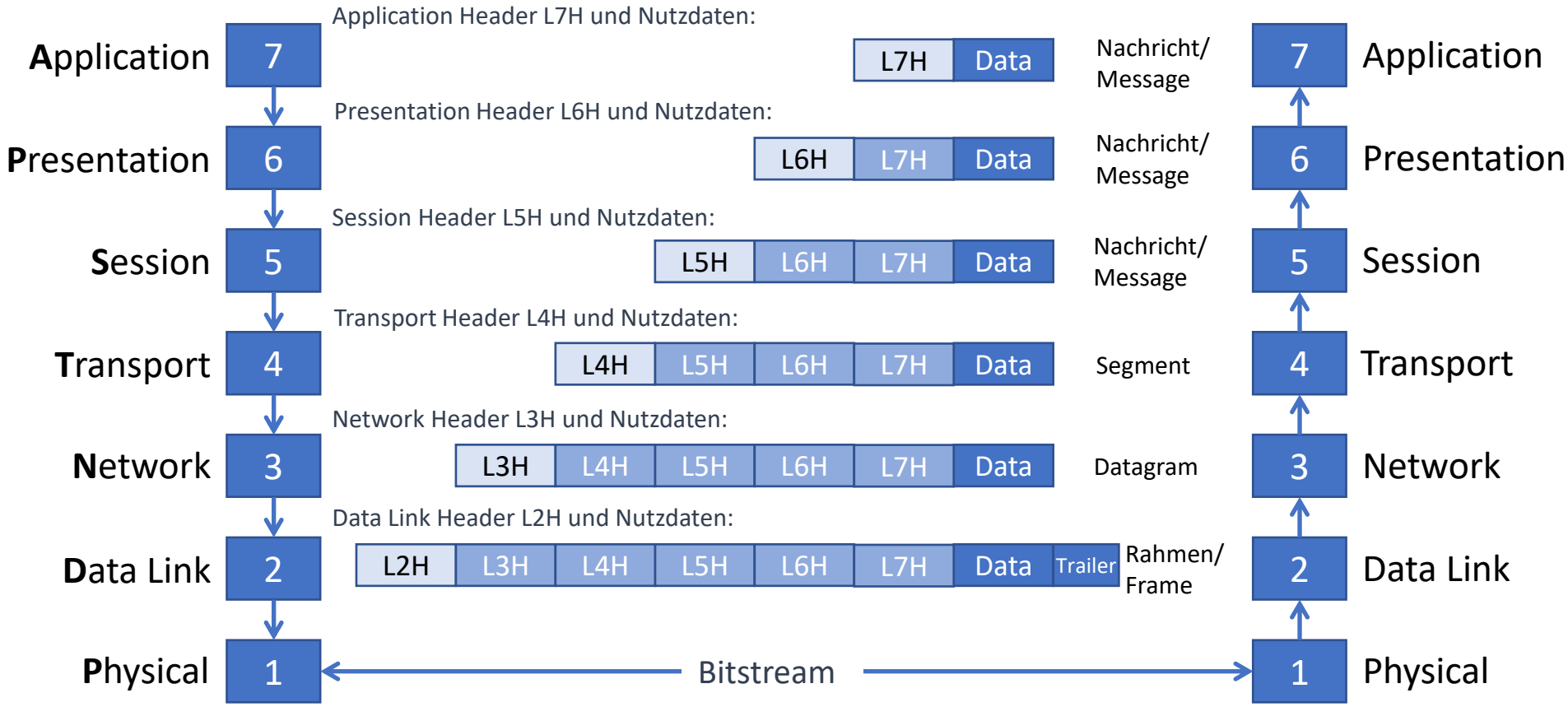
OSI Datenkapselung und -transport

Anwendungsorientiert:

- Anwendungsschicht
- Präsentationsschicht
- Sitzungsschicht

Transportorientiert:

- Transportschicht
- Vermittlungsschicht
- Sicherungsschicht
- Physische Schicht



„**P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way“

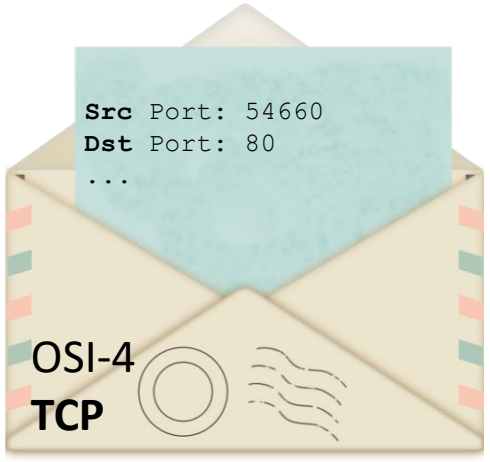
DIHSÜD Innovation Hub

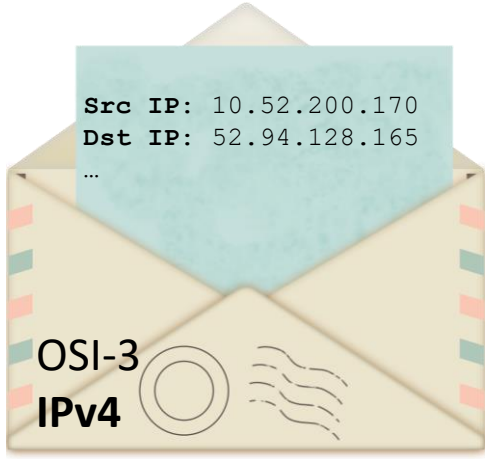
FH JOANNEUM University of Applied Sciences

OSI Kapselung
Beispiel HTTP
Port 80

Client Request

Ein Paket vom ***Client*** *geht an den* ***Server***





Legende:

Src … Source (Quelle)
Dst … Destination (Ziel)
IP … Internet Protokoll
Logische Adressierung
MAC … Media Access Control
Hardware Adresse
Zugriff auf das Medium
Netzwerkkarte
Port … "Nummer" des Dienstes, der am Server angesprochen wird- bzw. Nummer für "Rück-Antwort" von diesem Dienst

Physische Verbindung

`0001101010110110 0…`

OSI-1

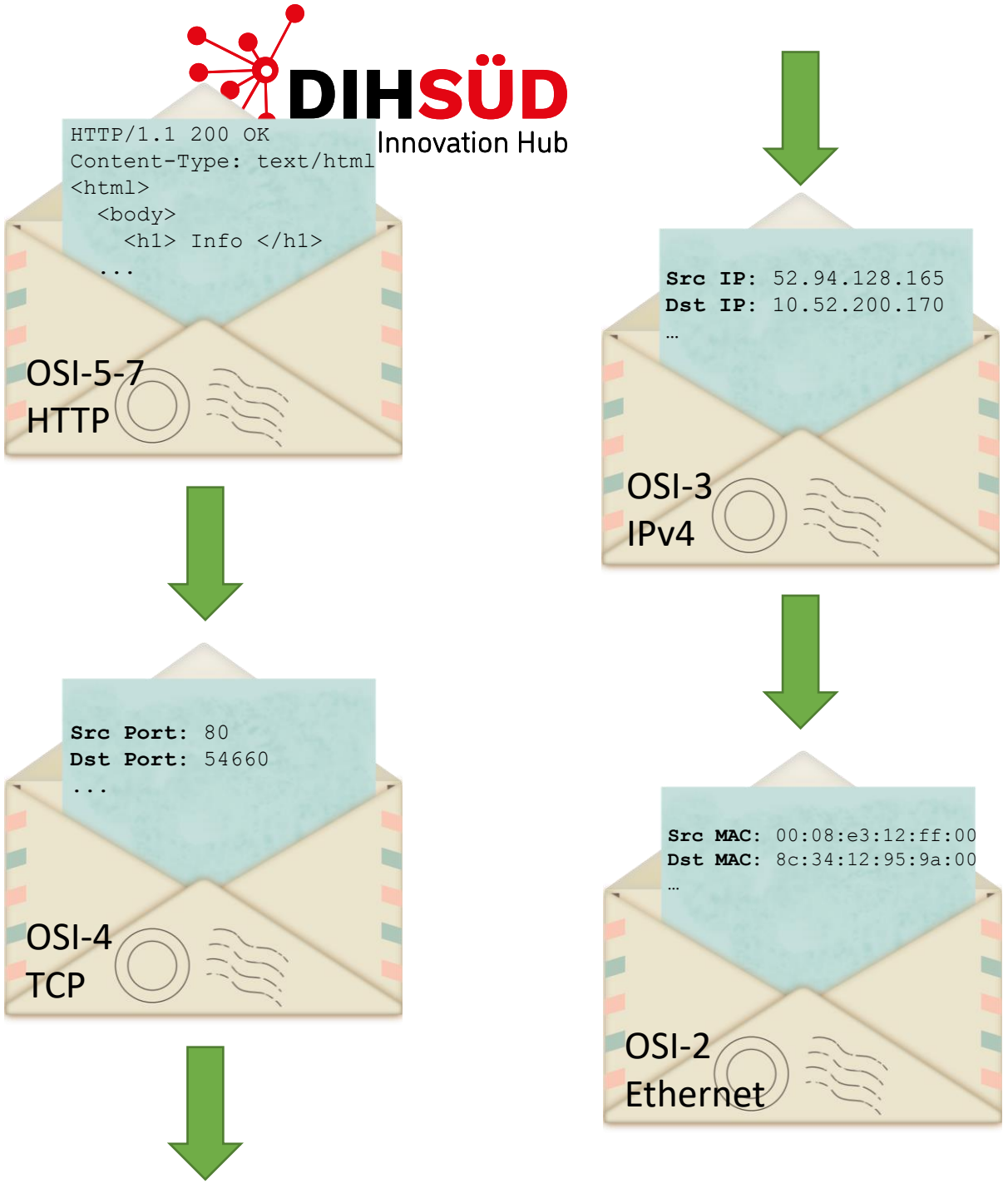
DIHSÜD Innovation Hub

FH JOANNEUM University of Applied Sciences

OSI Kapselung
Beispiel HTTP
Port 80

Server Response

Ein Paket vom ***Server*** *geht an den* ***Client*** *zurück*



Legende:

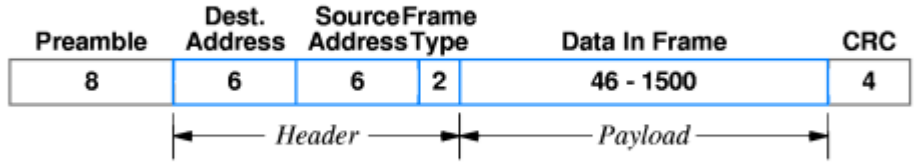
Src … Source (Quelle)
Dst … Destination (Ziel)
IP … Internet Protokoll
Logische Adressierung
MAC … Media Access Control
Hardware Adresse
Zugriff auf das Medium
Netzwerkkarte
Port … "Nummer" des Dienstes, der am Server angesprochen wird- bzw. Nummer für "Rück-Antwort" von diesem Dienst

Die physische Schicht – Physical Layer

- **Zweck**
  - Definiert Parameter der physischen Übertragung
  - Elektrische Kommunikation (Kodierungen)
  - Geräte / Schnittstellen
  - Automatic Crossover und Autonegotiation
- **Medien**
  - Kabel: Kupferkabel, Lichtwellenleiter
  - Funk (Mikrowelle und andere Teile des elektromagnetischen Spektrums)
  - Netzwerkkarte (NIC = Network Interface Card)
  - Andere Komponenten, die an das Netzwerk angeschlossen sind
- **Protokolle:** Ethernet (Physischer Teil)

Die Sicherungsschicht – Data Link Layer

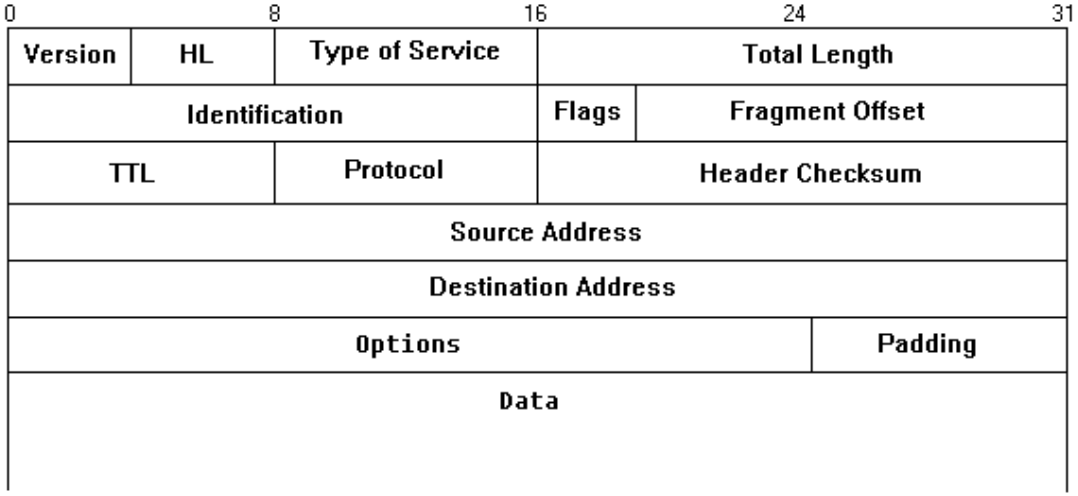
- **Zweck**:
  - Adressierung der Netzwerkknoten
  - Verbindet die Bits der physischen Schicht zu „**Frames**“
  - enthält Prüfinformation (CRC)
  - Fehlererkennung und –Behebung
  - Flusskontrolle
  - Zugriffskontrolle über gemeinsam genutzte Medien
- **Paketname**: Frame oder Rahmen
- **Protokolle:** HDCL, PPP, Ethernet (Protokollteil)



Ethernet Frame

Die Vermittlungsschicht - Network Layer

- **Zweck**:
  - Logische Adressen
  - Subnetting
  - Fragmentierung
  - Kontrolle mittels ICMP (Details),
  - **Routing**
- **Paketname**: Datagramm
- **Protokolle**: IPv4, IPv6



*IP **Datagram***

Zwischen Schichten 2 und 3

- Zuordnung physikalische auf logische Adressen (ARP – Address Resolution Protocol)

Die Transportschicht – Transport Layer

- **Zweck**:
  - Ende zu Ende Kommunikation
  - Verbindungslose/verbindungsorientierte Dienste
  - Gesicherte/ungesicherte Übertragung
  - Flusssteuerung
- **Paketname:** Segment (TCP), Datagram (UDP)
- **Protokolle**: TCP, UDP

Quell-Port			Ziel-Port
Sequenz-Nummer			
Acknowledgement-Nummer			
D. O.	Res.	Flags	Window-Größe
Check-Summe			Urgent-Pointer
Optionen/Füllbits			
Daten....			

