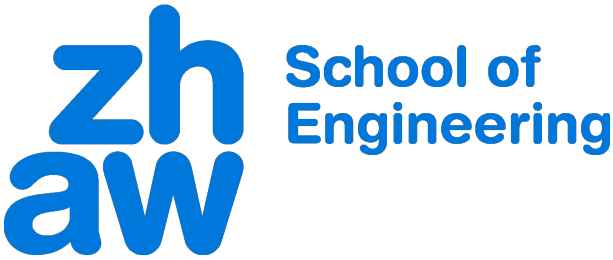
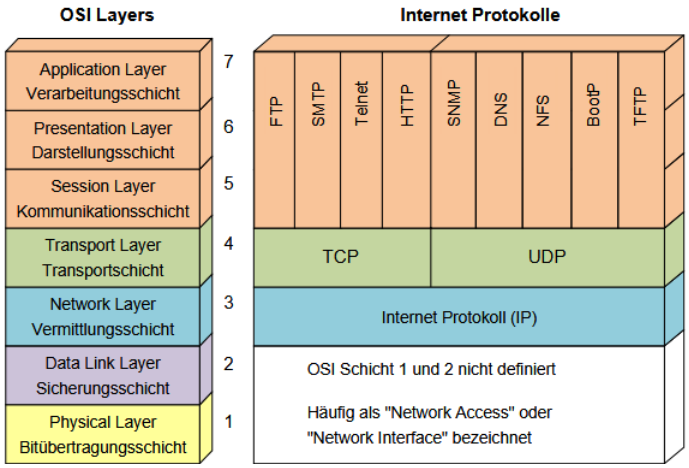
ZHAW Zurich University of Applied Sciences
Winterthur

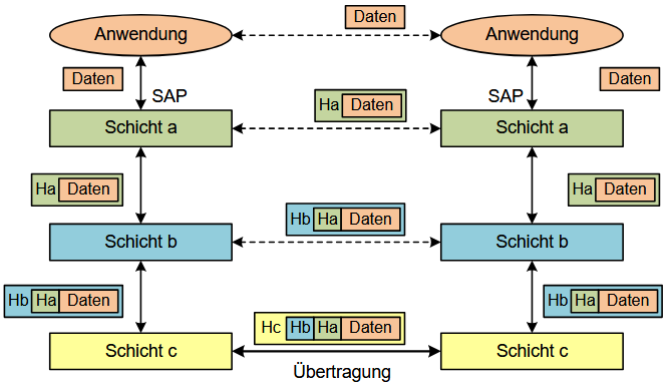


Zusammenfassung DCN
Studienwochen 1-14

Written by: Severin Sprenger
13. Oktober 2025
Zf. DCN SW 1-14

1 OSI-Model





1.1 Klassifizierung von Diensten

- **Zuverlässiger:** Fehlererkennung, Fehlerkorrektur, Quittierung von erhaltenen Daten
- **Unzuverlässiger:** Eine der Vorgaben für zuverlässige Dienste nicht gegeben

2 OSI Layer im Überblick

2.1 Physical Layer

- Übertragung eines Bitstromes
- Definiert elektrische Eigenschaften (Signalform, Art der Modulation)
- Codierung
- Mechanische Eigenschaften (Pinbelegung, Stecker, usw.)
- Übertragungsmedium (Formell kein Teil von OSI, wird aber durch Spezifikation mit beschrieben)

2.2 Data Link Layer

- Erstellt Frames and Daten
- Fehlererkennung und -korrektur
- Flow Control
- Adressierung (MAC-Adresse)
- Koordination des Zugriffs auf das Medium (Collision avoidance)

2.3 Network Layer

- Erlaubt Datenaustausch zwischen Knoten auf einheitliche Art
- Adressierung (IP-Adresse)
- Routing (Weiterleitung von Paketen)

2.3.1 Verbindungsorientiert / Leitungsvermittlung

- Ein Paket nimmt immer den gleichen Weg zum Ziel
- Beim senden eines Pakets wird ein Weg gewählt (Keine IP-Adressen werden verwendet)
- Quality of Service kann klar definiert werden
- Datenaustausch nur möglich wenn Sender weg zum Ziel kennt
- Reihenfolge der Daten bleibt immer gleich

2.3.2 Verbindungslos / Paketvermittlung

- Ein Paket muss nicht immer den gleichen Weg nehmen
- Knoten verfügen über eine Routing-Tabelle mit IP-Adressen
- Senden ohne Wegfindung (Ressourcen sparend)
- Rerouting möglich ohne äussere Eingriffe

2.4 Transport-Layer

2.4.1 User Data Protocol (UDP)

- Verbindungslos
- Unzuverlässig
- Send & forget
- Simplere Implementierung

2.4.2 Transmission Control Protocol (TCP)

- Verbindungsorientiert
- Zuverlässig
- Aushandeln von Optionen (Buffergrösse, Verschlüsselung, usw.)
- Tagging von Daten (Zur Wiederherstellung von Reihenfolge)

2.5 Application Layer

- Implementation von Protokollen (SMB, SMTP, HTTP, DNS, usw.)