TCP Header

Anwendungsorientierte Schichten

- Sitzungsschicht (Session Layer)
  - Sitzungen auf entfernten Systemen
  - Verbindungsaufbau und Abbau
  - Anmeldefunktionen

Protokolle & Anwendung:

- SMTP
  (inkl. MUA, MTA, Kommunikation), Push&Pull)
- DNS (allgemeine Funktion)
- E-Mail

Anwendungsorientierte Schichten

- Die Darstellungsschicht (Presentation Layer)
  - Darstellung von Daten
  - Konvertiert auszutauschende Daten in Standard-Formate
  - Kompression
  - Verschlüsselung

Protokolle & Anwendung :

- SMTP
  (inkl. MUA, MTA, Kommunikation), Push&Pull)
- DNS (allgemeine Funktion)
- E-Mail

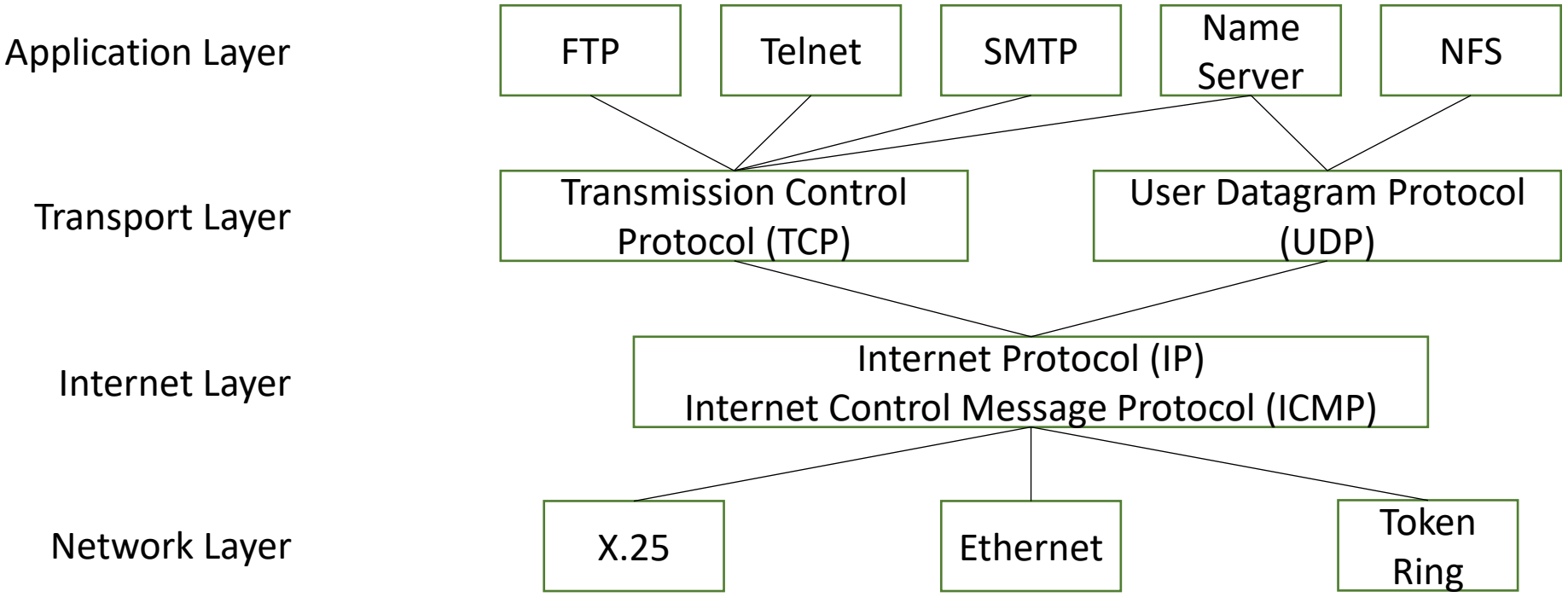
Anwendungsorientierte Schichten

- Die Anwendungsschicht (Application Layer)
  - Interaktion mit dem Benutzer
  - Stellt Interface für Befehle bereit
  - Implementierung in Anwendungs- und Serverprogrammen

Protokolle & Anwendung :

- SMTP
  (inkl. MUA, MTA, Kommunikation), Push&Pull)
- DNS (allgemeine Funktion)
- E-Mail

Protokolle im TCP/IP Stack



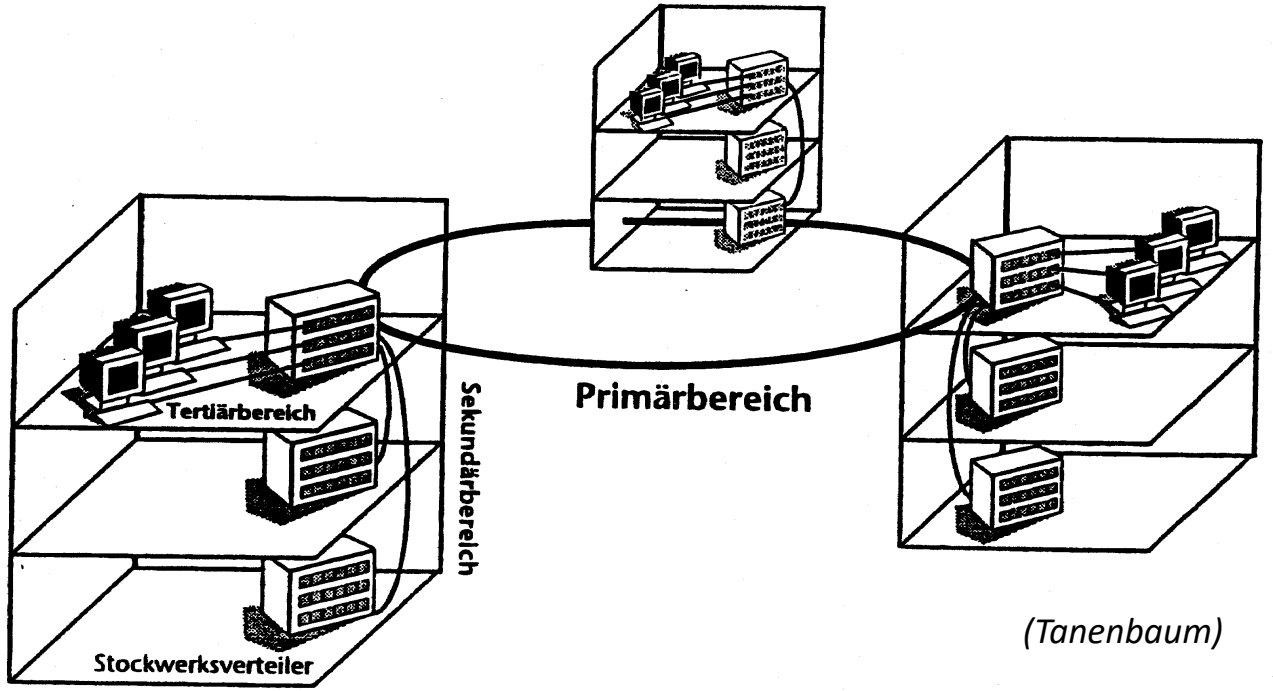
DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

OSI 1

Strukturierte Verkabelung

- **Primärverkabelung**
  - Zwischen Gebäuden
  - Vorwiegend Glasfaser
- **Sekundärverkabelung**
  - Etagen von Gebäuden
  - Switches als "Konzentratoren*"
  - Kupfer (TP**-Kabel) oder Glasfaser
- **Tertiärverkabelung**
  - Switches als "Konzentratoren*"
  - Kupferkabel (TP-Kabel)

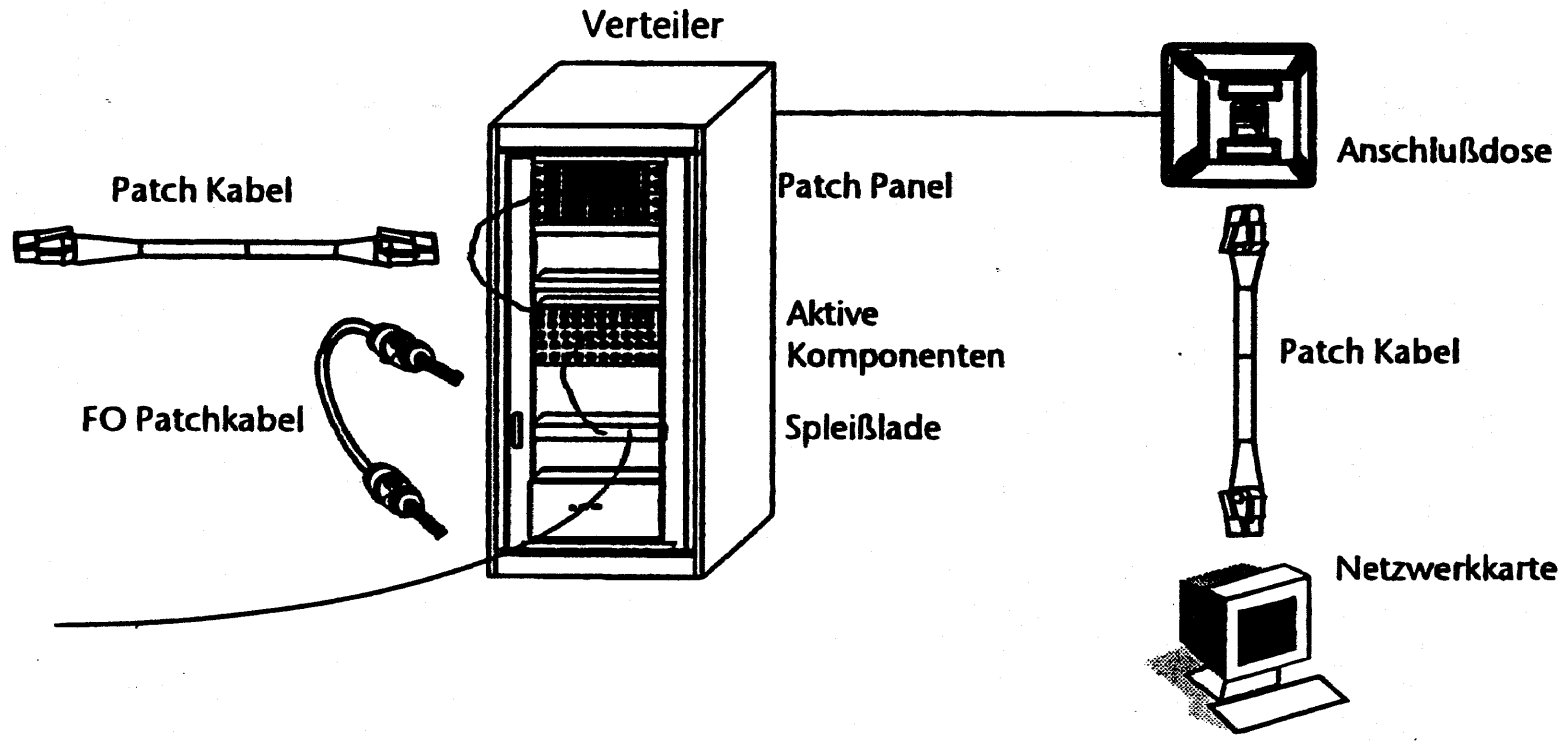


(Tanenbaum)

* Ein Konzentrator ist ein Gerät, das mehrere Leitungen einer bestimmten Datenrate auf eine Leitung mit größerem Durchsatz zusammenfasst und umgekehrt.

**Twisted-Pair Kabel – d.h. verdrillte Adernpaare im Kabel: Vorteil: Weniger Störungen durch Spannung – Robuster gegen physische Einwirkung- Ziehen, Drehen, usw.

19“ Schrank mit Patch Kabel



(Tanenbaum)

Ethernetkabel – „Patchkabel*“ (* Patchen = Zusammenschalten)

- Die wichtigsten Entwicklungen der „letzten“ Jahre
  - Fast Ethernet (100Base-T / 100Base-F)
  - Gigabit-Ethernet (1000Base-T)
  - 2,5/5-Gigabit Ethernet (2.5GBASE-T/5GBASE-T)
  - 10-Gigabit Ethernet 10GBASE-T
  - Gigabit Ethernet over plastic optical fiber (POF)
  - 25/40 Gigabit Ethernet (25G/40GBASE-T - bis 30 Meter)
  - 200/400 Gigabit Ethernet (200GbE/400GbE - fiber)

Benennung der Kabel:

<Zahl>BASE-<Typ>

Zahl → Datentransferrate
Typ → T … Twisted Pair
F … Fiber
X … Pins 4 Pairs
Full Duplex
(eXtended)

Standardisierung der Ethernet-Kabel

- Telecommunications Industry Association (TIA) als Teil der Electronic Industries Alliance (EIA) ist für Standards und auch für Ethernetkabel in **Kategorien**
- Die International Organization for Standardization (ISO) und die International Electrotechnical Commission (IEC) haben eine Einteilung der Kabel in **Klassen**

Kategorien lt. TIA

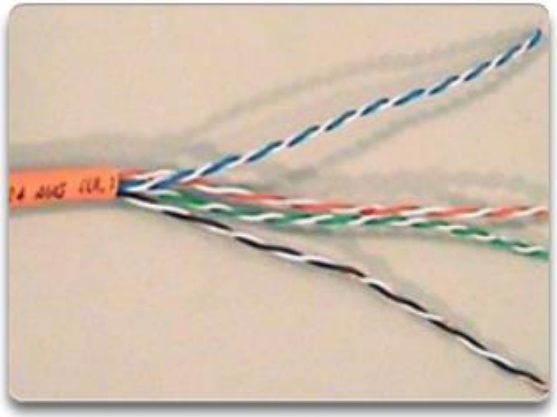
Cat1 → 0,4MHz Telefon, ISDN
Cat2 → 4MHz

Cat3 →16MHz →10Mb/s
Cat4 →20MHz →16Mb/s

Cat5 →125MHz Baudrate→ 100Mb/s
→ Kodierung 4B5B&MLT3 (*)
(Cat5e$_{nhanced}$ → 1000Mb/s)

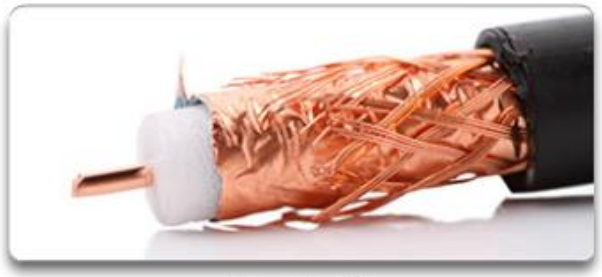
Cat6 →250MHz
Cat7 →600MHz
Cat7A →1000MHz

Kupferkabel als Übertragungsmedium



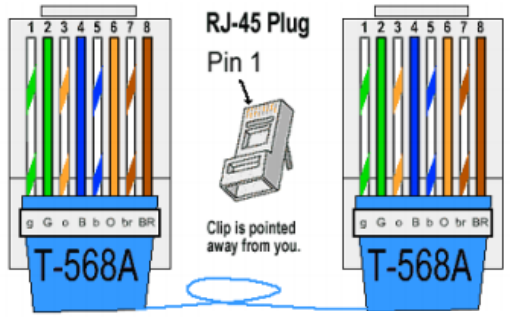
Unshielded Twisted-Pair (UTP) cable

Shielded Twisted-Pair (STP) cable

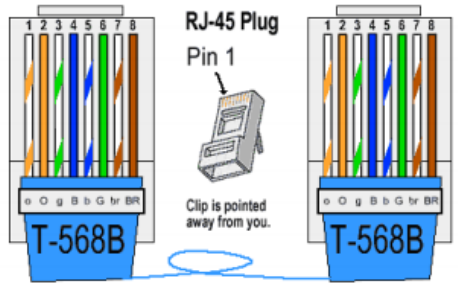


Coaxial cable

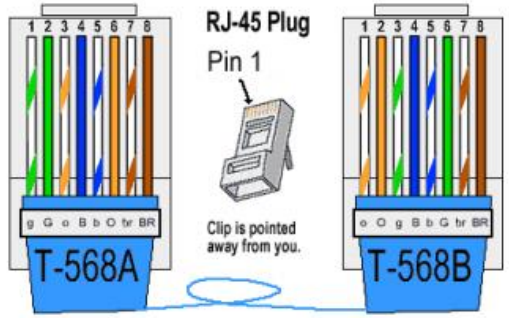
T-568A Straight-Through



T-568B Straight-Through



RJ-45 Crossover Ethernet Cable



Automatic Crossover

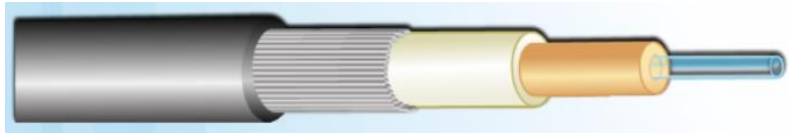
- Automatische MDI*/MDI-X Konfiguration ist als optionales Feature im 1000BASE-T Standard definiert.
- DH. dass “straight-through” Kabel wahrscheinlich immer zwischen Gigabit fähigen Interfaces funktionieren werden.
- Die Notwendigkeit für Cross-Over Kabel wird dadurch eliminiert.

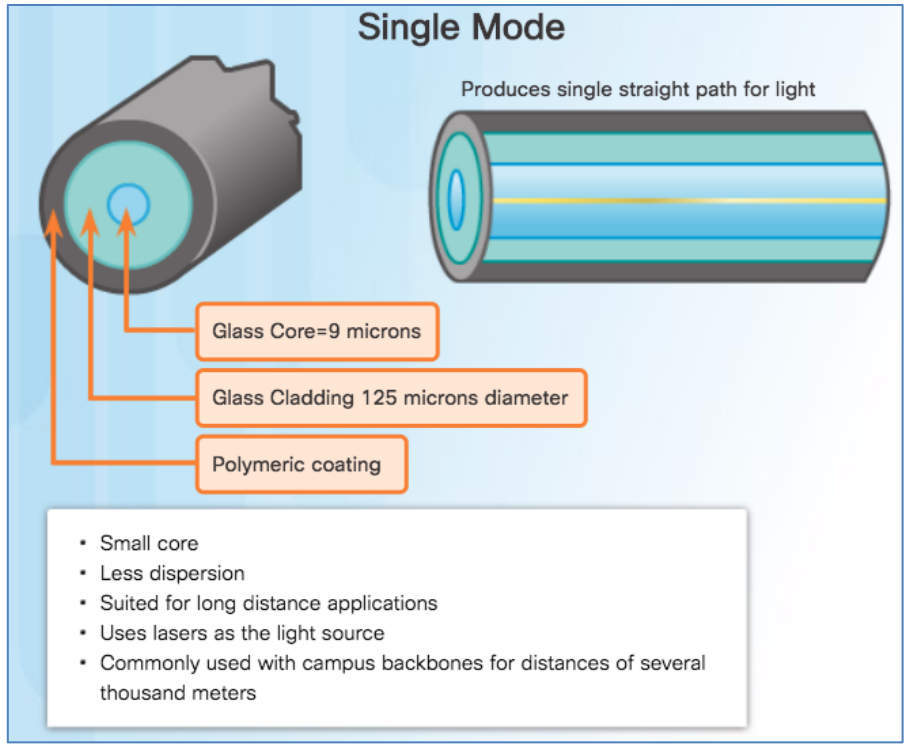
*Medium Dependent Interface

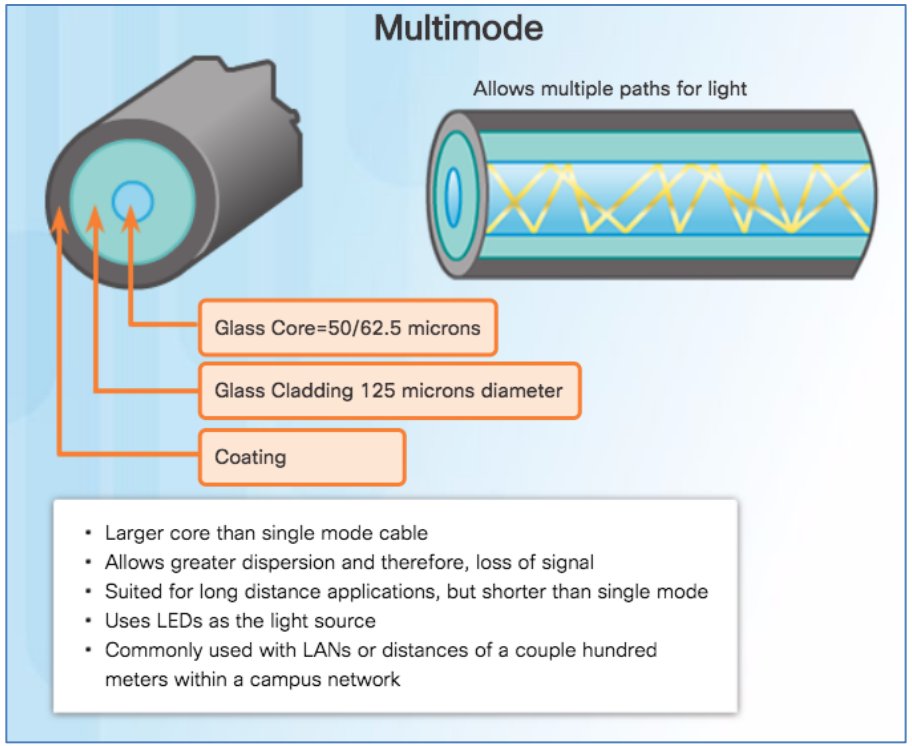
„Autonegotiation“

- Ist eine Ethernet Prozedur nach der 2 verbundene Geräte gemeinsame Verbindungseinstellungen treffen, wie zum Beispiel Geschwindigkeit und Duplex Modus.
- Autonegotiation (ANeg) kann zwischen Geräten mit
  - unterschiedlichen Übertragungsraten (zB.: 10 Mbit/s und 100 Mbit/s) und
  - verschiedenen Duplex Modi (half duplex und full duplex) und/oder
  - verschiedenen Standards mit der gleichen Geschwindigkeit verwendet werden.
- Jedes Gerät deklariert seine Eigenschaften und mögliche Operationsmodi.
- Die zwei Geräte wählen den best-möglichen Modus und einigen sich drauf diesen zu verwenden.

Lichtwellenleiter





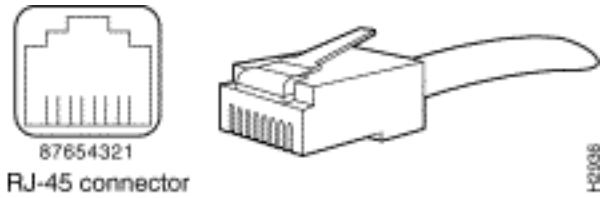


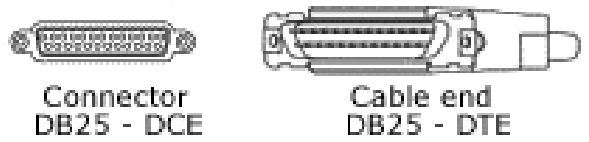
Kupfer versus Lichtwellen

Eigenschaften	UTP Kabel	Lichtwellenleiter
Max. Bandbreite	40GB/s	400GB/s
Mögl. Kabellänge	1-100m	1-100,000m
Anfälligkeit gegen Störungen	Niedrig	Hoch
Kosten	Niedrig	Hoch
Aufwand Installation	Niedrig	Hoch

Serielle Verbindungen (zwischen Routern)

- RS-232 Standard
  - DB-25/DE-9 Connector
  - RJ-45 Connector
- Wird zwischen Routern auch "Back-to-Back" Verbindung genannt!
- "Data Communications Equipment" (DCE)
  - Gibt den Takt vor. D.h. man muss am Gerät eine „clock rate“ einstellen.
- "Data Terminal Equipment" (DTE)





Console Cable Connection

WLAN – IEEE 802.11

- WLAN nutzt elektromagnetische Signale die Binärdaten representieren. Diese Daten warden über Funk übertragen
- WLAN Probleme:
  - **Empfangsgebiet:** Mauern, Rohre, elektrische Verkabelung in Gebäuden können die Ausbreitung der Funkwellen beeinträchtigen.
  - **Störungen:** Andere Funk Signale (z.B. WLAN Geräte in der Nähe, Mikrowellen) können das eigenen Signal stören.
  - **Security:** Jeder kann Datenverkehr mitlesen – Auch nicht authentifizierte Benutzer.
  - **Geteiltes Medium:** Nur ein Gerät kann gleichzeitig

Wireless Access Point (AP): Empfängt Signale aller verbundenen Geräte und leitet sie über ein kabelgebundenes Medium weiter.

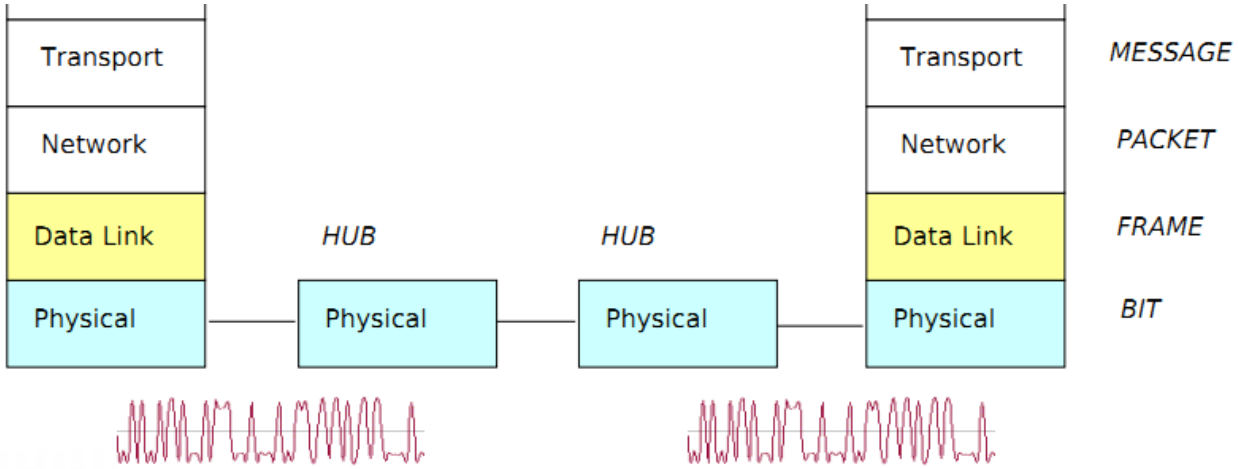
Wireless NIC Adapter: Erlaubt Kommunikation über WLAN für einen Host.

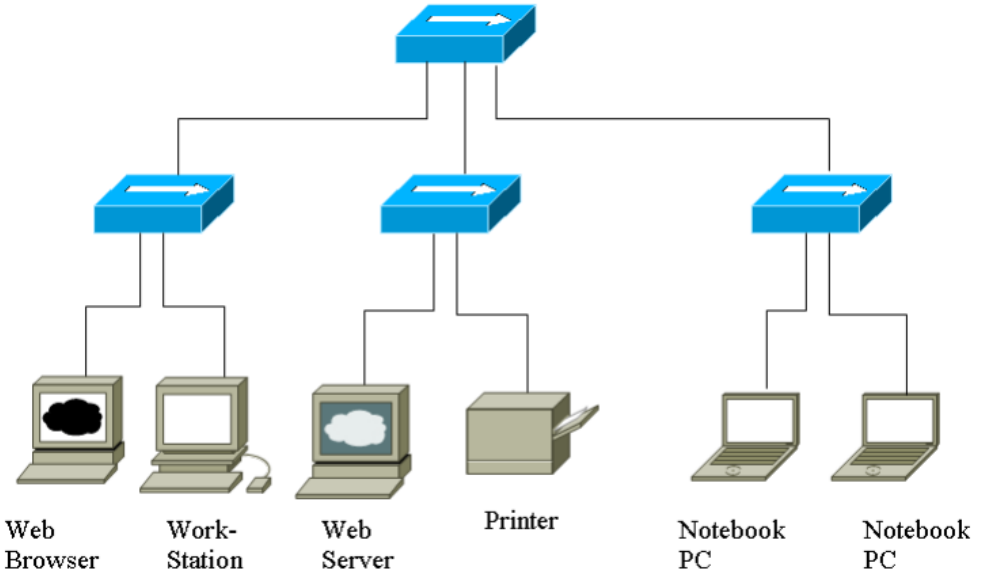
Komponenten – Repeater & Hubs

CISCO Symbols

10BASE-T Hub (small hub)

100BASE-T Hub





DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

OSI 2

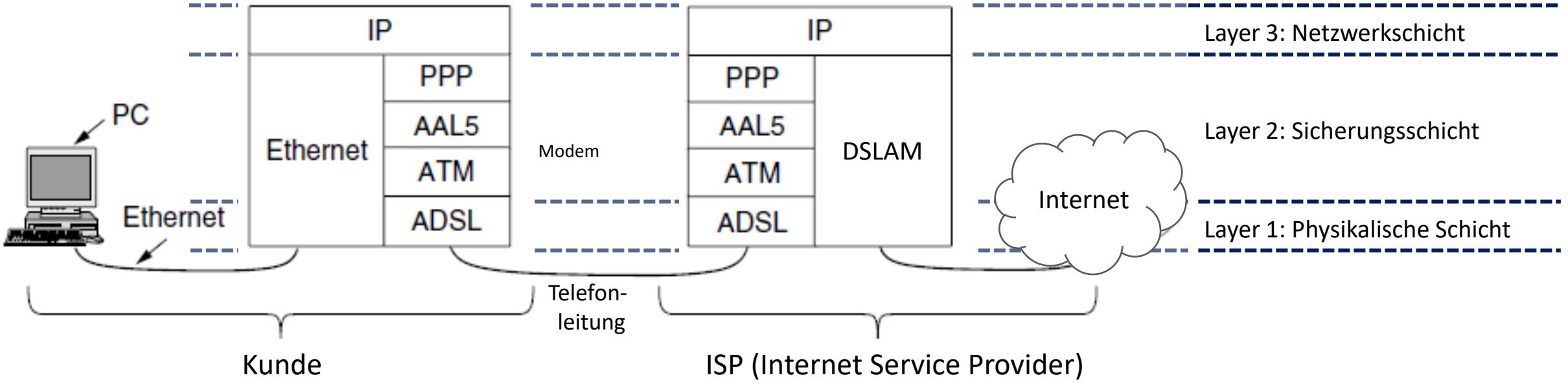
Überblick

- Senden und Empfangen von Informationseinheiten- so genannten **Rahmen (Frame)**, in welchen Daten der oberen Schichten verpackt sind.
- **Probleme**, die gelöst werden müssen sind …
  - **Fehlerhafte Bits** bei der Übertragung
  - Unterschiedliche **Datenraten** der Übertragungsmedien(Kabel, Funk, Lichtwellenleiter, …)
- **Lösungen** sind …
  - **Prüfsumme**
  - **Flußkontrolle**

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Kommunikation über ADSL Modem



http://netgear.com

http://www.zyxelguard.com/IES-5000.asp

IP *Internet Protocol*
PPP *Point to Point Protocol*
ADSL *Asymmetric Digital Subscriber Loop*
ATM *Asynchronous Transfer Mode*
AAL5 *ATM Adaptation Layer 5*
DSLAM *Digital Subscriber Line Access Multiplexer*

vgl. Computer Networks, Tanenbaum, 5th Edition, 2011, Seite 249

Rahmen (Frames) erstellen

4 Möglichkeiten (nur zur Vollständigkeit):

- **Byte Count (Bytes zählen)**
- **Flag Bytes** (**Hinweis-Bytes**) mit **Byte-Stuffing**
- **Flag Bits (Hinweis-Bits**) mit **Bit-Stuffing**
- **Coding Violation (Kodierungsverletzung)** in der physischen Schicht

vgl. Computer Networks, Tanenbaum, 5th Edition, 2011, Seite 197

Fehler im Datenstrom

- **Error Correcting Codes** (Fehlerkorrektur)
  - Bei fehleranfälligen Medien (WLAN)
  - Redundante Daten notwendig
  - Forward Error Correction (FEC)
- **Error Detecting Codes** (Fehlererkennung)
  - Bei wenig fehleranfälligen Medien und wenn eine erneute Übertragung schnell ist / wenig kostet (Lichtwellenleiter)
  - Parity
  - Prüfsummen
  - Cyclic Redundancy Check (CRC)
- Beispiel: **Hamming Code**

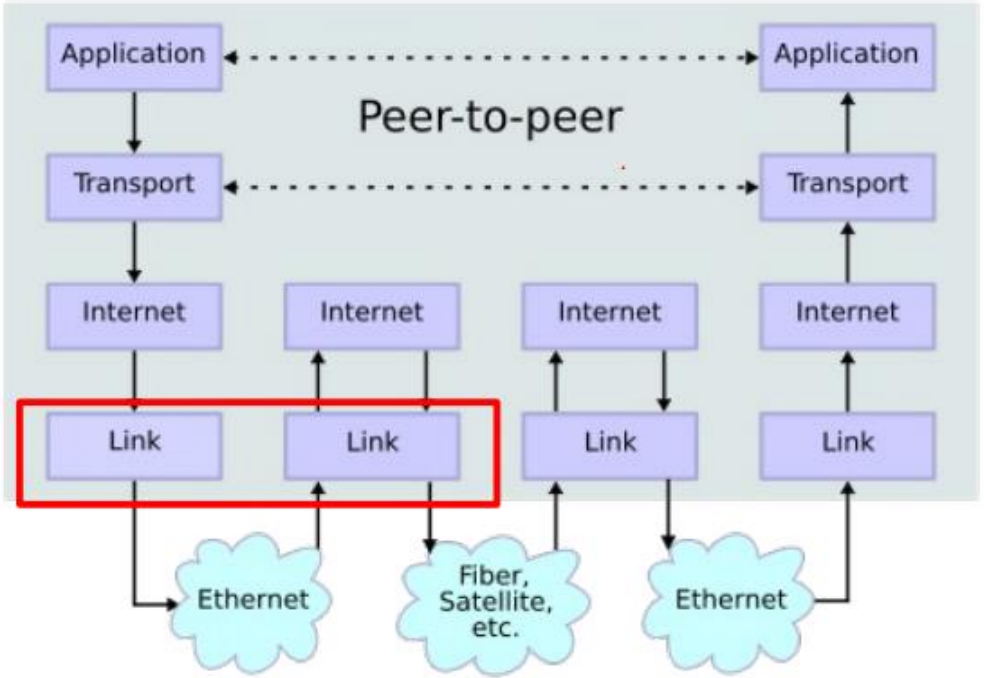
Flußkontrolle

- **Feedback-based** (Feedbackbasiert)
  - Stop & Wait (HDLC)
- **Priority-based** (Priorisierungsbasierend)
  - Ethernet
- **Rate-based** (Datenratenbasiert)
  - Sliding-Windows (Schiebefenster)
  - TCP (Transportschicht!)

Schicht 2 **Protokolle**

- **PPP** (byte orientiert)
- **HDLC** (bit orientiert)
  - Sliding Windows (*Diese Flußsteuerung ist genauer in Schicht 4 beschrieben*)
  - Zuverlässige Verbindung
- **Ethernet**
  - Ethernet II (DIX)
  - Ethernet 802.3
- Und viele mehr ….