2.6 Presentation Layer

- Umwandlung der Darstellung von Daten
- Umwandeln von Daten (ASCII, ISO, Unicode, usw.)

2.7 Session Layer

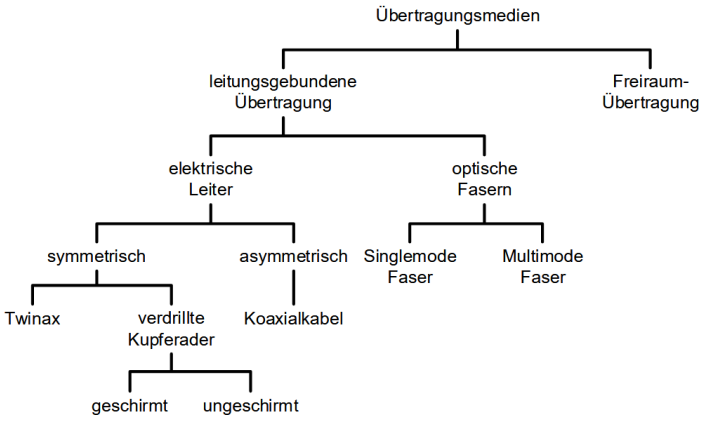
- Auf- und Abbau einer Session
- Falls Transportverbindung unterbrochen, kann Session wieder Aufgebaut werden

3 Übertragungsmedien

Das Medium gehört nicht zum Physical Layer und ist somit auch kein Teil des OSI/Modells. Ein Medium muss folgende Eigenschaften definieren:

Medium (Kabel, Lichtwellenleiter, usw.), Bandbreite, Dämpfung, Übersprechen (Cross talk)

3.1 Klassifizierung



3.2 Ausbreitungsgeschwindigkeit in Medien

- **Licht im Vakuum:** $c = 299792458\ \frac{\text{m}}{\text{s}}$
- **Licht in Glas:** $c_G = \frac{c}{n}$
- **El. Signal in Leiter** $c_L = \frac{c}{\sqrt{\varepsilon_r}}$

$$n \rightarrow \text{Brechungsindex}, \varepsilon_r \rightarrow \text{Permittivität}$$

Grundsätzlich gilt:

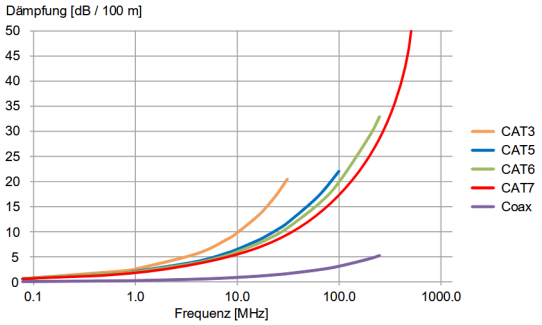
$$n = 1.5 \implies c_G \approx 200000\ \frac{\text{km}}{\text{s}}$$
$$\varepsilon_r = 2.25 \implies c_L \approx 200000\ \frac{\text{km}}{\text{s}}$$

3.3 Dämpfung (Attenuation)

$$A = 10 \cdot \log\left(\frac{P_1}{P_2}\right)$$
$$= 20 \cdot \log\left(\frac{U_1}{U_2}\right)$$
$$\frac{P_1}{P_2} = \left(\frac{U_1}{U_2}\right)^2$$

$$A \rightarrow \text{Dämpfung von Pos. 1 zu Pos. 2 in dB}$$

Dämpfung eines Mediums ist normalerweise als $\frac{\text{dB}}{100\text{m}}$ angegeben.



3.4 Störungen

$$\text{SNR} = \frac{P_{sig}}{P_{noi}}$$
$$\text{SNR}_{\text{dB}} = 10 \cdot \log\left(\frac{P_{sig}}{P_{noi}}\right)$$

$\text{SNR}_{\text{dB}} \rightarrow$ Signal to Noise Ratio in dB, $P_{sig} \rightarrow$ Leistung des Signals, $P_{noi} \rightarrow$ Leistung der Störung

3.4.1 Crosstalk

Crosstalk wird durch Kapazitäten und Induktivitäten im Kabel und Stecker ausgelöst.