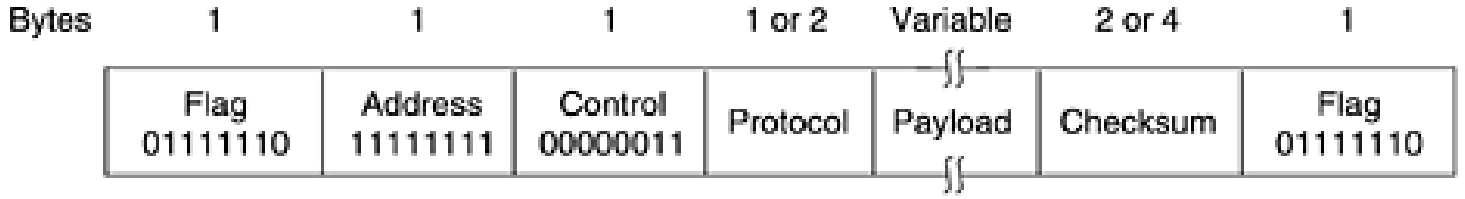
  (WLAN, I^2C, Spanning Tree Protocol, FDDI-FiberDistributedDataInterface, …)



Punkt zu Punkt Protokolle

- **HDLC** (High Level Data Link Control)

- **PPP** (Punkt-zu-Punkt Protokoll)
  - Verwendung: Router zu Router oder Heimanwender zu ISP
  - RFC1661++



Ethernet

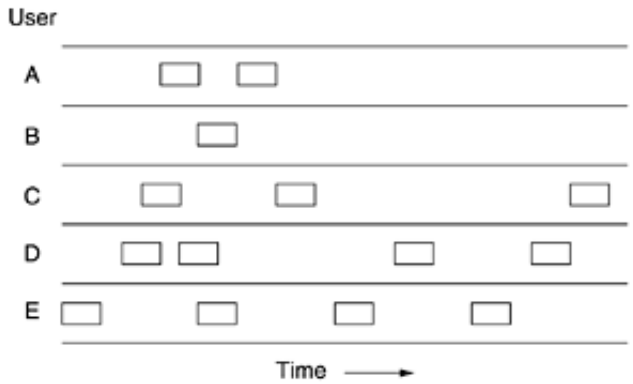
- **Spezifikation** von Funktionalitäten in
  - **physischer Schicht** (Layer 1)
  - **Sicherungsschicht** (Layer 2)
- Packt das **IP Datagramm** in einen **Ethernet Frame (Rahmen).**
- Fügt die **physikalischen Adressen** der Quelle (MUA) und des Ziels (MTA von Jane) dazu. (**MAC - Media Access Control Adressen**)
- Versendet die **Frames über das Netzwerkinterface**.
- "**Ether**"(dt. Äther) , weil dieses Protokoll **nicht auf ein Übertragungsmedium beschränkt** ist: Medien wie Kabel, Luftschnittstelle, Lichtwellen, usw. sind möglich
- Arbeitet innerhalb einer **Kollissionsdomäne**
- Ursprünglich von DEC, Intel und Xerox (DIX) spezifiziert, dann auch in IEEE802.3

Collision Domain (Kollisionsdomäne)

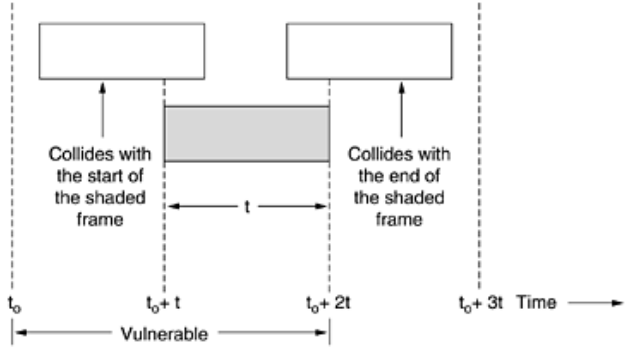
- Wenn Netzwerkgeräte um ein **gemeinsames Übertragungsmedium konkurrieren** spricht man von einer Kollisionsdomäne
- Teil des Ethernet II Standards
  - Bei **Voll-Duplex** geschehen **keine Kollisionen** mehr
  - Kollisionen zwischen **Netzwerkkarte und Switch Port bei Halb-Duplex**
  - Aus dem folgenden **10GB Ethernet Standard herausgefallen**
- **Wichtig bei WLAN**, weil hier das **gleiche Medium (Funk)** verwendet wird.

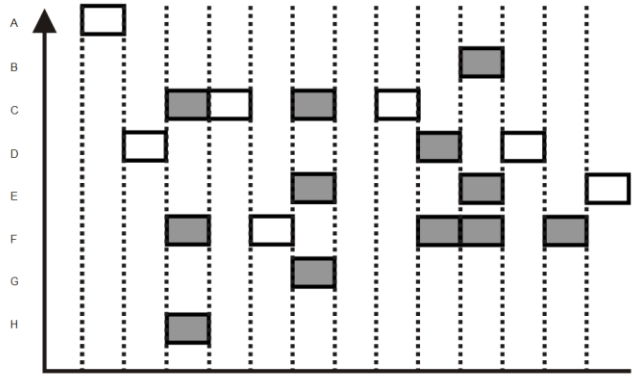
Media Access Control (Broadcast Domain): Geschichte

- **Aloha Protokoll**
  - Problem: **Kollisionen**!
  - **Effizienz: ca 17%**
- **Slotted Aloha Protokoll**
  - Alle Rahmen sind gleich groß und haben angepasste Sendeintervalle ("Time-Slots")
  - Übertragung beginnt mit neuem "Time-Slot"
  - Kollisionen werden von allen erkannt
  - Horchen: Slot frei? Wenn ja, senden, wenn keine Kollision, dann weiter senden
  - Problem: **Bandbreite**!
  - **Effizienz: ca 33%**



vgl. Computer Networks, Tanenbaum, 5th Edition, 2011





http://upload.wikimedia.org/wikipedia/commons/7/7a/Slotted_ALOHA.svg

Media Access Control (Broadcast Domain): Ethernet
Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection (CSMA/CD)

- Erkennen (=Sense), in welchem **Zustand** sich das **Übertragungsmedium** (=Carrier) befindet: **Frei oder Belegt**
- Da sich **mehrere Teilnehmer in der Kollisionsdomäne** ein Übertragungsmedium teilen spricht man von "Multiple Access"
- Wenn mehrere Teilnehmer gleichzeitig senden überlagern sich ihre Signale. Diese **Kollisionen werden erkannt**. (Detection)

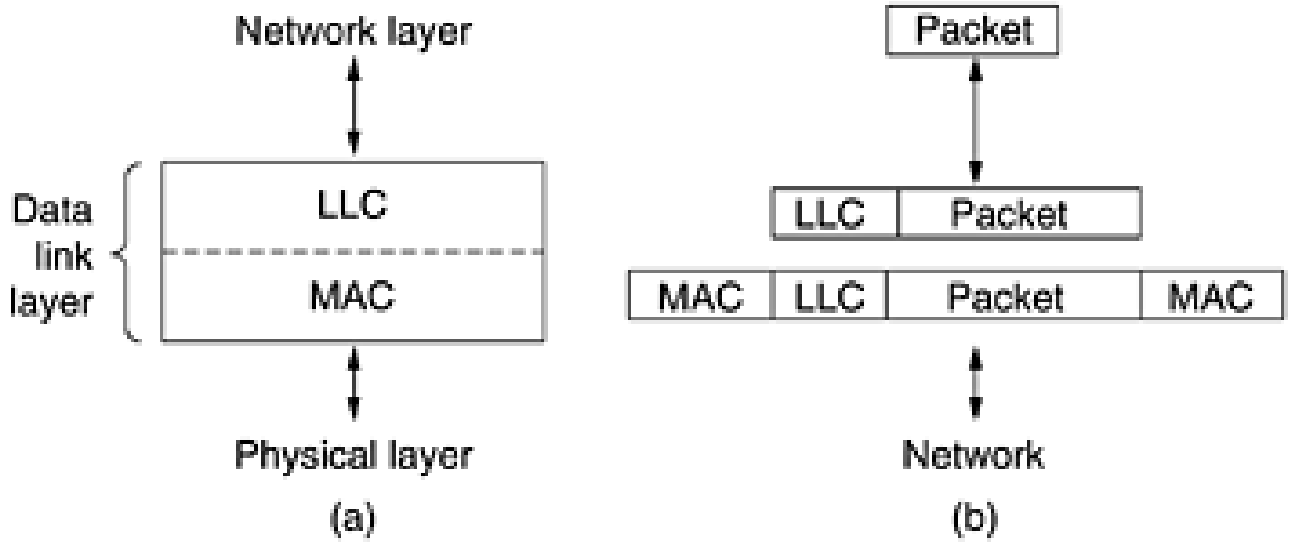
CS Carrier Sense „Vor dem Senden abhören“
MA Multiple Access
CD Collision Detect „Abhören während des Sendens“

Überwachung der Übertragung

- **Verbindungsorientiert**:
  Lösung: Steuerrahmen zurücksenden, der über positive/negative Übertragung berichtet.
- **Störungen:** (‚welche Rahmen verschwinden lassen)
  Lösung: Ein „Timer“ sorgt für diese Überwachung.
- **Rahmen kommt mehrmals an:**
  Lösung: Nummerierte Rahmen sorgen für richtige Reihenfolge und wirken Redundanzen entgegen!

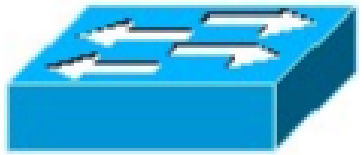
Ethernet **Logical Link Layer** (LLC) Teilschicht

- Folge- und
- Bestätigungsnummer
- Unzuverlässig, bestätigter oder zuverlässiger verbindungsorientierte Verbindung

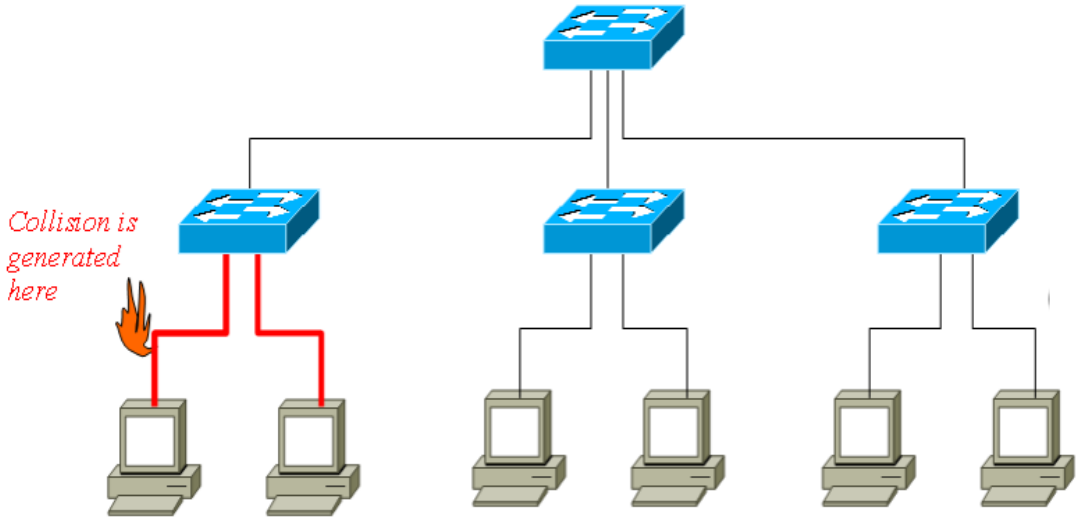


vgl. Computer Networks, Tanenbaum, 5th Edition, 2011

Switch (Schicht 2 Netzwerkverteiler)



Symbol
(Cisco)



(Cisco)

Kollisionen kommen nur zwischen Netzwerkgerät und Switchport **im Half-Duplex Modus** zustande

Frame Forwarding (Weiterleitung der Rahmen)

- Am Switch existiert eine **MAC Adress-Tabelle, anhand der er Nachrichten zielgerichtet weiterleitet**
- Die Tabelle wird **nach Einschalten des Switchs** anhand der Nachrichten **aufgebaut**!
- Wenn der Switch **keine Adresszuordnung** hat, geht er in den **„Flooding“ Modus** und sendet das Paket **wie ein Hub an alle**
- Wenn das **Ziel am selben Port** liegt, wird **nicht weitergeleitet** (**„Filtering“**)
- Wenn die **Adresstabelle überläuft**, schaltet der Switch in den **„Flooding“ Modus**.

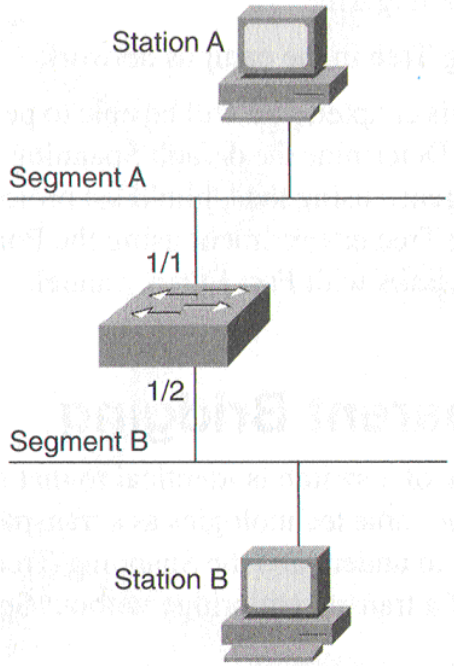
Erweiterte Funktionen von "managed" Switches"

- **Ports ein-** und **aus**schalten
- **Verbindungsgeschwindigkeit** und Duplex Modi einstellen
- **Prioritäten** für Ports festlegen
- **MAC Adressen filtern**
- Das **Spanning Tree Protocol (STP)**
- Überwachen des Geräts und der Ports über das **Simple Network Management Protokoll (SNMP)**
- **Port Spiegelung**
- **Link Aggregation** („bonding“/“trunking“)
- **Virtuelle LANs einsetzen (VLANs)**

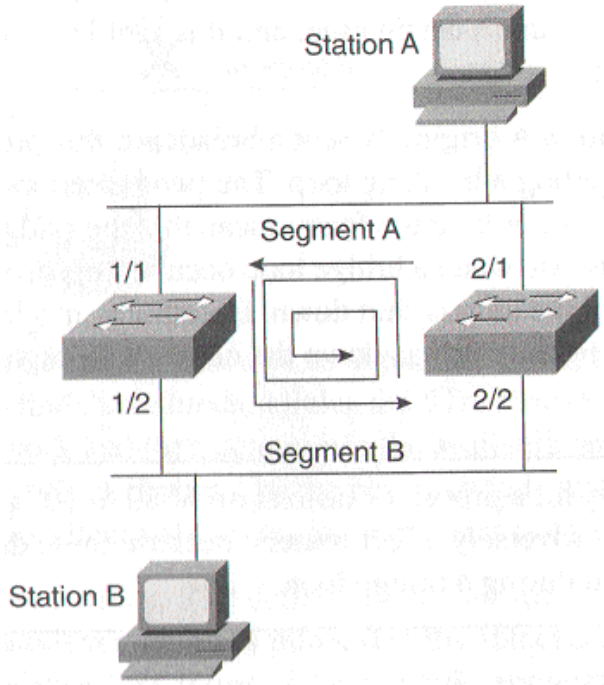
DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

„Bridging“



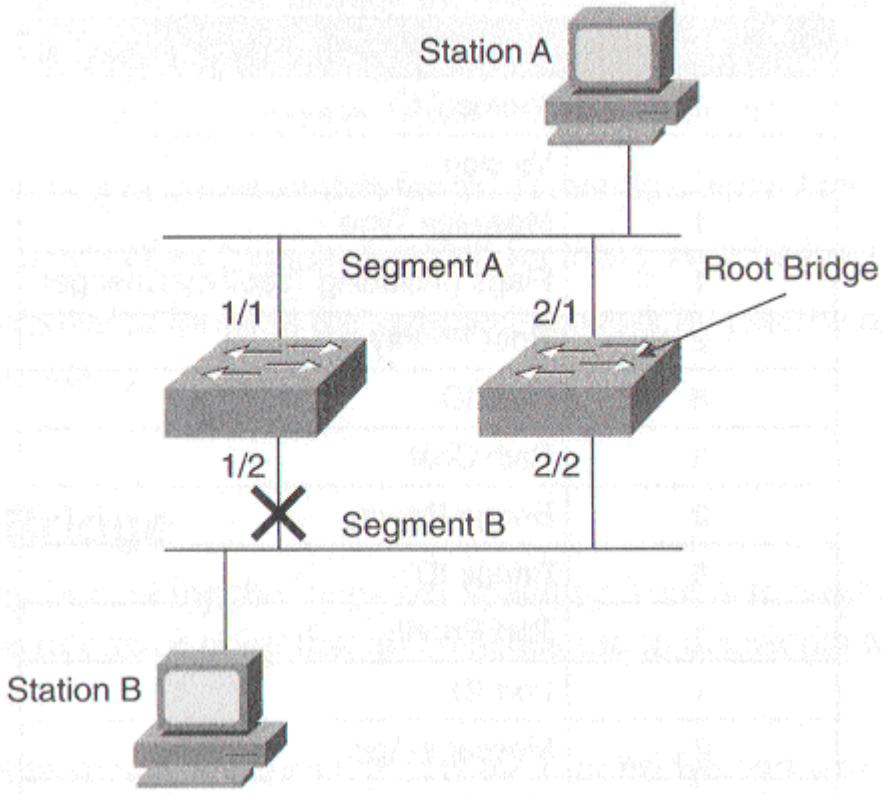
Transparent



Schleife

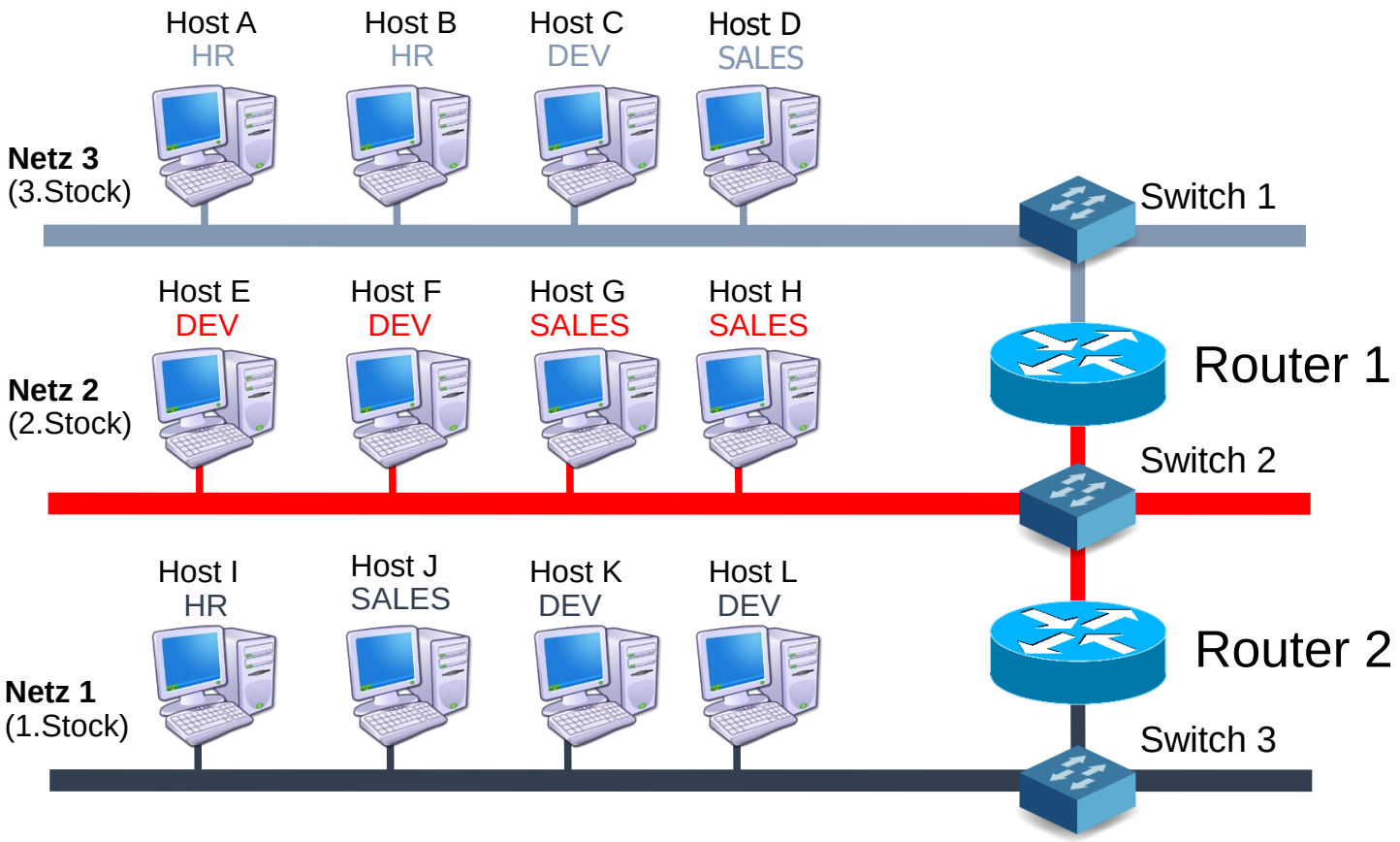
Spanning Tree Protocol

- Dient der **Eliminierung von Schleifen**
- Um das zu erreichen definiert das „Spanning Tree Protokoll“ eine **Baumstruktur, die alle Switches eines Subnetzes umspannt**.
- Es wird eine „**Root Bridge**“ definiert von der aus der Baum aufgespannt wird.



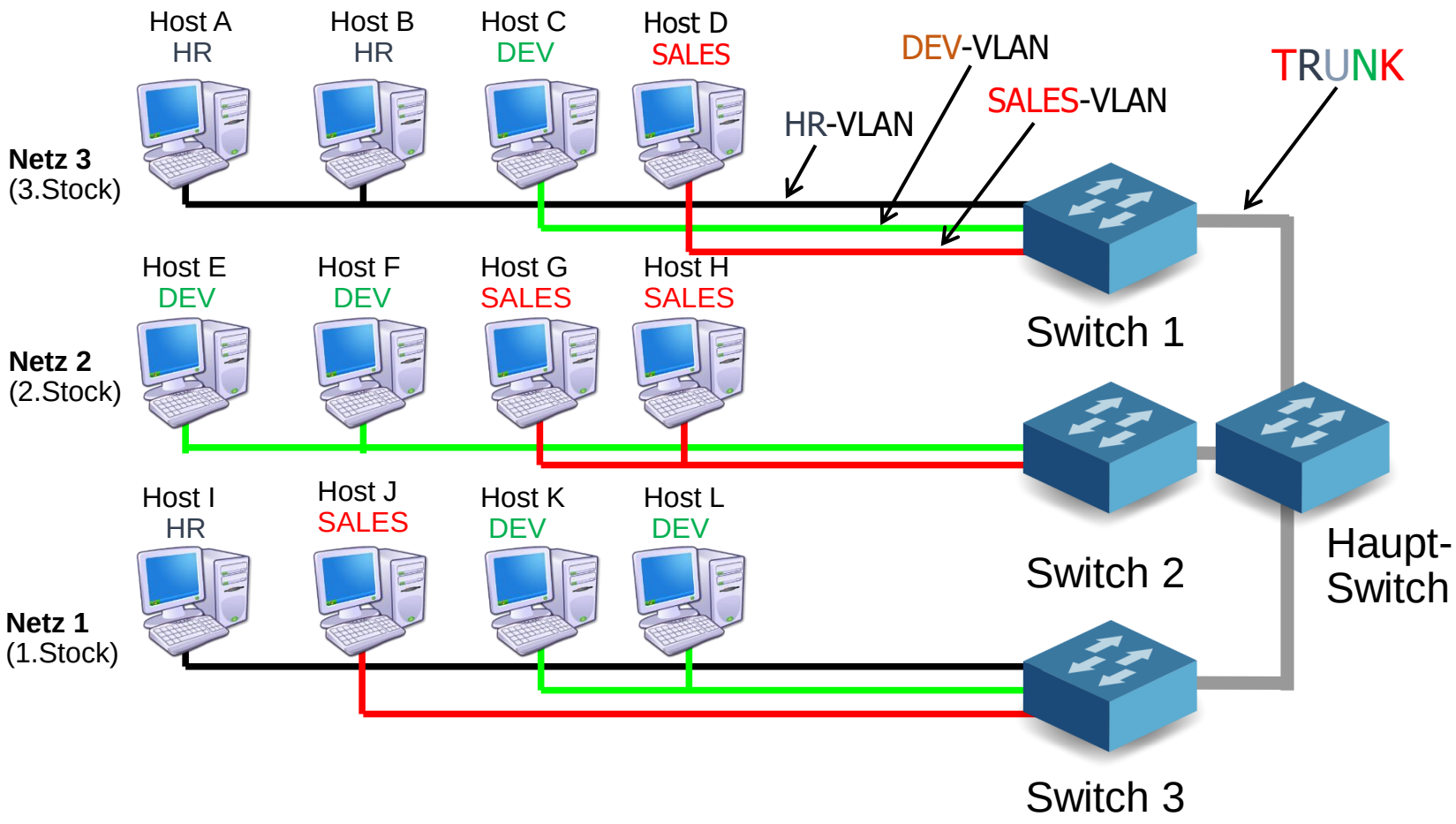
Segmentierung mit Routern

- Jedes Segment ist ein **individuelles Subnetz unabhängig** von der **Funktion der beteiligten Hosts**
- Das Subnetz ist **durch die physikalische Anordnung** definiert



Segmentierung mit Switches

- Mittels **Virtuellen LANs (VLANs)**
- Jedes **VLAN** ist eine **eigene Broadcast-Domain**
- Vorteile:
  - **Security**
  - **Segmentierung**
  - **Flexibilität**



DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

OSI 3

Routing

- Routing beschreibt die **Auswahl eines Pfades** (Netzwerk-) um Pakete über Netzwerkgrenzen zu senden.
- Es gibt verschiedene **Routing Protokolle**, die entweder innerhalb eines betrieblichen Netzwerks oder außerhalb Anwendung finden.
- Ein Router ist ein Computer, der mehr als eine Netzwerkkarte hat und dadurch Pakete von einem Netzwerk in das andere weiterleitet. Die Weiterleitung passiert nach Regeln und wird “Routen” (Routing) genannt.
- Die hierarchische Struktur des Internets verlangt nicht, dass ein Router die ganze Route wissen muss.
- Einige Router wissen nur über ihre eigenen Netzwerke und über Standardrouten Bescheid (**Default Gateway**).

IP- Das Internet Protokoll

- Stellt ein Adressierungsschema für Netzwerke und Rechner dar

- IP Adressen kommen in zwei Geschmacksrichtungen
  - IPv4 (antik, 32 bit) → 4,3 Milliarden Adressen
  - IPv6 (neu, 128bit) → 340 Sextillionen Adressen

- Zusammen mit anderen Protokollen zuständig für den Transport von Paketen über vordefinierte Routen

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Anzahl IP Adressen – IPv4 vs. IPv6

32 bit =

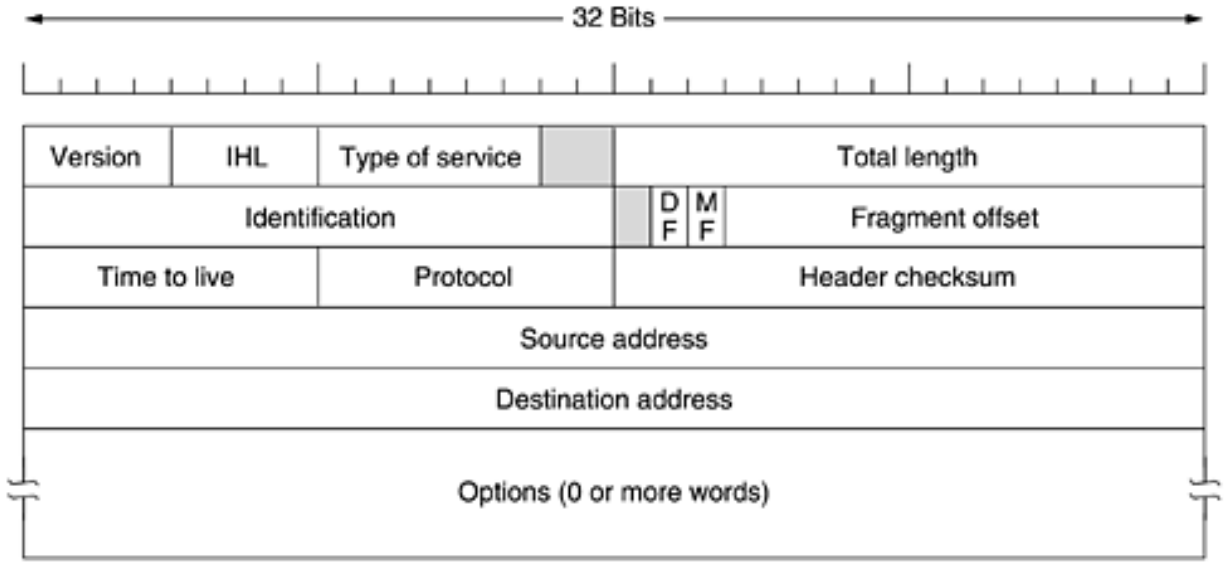
4 294 967 296

128 bit =

340 282 366 920 938 463 463 374 607 431 768 211 456

IPv4 Protokoll

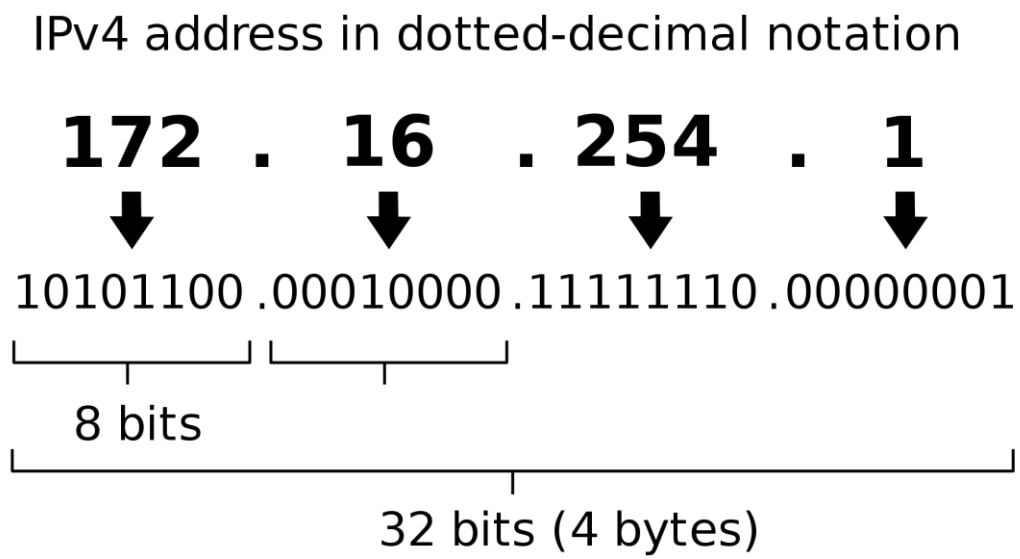
- **Version**
- Header Länge*
- Dienstart
- Größe des Datagramms
- Identifikation für Fragmente
- Entweder hat das Paket keine oder mehrere Fragmente
- Transport Prozess Protokoll

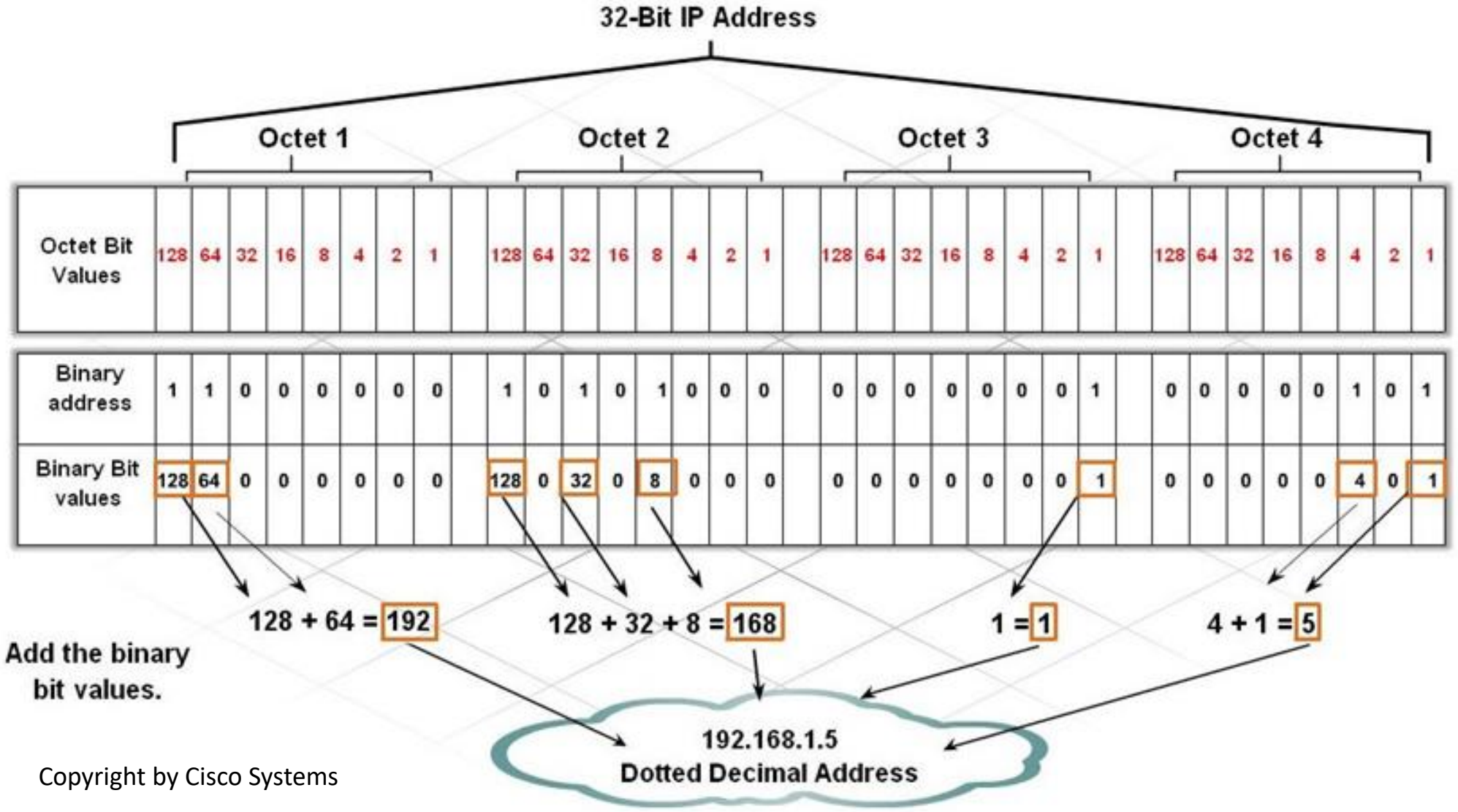



```
Internet Protocol Version 4, Src: 10.52.200.203, Dst: 40.101.76.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x2802 (10242)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x8ae7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.52.200.203
    Destination: 40.101.76.130
```

Adressierung in IPv4

- Die IP Adresse besteht aus einem **32 Bit** Integer Wert
- Aus Gründen der Lesbarkeit werden die **vier Byte Blöcke** der IPv4 Adresse **dezimal dargestellt**.
- Beispiel: 89.105.0.1 =
  - 1500053505 (dez)
  - 59 69 00 01 (hex) oder
  - 10110010110100100000000000000001 (bin)
- Jede reguläre IP Adresse besteht aus einem **Host**anteil und einem **Netzwerk**anteil





IP Adresse Aufbau

192.168.0.1/24

- Netzwerkanteil – Netzwerk 192.168.0.0
- Hostanteil
- Subnetzmaske

Die Netzmaske - Subnetzmaske

- 32 bit langer integer Wert
- 4 Byte Oktette in dezimal dargestellt
- z.B. 255.255.255.0 oder /24 (Anzahl der 1er Bits)
- Dient der Teilung der Rechner und der Netzwerke
- Aufteilung Host-/Netzwerkanteil der IP Adresse wird durch ein bitweises UND (AND) errechnet

Beispiel 1/3

- IP Adresse: 192.168.199.4
- Netzmaske: 255.255.255.0 oder /24

- IP Adresse in hexadezimal: `C0A8C704`
- Netzmaske in hexadezimal: `FFFFFF00`

- IP Adresse binär: `11000000 10101000 11000111 00000100`

- Netzmaske binär: `11111111 11111111 11111111 00000000`

Beispiel 2/3

```
Network                          | Host
---------------------------------+---------
11000000 10101000 11000111 | 00000100  address
11111111 11111111 11111111 | 00000000  netmask
---------------------------------+---------
11000000 10101000 11000111 | 00000000  result
```

Beispiel 3/3

- Ergebnis: `11000000 10101000 00000000 00000000`
- In Dezimal: 192.168.199.0
- Gegebene IP: 192.168.199.4 (aus Slide 77)
- Range: 192.168.199.1 -192.168.199.254
- Netzwerk Adresse: 192.168.199.0
- Broadcast Adresse: 192.168.199.255

Die Klassengesellschaft

- Früher wurden Netzwerke in Klassen eingeteilt.