- Near End Crosstalk → Empfängerseite
- Far End Crosstalk → Senderseite

3.5 Twisted Pair

- STP → Shielded Twisted Pair
- UTP → Unshielded Twisted Pair

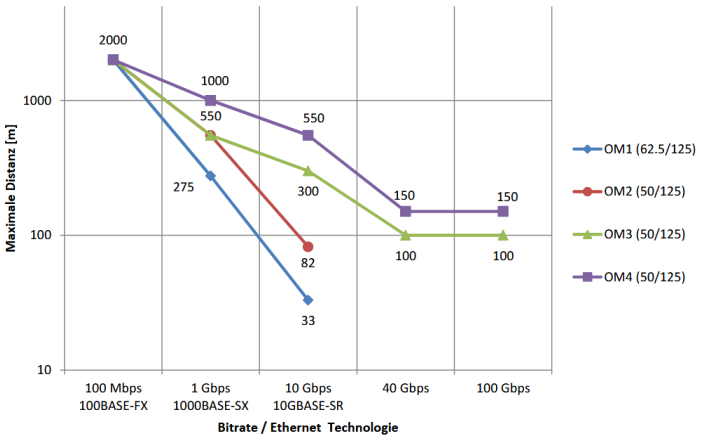
Kabel werden wie folgt Klassifiziert: **xx**/**y**TP

xx	**y**
U = unshielded	U = unshielded
F = Foil shield	F = Foil shield
S = Mesh shield	S = Mesh shield
SF = Mesh & foil shield	

- **Cat. 1 - 4.:** $< 1 \ \frac{\text{Mbit}}{\text{s}}$
- **Cat 5.:** $100 \text{ MHz}, 100 \ \frac{\text{Mbit}}{\text{s}}, s < 100 \text{ m} \implies 1 \ \frac{\text{Gbit}}{\text{s}}$
- **Cat 6.:** $250 \text{ MHz}, 1 \ \frac{\text{Gbit}}{\text{s}}, s < 55 \text{ m} \implies 10 \ \frac{\text{Gbit}}{\text{s}}$
- **Cat 7.:** $600 \text{ MHz}, s < 100 \text{ m} \implies 10 \ \frac{\text{Gbit}}{\text{s}}$

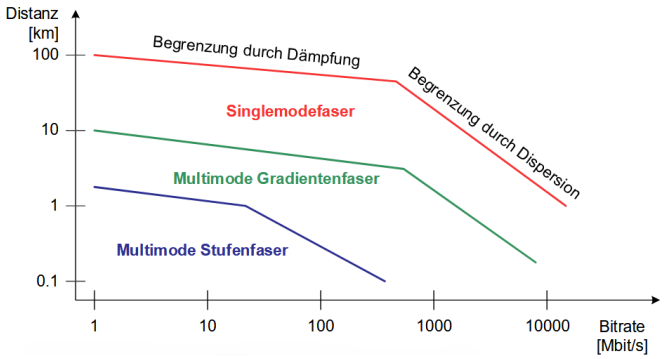
3.6 Multimode Glasfaser

- Günstig in der Anschaffung
- Relativ dicker Kern
- Günstige LED und Laser Quellen können verwendet werden
- Mantel und Kern haben verschiedene Brechungsindexe
- Signale können verschiedene Wege nehmen
- Moden-Dispersion → Pulse überlappen bei hohen Frequenzen, wegen Reflexionen



3.7 Singemode Glasfaser

- Teurer als Multimode
- Dünner Kern (≈ 9 um)
- Keine Moden-Dispersion
- Genauere Laser müssen als Quellen verwendet werden
- $s < 80$ km $\implies 10\ \frac{\text{Gbit}}{\text{s}}$, $s < 40$ km $\implies 100\ \frac{\text{Gbit}}{\text{s}}$,