- Mögliche Klassen:

- 255.0.0.0 → Class A
- 255.255.0.0 → Class B
- 255.255.255.0 → Class C

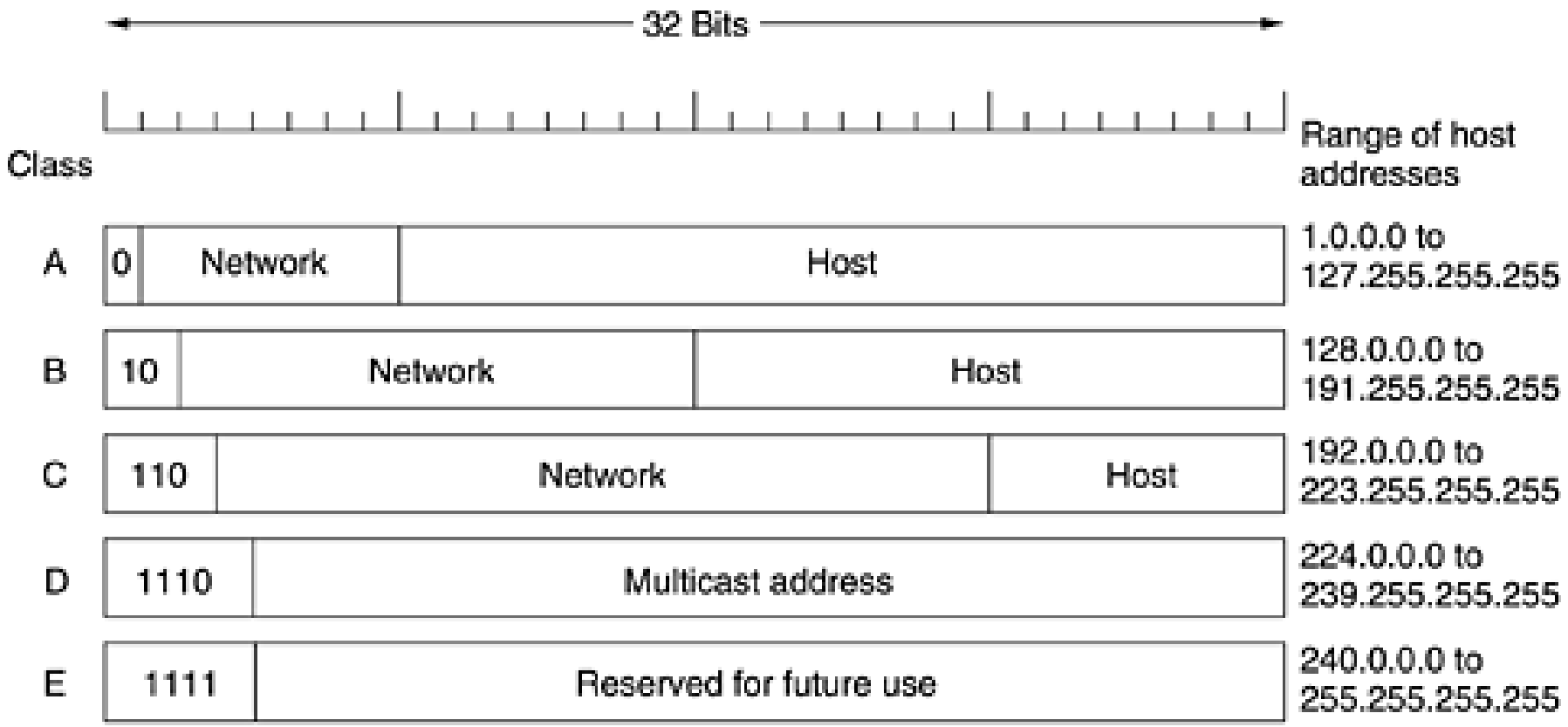
Die Klassengesellschaft (Cont.)

- Class A :
  - MSB (Most significant Byte) immer „0“
  - 126 mögliche Netzwerke mit je 16 777 214 Hosts

- Class B:
  - MSB immer „10“
  - 16 384 Netzwerke mit je 65 534 Hosts

- Class C:
  - MSB immer „110“
  - 2 097 152 Netzwerke mit je 254 Hosts

IPv4 Adressklassen



(Tanenbaum: Computer Networks)

IPv4 Adressklassen

Class	Subnetzmaske	Anzahl Netzwerke	Anzahl Adressen	Adressbereich
A	255.0.0.0	128 (2^7)	2 147 483 648	1.0.0.0 – 126.0.0.0 *
B	255.255.0.0	16 384 (2^14)	1 073 741 824	128.0.0.0 – 191.255.0.0
C	255.255.255.0	2 097 152 (2^21)	536 870 912	192.0.0.0 – 223.255.255.0
D (multicast)	-	-	-	224.0.0.0 – 239.255.255.255
E (reserviert)	-	-	-	240.0.0.0 – 255.255.255.255

* 127.0.0.0 – 127.255.255.255 sind reserviert für Loopback Adressen

Klassenlose Gesellschaft: **CIDR**

- Classless Inter Domain Routing (CIDR)
  - Auflösen der strikten Subnetzmasken
  - Variable Length Subnet Mask (VLSM)

Notation	Subnetzmaske binär	Subnetzmaske dezimal	Nutzbare Host-Adressen
/8	11111111.00000000.00000000.00000000	255.0.0.0	16 777 214
/9	11111111.10000000.00000000.00000000	255.128.0.0	8 388 606
/10	11111111.11000000.00000000.00000000	255.192.0.0	4 194 302
/11	11111111.11100000.00000000.00000000	255.224.0.0	2 097 150

Berechnung Anzahl möglicher Hosts

- **$N=2^n-1-1$**
  - Bei n=0 Bits in der Netzmaske
  - Abziehen von Broadcast-/Netzwerkadresse

- *Beispiel*
  - 255.255.224.0 → /19 → 11111111.11111111.111*00000.00000000*$_2$
  - 0 Bits: n = 32 Bits – 19 Einsen = **13** Nullen
  - N = 2^{13}-2 = 8192 -2 = 8190

Spezielle IP Adressen

- **0.0.0.0**
  bezieht sich auf das aktuelle Netzwerk – diese Adresse wird auch beim Booten verwendet.

- **255.255.255.255**
  Broadcast Adresse, mit der an alle Netzwerke gesendet wird.
  (Oft deaktiviert- und wenn dann mit einem gültigen Netzwerk verwendet!)

- **127.x.x.x**
  „Loopback“ Adressierung zum lokalen Testen

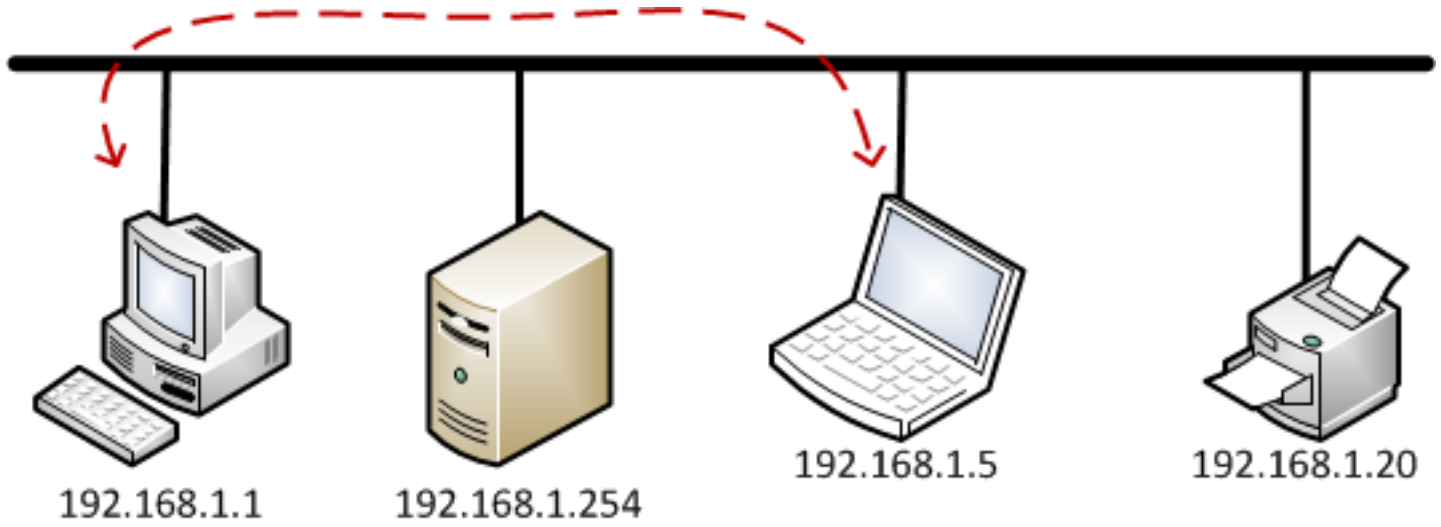
Subnetze – Private Adressbereiche

- Für die Nutzung innerhalb eines LANs
  - Network Address Translation (NAT) für Verbindung ins Internet

CIDR-Notation	Adressbereich	Anzahl nutzbarer Adressen
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 214
172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 574
192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 534

Subnetze – Private Adressbereiche

PC und Notebook können miteinander kommunizieren, weil sie im selben Netzwerk sind.

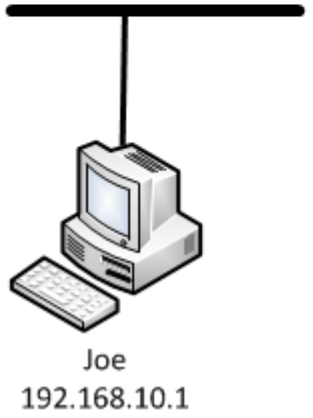


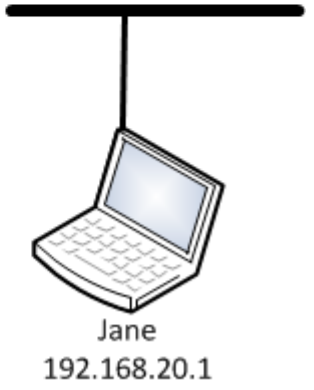
Subnetze – Private Adressbereiche

- Was aber, wenn Joe und Jane in unterschiedlichen physikalischen Netzwerken sind?

- Eine Verbindung ist notwendig!

- Router – zur Weiterleitung in andere Netzwerke



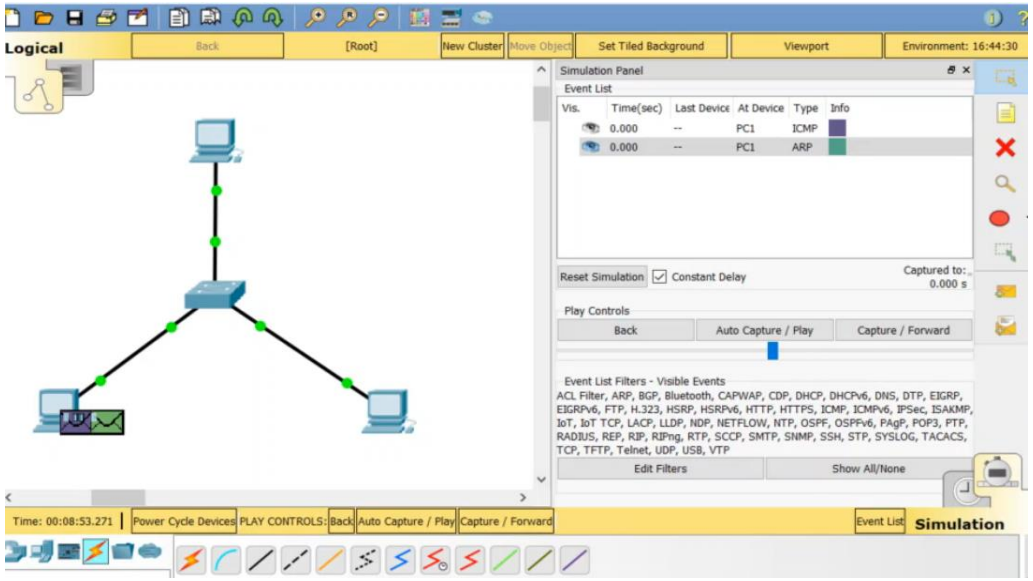


DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

ARP – Address Resolution Protocol

- Auflösung von **IP Adresse** (Layer 3) zu **MAC Adresse** (Layer2)
- Mein Host kennt die MAC Adresse des Ziels nicht
- Video: Ping an Host im selben Netzwerk



ARP – Request

```
▼ Ethernet II, Src: LcfcHefe_60:13:9a (8c:16:45:60:13:9a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: LcfcHefe_60:13:9a (8c:16:45:60:13:9a)
      Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: LcfcHefe_60:13:9a (8c:16:45:60:13:9a)
      Sender IP address: 10.52.200.203
      Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Target IP address: 10.52.1.254
```

ARP – Reply

```
Ethernet II, Src: Cisco_ff:fd:2c (00:08:e3:ff:fd:2c), Dst: LcfcHefe_60:13:9a (8c:16:45:60:13:9a)
    Destination: LcfcHefe_60:13:9a (8c:16:45:60:13:9a)
    Source: Cisco_ff:fd:2c (00:08:e3:ff:fd:2c)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Cisco_ff:fd:2c (00:08:e3:ff:fd:2c)
    Sender IP address: 10.52.1.254
    Target MAC address: LcfcHefe_60:13:9a (8c:16:45:60:13:9a)
    Target IP address: 10.52.200.203
```

ARP – Address Resolution Protocol

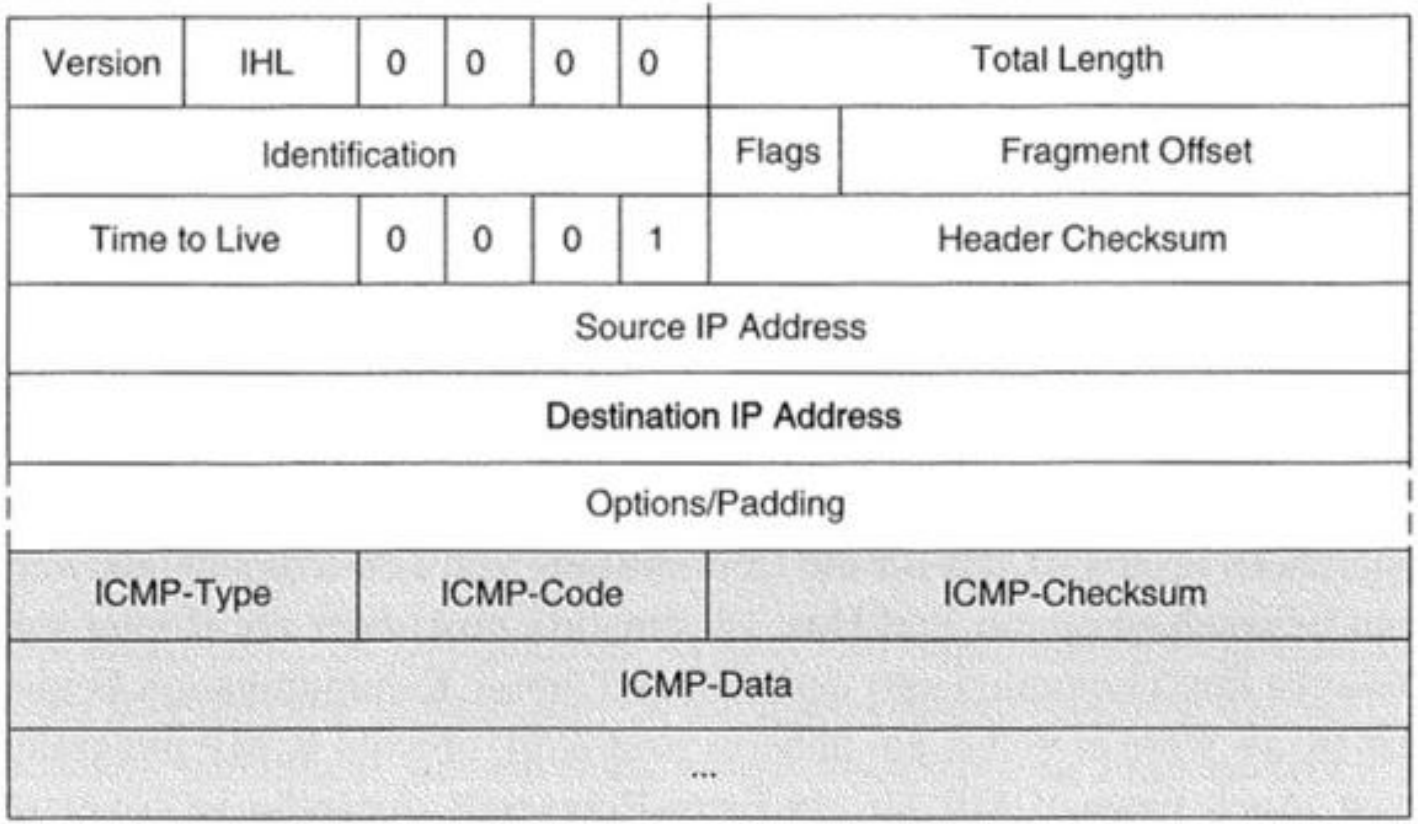
- Nützliche Befehle:
  - **`arp -a`**
    Zeigt alle Einträge an, die im ARP Cache sind. „arp –g“ funktioniert auch!
  - **`arp -d`** *<IP Adresse>*
    Damit kann man Einträge löschen bevor ihre Gültigkeit abläuft.
  - **`arp -s`** *<IP-Adresse> <MAC-Adresse>*
    Zum Hinzufügen von Einträgen.

- RARP - Reverse Address Resolution Protocol
  - IP Adresse auf Grund einer MAC Adresse herausfinden. Obsolet durch moderne DHCP Dienste, die viel mehr bieten.

ICMP

- Internet Control Message Protocol – RfC 792
- Layer 3 – gekapselt innerhalb des IP
- Ziele:
  - Fehler melden
  - Testen
  - Informationsbeschaffung
- Charakteristika:
  - Bestandteil vom IP
  - Meldet Fehler im Netzwerk, trägt aber nicht zur Verlässlichkeit des Netzwerks bei
  - Eigene Fehler werden nicht berichtet (Damit keine Schleifen entstehen!)

ICMP im Datagramm



ICMP Nachrichtenfelder

- ICMP Type (8 bit)
  - Basiskategorie / Typ einer Nachricht
- ICMP Code (8 bit)
  - Unterkategorie
- ICMP Checksum (16 bit)
  - Prüfsumme aus Inhaltsfeld
- ICMP Data (Variable Länge)
  - Daten, die zum Beispiel Adressen sein können und zum Packet passen, welches die ICMP Nachricht enthält.

ICMP Fehlermeldungen

- Ziel nicht erreichbar (3, „Destination unreachable“) – Host oder Port
- Datenüberlauf der Quelle (4, „Source Quench“) – Puffer sind voll
- Umleitung (5, „Redirect“) - Info wegen Weiterleitung zu Routern
- Timeout (11,“Time (to live) exeeded“) – Zeit abgelaufen
- Konfigurationsproblem (12, „Parameter problem“) – ICMP fehlerhaft

ICMP - Informationen

- Echo Antwort (0, „Echo reply“)
  Echo Anfrage (8,“Echo request“) – „Ping“

- Zeitstempel (13, „Timestamp“)
  Zeitstempel Antwort (14, „Timestamp reply“)

- Information (15, „ Information “)
  Information Antwort (16, „ Information reply“)

- Adresse (17, „ Adresse “)
  Adresse Antwort (18, „ Adresse reply“)

ICMP - Ping

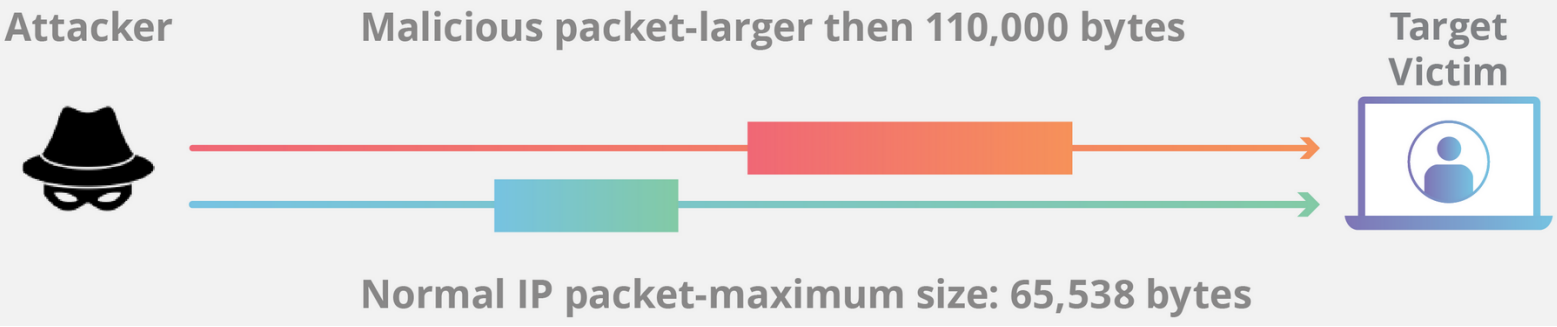
- Erreichbarkeit feststellen:
  Sender setzt eine ICMP Nachricht vom Typ 8 ab („echo (request)“)

- Der Empfänger sendet eine ICMP Nachricht vom Typ 0 zurück.

- Wenn keine Nachricht zurückkommt, dann …
  - Ist das Ziel nicht erreichbar.
  - Oder der Administrator hat ICMP abgestellt! (Nicht so gut…)

ICMP – „Ping of Death“

- Die TCP/IP Implementierungen früherer Betriebssysteme hatten Probleme mit Paketen >65535Bytes → Crash wegen Buffer Overflow
- Das konnte relativ einfach erreicht werden:
  - Senden von IP Fragmenten
  - Das letzte Fragment hat einen Offset von 65528 und ein Datenfeld >= 1200Bytes
  - Bei Zusammensetzen beim Opfer: IP Paket > 65553 → R.I.P
- Kann mit jedem IP Paket erreicht werden.



https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

ICMP - Traceroute

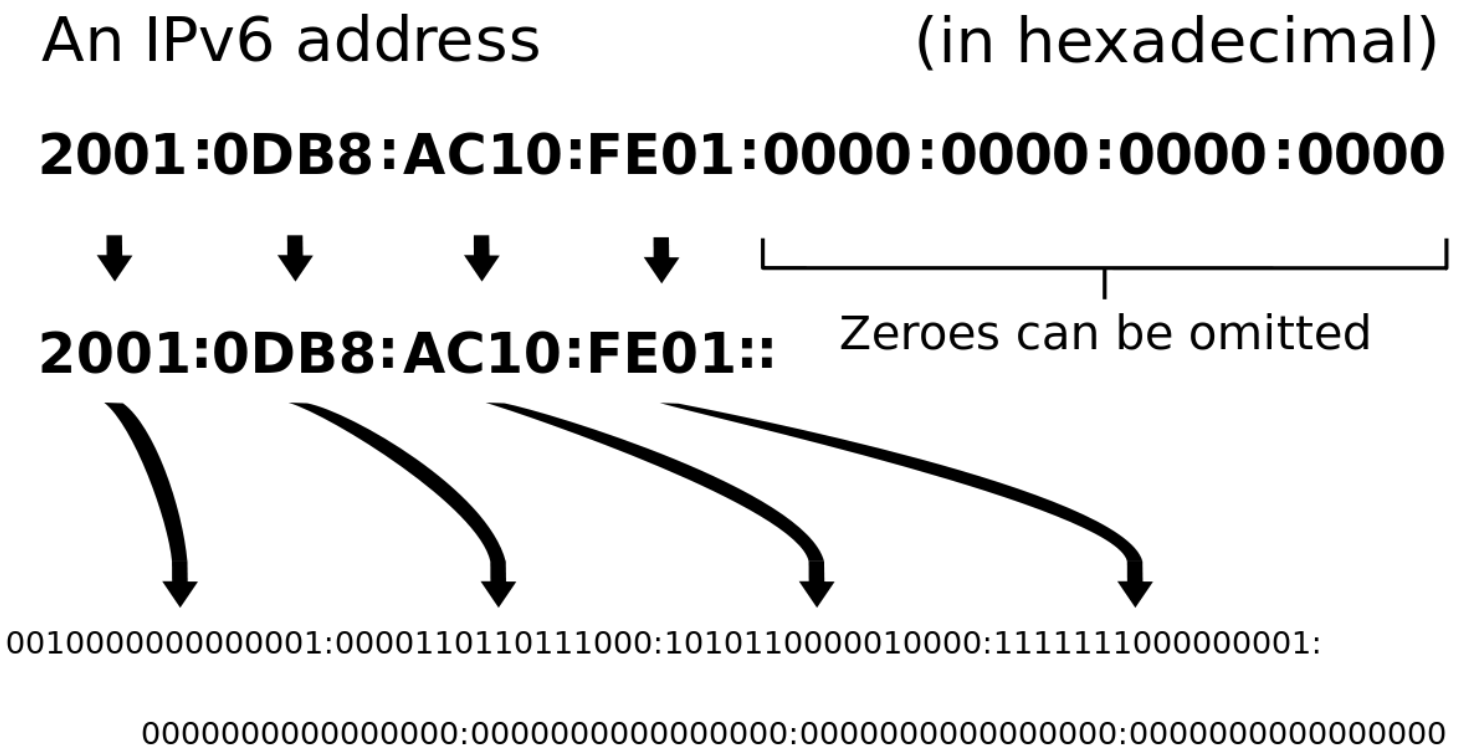
- Sender versendet ein ICMP Paket mit der TTL = 1
- Der nächste Router (Hop) rechnet 1 runter: ICMP „Time exceeded“
- Sender versendet ein ICMP Paket mit der TTL = 2
- Der übernächste Router (Hop) erreicht TTL = 0: ICMP „Time exceeded“

- Dieser Vorgang wird fortgeführt bis:
  - Das Ziel gefunden wurde oder
  - Keine brauchbare Antwort mehr kommt

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

IPv6 Adressen



https://upload.wikimedia.org/wikipedia/commons/thumb/7/70/Ipv6_address_leading_zeros.svg/1200px-Ipv6_address_leading_zeros.svg.png

Unterschiede IPv4 zu IPv6

- Options
  - Nicht in IPv6 vorhanden.
  - Für IPv6 werden Optionen im Extension Header gesendet. (Header Chaining)

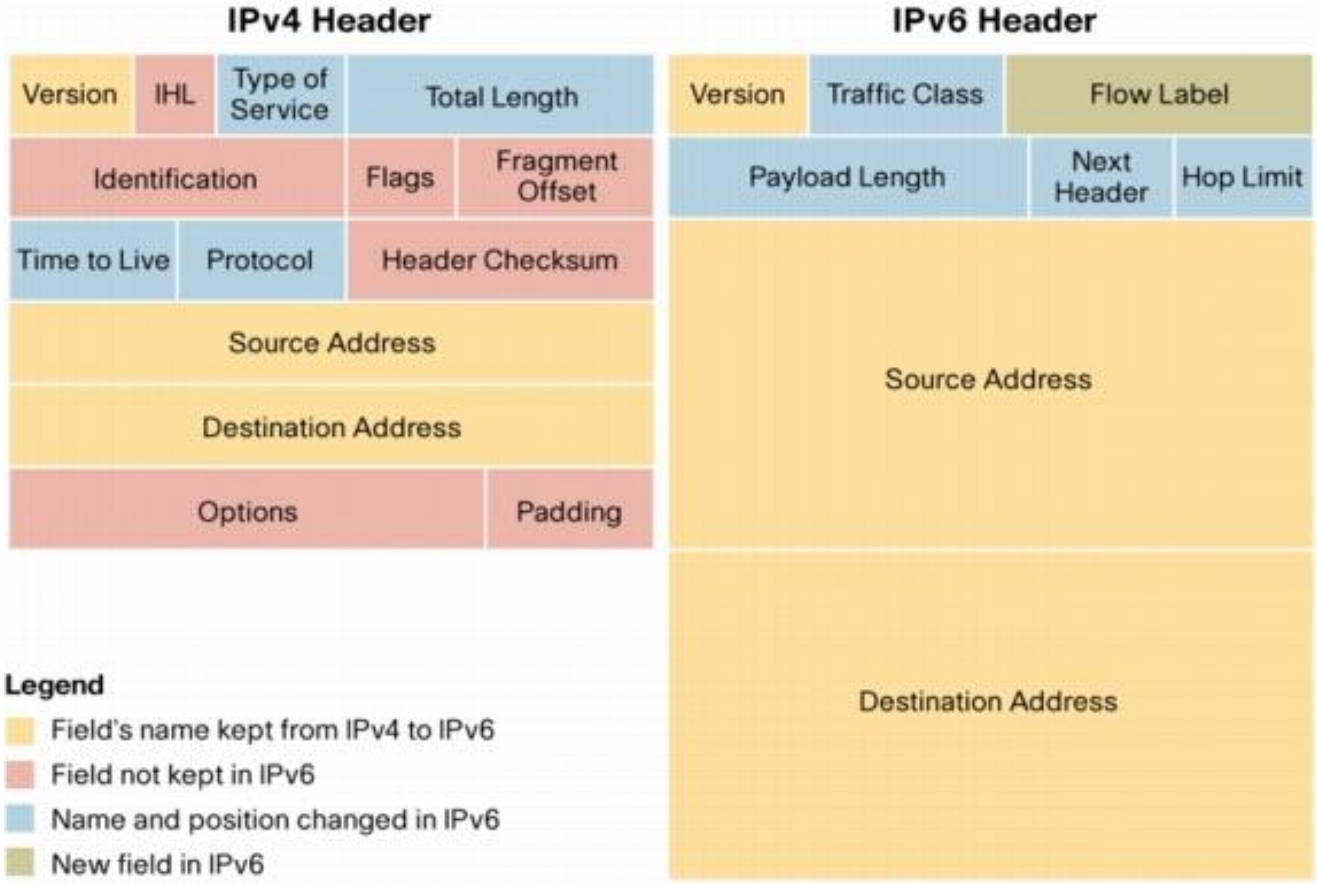
- Optionale Header werden in IPv6 über das „Next Header“ Feld definiert.

- Fragmentierung ist in IPv6 nur über den Sender und nicht über Router erlaubt. Daher ist die Bestimmung der MTU entlang des Pfads Pflicht.

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

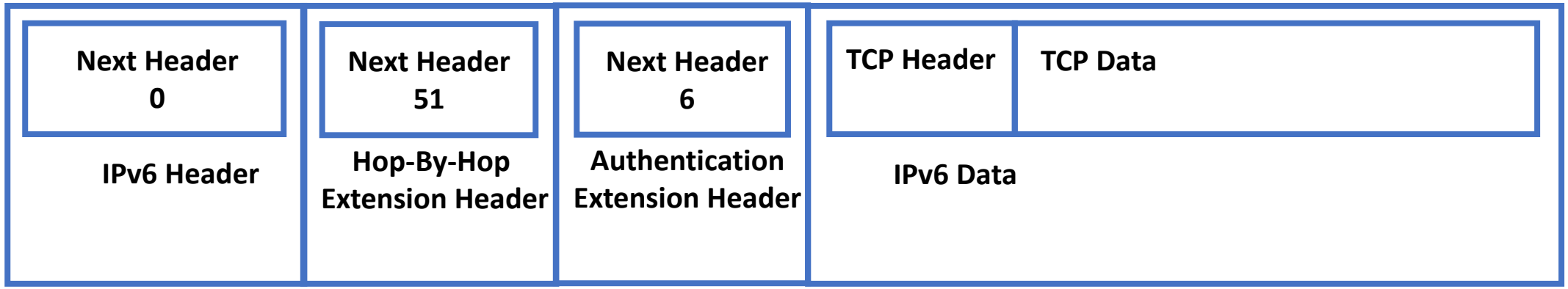
IPv4 vs. IPv6 - Header



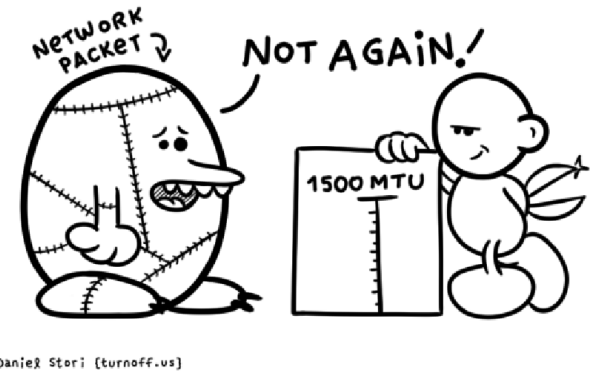
https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

IPv6 – Extension Header

- Header chaining
  - Mehrere Extension Header möglich
  - Reihenfolge sollte eingehalten werden



Fragmentierung



- **MTU** (Maximum Transmission Unit)
  - Maximale Größe des Layer 3 Pakets, welches in den darunterliegenden Rahmen passt.
  - Verschiedene Netzwerktechnologien haben unterschiedliche MTUs.
  - Beispiel: Ethernet: 1500Bytes oder X.25: 576Bytes
- **Problem**
  - Ein Router bekommt ein IP Paket mit 1230Bytes über die Ethernet Schnittstelle
  - Nun soll das Paket via X.25 weitergeleitet werden…?
- **Lösung**
  - Das Paket fallen lassen und zum Beispiel ein ICMP zurücksenden (Packet Too Big“)
  - In kleinere Teile splitten, so daß es in die MTU passt. → Fragmentierung

Fragmentierung (Cont.)

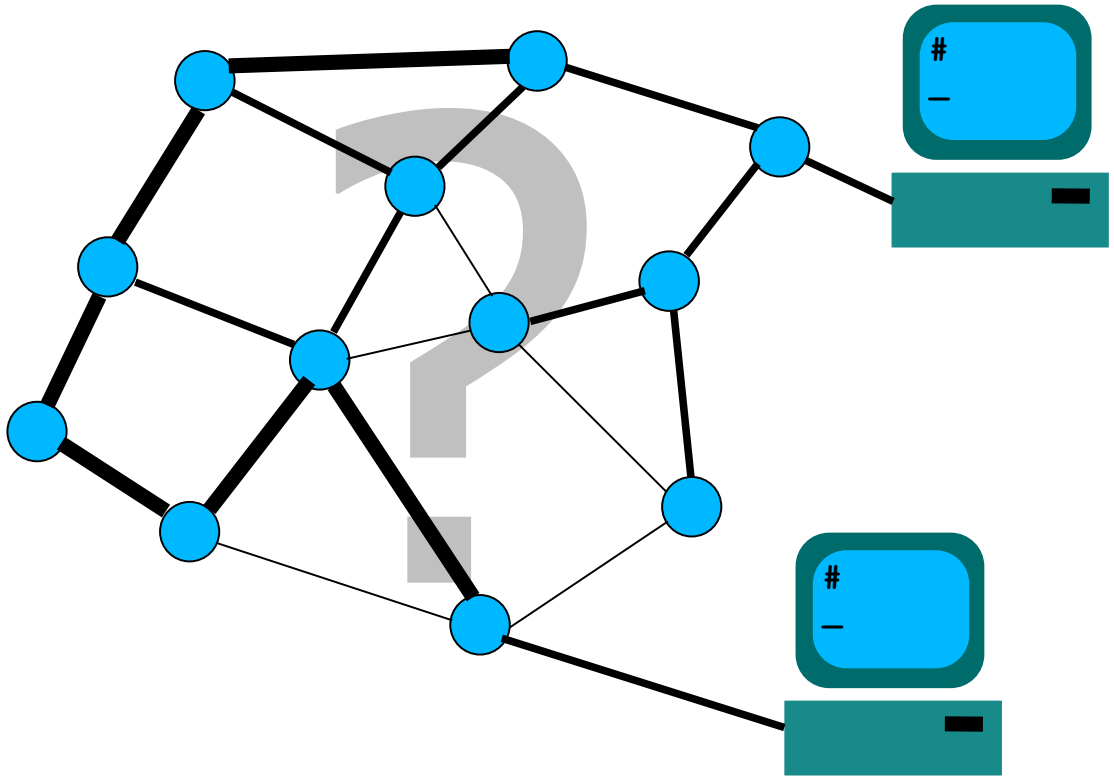
- Fragmente sind eigene IP Pakete (PDUs – Protocol Data Units)
- Fragmente enthalten keine spezifische Layer 4 Information.
- Der Empfänger baut die Pakete zusammen - auch ein Router kann es.
- DF, MF, Identification und Offset sind zur Kontrolle der Fragmentierung

- **Problem**
  - Wenn ein Fragment verloren wird, muss das ganze Layer 4 Segment neu gesendet werden.

- **Lösung**
  - Die kleinste MTU auf der Route herausfinden und in dieser Größe senden…

Routing

- Router behalten Routing Informationen in einer Tabelle.
- Routen können **statisch** eingetragen sein oder **dynamisch** über eigene Protokolle bestimmt werden.
- Beim dynamischen Routing können sich die Routen aus verschiedenen Gründen ändern…



Network Layer - Aufgaben

- Logische Adressierung von Interfaces und Hosts (IP Adressen)
- Aufbau von Netzwerken zu unterschiedlichen Hosts (Netzwerkklassen, Private Netzwerke, etc.)
- Transfer von Paketen über Netzwerkgrenzen hinweg (**Routing** → LV: Netzwerkmanagement)
- Kontrolle über Netzwerke

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

OSI 4

Transportschicht - Überblick

- „**Ports**“ und andere zusätzliche Informationen werden den Paketen vorangestellt.
- Ports identifizieren **Anwendungen zwischen 2 Kommunikationspartnern**
  (welche durch ihre IP Adressen identifiziert werden)
- Es gibt immer 2 Ports:
  - Der **Quellport** (Source Port)
  - Der **Zielport** (Destination Port)
- Der **Zielport identifiziert üblicherweise den angeforderten Dienst**.

Transmission Control Protocol (TCP)

- Grundidee
  - „Sich nicht um einzelne Netzwerkpakete kümmern sondern das **Empfangen/Senden großer Datenmengen in einer TCP Sitzung** ermöglichen."
  - Daraus folgt: „Eine Verbindung muss hergestellt und aufrecht erhalten bleiben."
- TCP verpackt Daten in so genannte **Segmente**.
  - Die Größe der Segmente wird durch darunterliegende Protokolle definiert.
  - Die Anwendungsdaten werden mit einem TCP Header versehen, der alle Informationen enthält, um die Daten sicher und verlässlich zu transferieren.
- **Verbindungsorientiert**
  - **Verbindungs-Management,** Kommunikationsdienst zwischen 2 Partnern und **Datentransport**!
  - **Full-Duplex** (Mehrfachverbindungen möglich)
  - Aber **Kosten beim Datendurchsatz**
  - **Hohen administrative Aufwand** im Protokoll und im Header

Schicht	Dienste / Protokolle / Anwendungen			
Anwendung	HTTP	IMAP	DNS	SNMP
Transport	TCP		UDP	
Internet	IP (IPv4 / IPv6)			
Netzzugang	Ethernet, ...			

Transportschicht im IP Stack

Quell-Port			Ziel-Port
Sequenz-Nummer			
Acknowledgement-Nummer			
D. O.	Res.	Flags	Window-Größe
Check-Summe			Urgent-Pointer
Optionen/Füllbits			
Daten....			

TCP Header

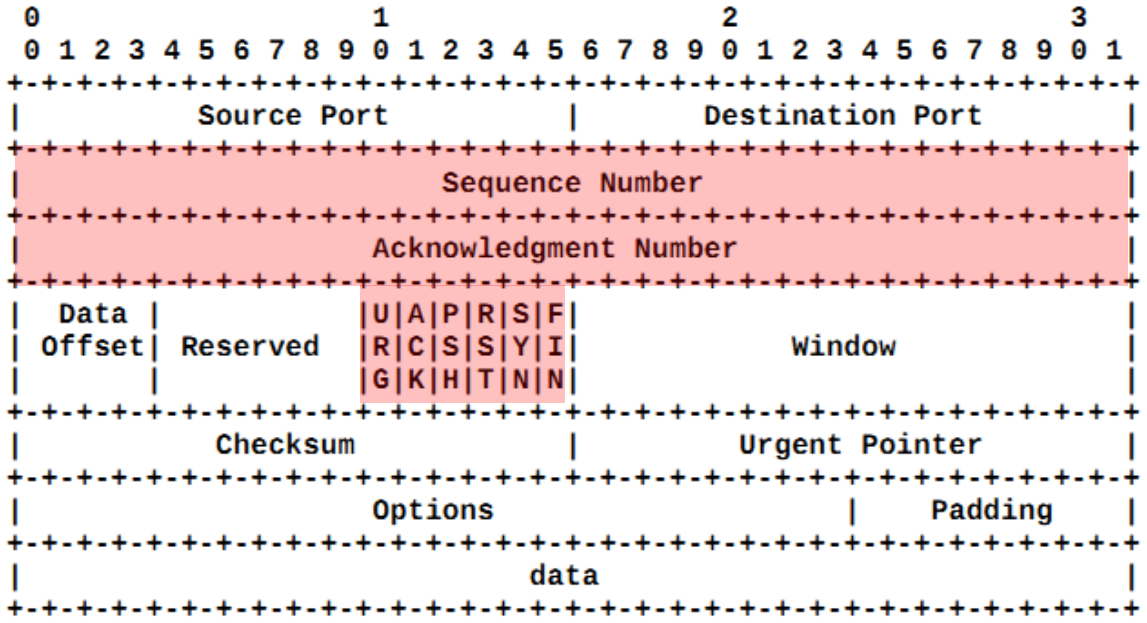
TCP: Funktionsüberblick

- **Verbindungs-Management**
  Aufbau, Überwachung und Abbau einer Verbindung
- **Verlässliche Kommunikation**
  Keine Pakete gehen verloren.
- **Fehlererkennung**
  Daten bleiben unverändert. (Integrität!)
- **Flußkontrolle**
  Übertragungsrate wird den Übertragungskanal angepasst.
- **Überlastungsschutz**
  Paketstau in Netzen mit viel Verkehr/Netzlast wird vermieden.
- **Zeitüberwachung**
  Bei Zeitüberschreitung wird eine Verbindung aufgelöst.

TCP: Verbindungsmanagement

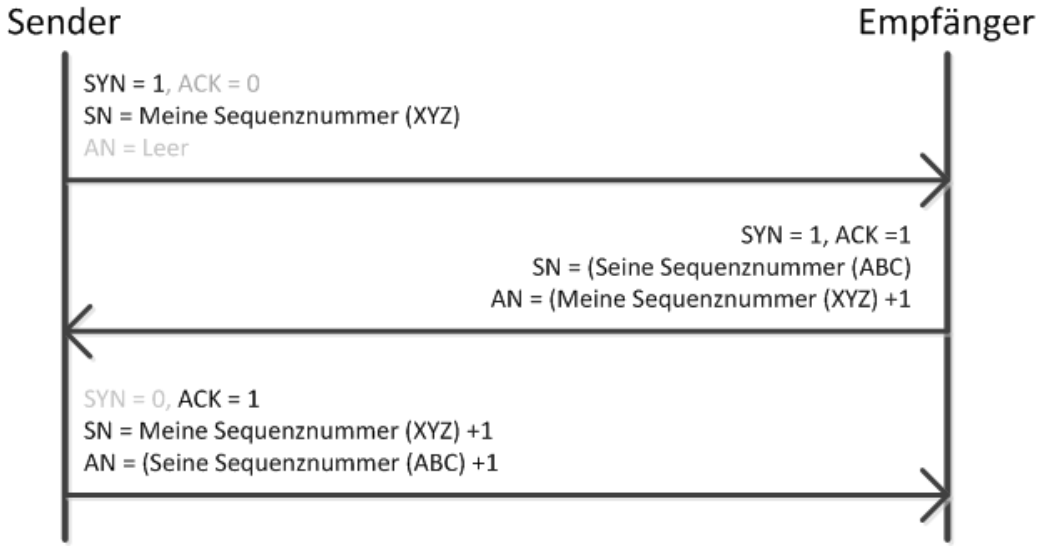
- Sequenznummer & Bestätigungsnummer

  Wichtig ist, dass sich beide Kommunikationspartner auf eine Sequenznummerierung einigen. Daher sind diese Bereiche für die Verbindung wichtig.
- Flags
  - URG (Urgent Pointer): Daten mit Priorität behandeln
  - **ACK** (Acknowledgement): Empfangsbestätigung
  - PSH (Push): Daten müssen sofort behandelt werden.
  - **RST** (Reset): Verbindung wegen Fehler beendet.
  - **SYN** (Synchronize): Zum Aufbau einer Verbindung verwendet.
  - **FIN** (Final): Ende einer Verbindung.



TCP: **3 Way Handshake** (3 Phasen Verbindungsaufbau)

- **Phase1**:
  SYN und ISN_{Sender} im Sequenznummernfeld an Empfänger
- **Phase2**:
  Empfänger sendet SYN, ACK, $ISN_{Empfänger}$ im Sequenznummernfeld und ISN_{Sender} +1 im Bestätigungsnummernfeld zurück.
- **Phase3**:
  ACK und ISN_{Sender} +1 im Sequenznummernfeld und $ISN_{Empfänger}$ +1 im Bestätigungsnummernfeld an Empfänger.



Funktioniert nur, wenn beide Partner für eine Verbindung bereit sind. (Zum Beispiel wartet der Webserver auf eine Anfrage: Passiver, offener Status)

TCP: Verbindungsabbau

- **Ungeplanter Verbindungsabbruch:**
  RST Flag von einem der Partner.
- **Normaler Verbindungsabbau:**
  Gegenseitiges Senden von FIN und Antworten mit ACK Flags.
- **Schneller, normaler Verbindungsabbau:**
  Gleichzeitiges senden von FIN und ACK in einem Paket.

TCP: Verlässliche Kommunikation

- Sequenznummern identifizieren Pakete.
- Dazu wird zuerst eine zufällige „Initial Sequence Number“ (ISN) erzeugt.
- Jedes Byte an Daten erhöht die Sequenznummer.
- Der Empfänger muss die Sequenznummern annehmen.
- Dazu sendet der Empfänger die nächst höchste Sequenznummer, die er bekommen hat zurück!

Beispiel:

- ISN = 100
- Das übertragene Segment enthält Bytes mit den Nummern: 100, 101, 102, 103, 104, 105
- Die Nummer 100 wird übertragen.
- Der Empfänger sendet 106 zurück. (= die Nummer des nächsten erwarteten Bytes)

TCP: **Flusskontrolle: Sliding Windows** (Schiebfenster)

- Übertragungsgeschwindigkeit wird gemessen.
- Zeitnahe und verlässliche Bearbeitung der Daten wird ermöglicht.
  Wenn ein Empfänger wenig Daten empfangen kann, wird der Datenfluss herabgesetzt.

„Sliding Windows“ (Schiebefenster) – Funktionsweise:

- Partner bestimmen eine „Fenstergröße“ (***Window Size***) für Daten.
- Der Empfänger kann alle Segmente oder nur das letzte Segment (am besten das des Fensters) bestätigen. (Letzteres= weniger Overhead)
- Fehlende Segmente (oder falls sie nicht zeitgerecht angekommen sind) werden noch mal gesendet.
- Es gibt eine dynamisch bestimmte Zeit (***Round Trip Time – RTT***), in der die Bestätigung da sein muss.

Das **User Datagram Protocol** (UDP)

- **Verbindungslos** (kein Handshake, keine Bestätigungen werden gefordert)
- **Unverlässlich** – Anwendungen müssen sich selbst um die Überprüfung des Datenaustauschs kümmern
- **Einfach und schnell**, weil kein Overhead
- Funktionen von TCP können in der darüberliegenden Schicht optimiert implementiert werden

Schicht	Dienste / Protokolle / Anwendungen			
Anwendung	HTTP	IMAP	DNS	SNMP
Transport	TCP		UDP	
Internet	IP (IPv4 / IPv6)			
Netzzugang	Ethernet, ...			

Transportschicht im IP Stack

Quell-Port	Ziel-Port
Länge	Check-Summe
Daten...	

UDP Header

UDP versus TCP

TCP

- Verbindungsorientiert
- Administrativer Overhead
- Ungeeignet für schnelle („Realtime“) Übertragungen
- Protokolle:
  HTTP, SMTP, POP3 (post office protocol), IMAP4 (internet message access protocol) ,FTP (file transfer protocol), Telnet

UDP

- Verbindungslos
- Keine administrative Funktionen
- Streaming
- Protokolle:
  DNS, SNMP (simple network management protocol), TFTP (trivial file transfer protocol), DHCP (dynamic host configuration protocol)

Zusammenfassung Transportschicht

- Dezidierte Verbindungen → TCP
- Kontrollierte Verbindungsaufbau und -abbau → TCP
- Fehlererkennung und Flußkontrolle → TCP
- Multiplexing – Mehrere parallele Verbindungen → UDP, TCP
- Optimierter Datenfluss („Windowing“) → TCP
- Priorisierung von Daten → TCP

Beispiele in Anwendungen

- **TCP**:
  HTTP, SMTP, POP3 (post office protocol), IMAP4 (internet message access protocol) , FTP (file transfer protocol), Telnet, etc.
- **UDP**:
  DNS, SNMP (simple network management protocol), TFTP (trivial file transfer protocol), DHCP (dynamic host configuration protocol), RTP (real time transport protocol) etc.

DIHSÜD Digital Innovation Hub

FH JOANNEUM University of Applied Sciences

Fragen?