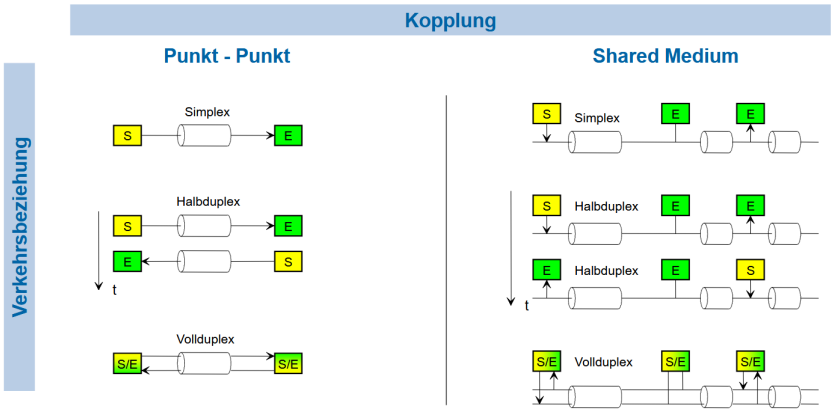


4 Physical Layer

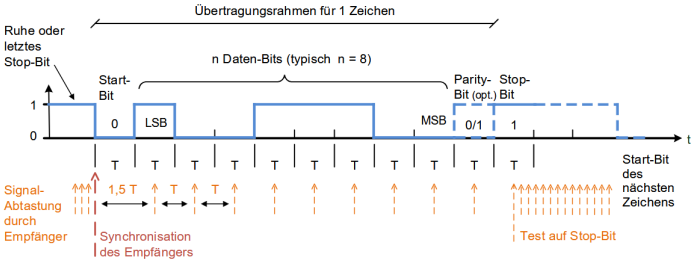
Der Physical Layer beschreibt:

Verkehrsbeziehung (Simplex, Half-Duplex, Full-Duplex), Kopplung (Point to Point, Shared Medium), Medium (Koaxialkabel, Twisted Pair, Lichtwellenleiter, usw.), Übertragungsverfahren (Synchron oder Asynchron, Modulation)

4.1 Verkehrsbeziehung und Kopplung



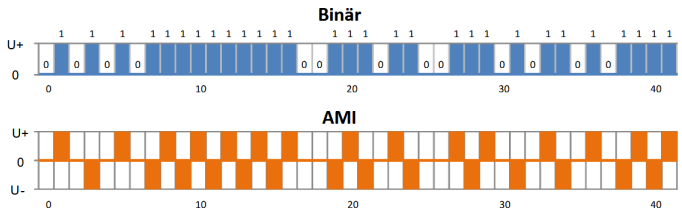
4.2 Asynchrone Übertragung



4.3 Leitungscodes

Das Ziel von Leitungscodes ist die vorhandene Bandbreite effizient nutzen, Talkrückgewinnung ermöglichen, Möglichst gleichspannungsfrei sein (Isolation mit Transformatoren ermöglichen)

4.3.1 AMI (Alternate Mark Inversion)



4.4 Bitrate / Baudrate

$$N = \text{lb}\,(n)$$
$$N = \frac{R}{B}$$

$N \rightarrow$ Anzahl benötigter Bits, $n \rightarrow$ Anzahl unterschiedlicher Signalzustände

- $[f_s] = \text{Bd} = \frac{\text{Symbols}}{\text{s}} \rightarrow$ Symbolrate (Baudrate)
- $[B] = \text{Hz} \rightarrow$ Bandbreite
- $[R] = \frac{\text{bit}}{\text{s}} \rightarrow$ Bitrate
- $[C] = \frac{\text{bit}}{\text{s}} \rightarrow$ Kanalkapazität

4.4.1 Nutzung der Bandbreite (nach Nyquist)

Die Folgende Formel gilt für einen idealen Leiter ohne Störungen.

$$f_s = 2 \cdot B$$

Für reale Medien gilt:

$$f_s < 2 \cdot B$$

Wobei B aus einer Tabelle oder einem Diagram abgelesen wird und f_s die Symbolrate des Protokolls ist (z.B. 1000BASE-T).

4.4.2 Maximale Bit-Rate (nach Hartley)

Bei diesem maxima wurde noch keine Störungen berücksichtigt.

$$M = 1 + \frac{A}{\Delta V}$$
$$M = \sqrt{1 + \text{SNR}}$$
$$I_S = \text{lb}\,(M)$$
$$R \leqslant 2 \cdot B \cdot I_S$$

$M \rightarrow$ Unterscheidbare Signalzustände,
$A \rightarrow$ Maximaler Wert des Signals,
$\Delta V \rightarrow$ Differenz zwischen einzelnen Signalzuständen,
$I_S \rightarrow$ Informationsgehalt eines Symbols,
$R \rightarrow$ Maximale Bit-Rate

4.4.3 Kanalkapazität (nach Shannon)

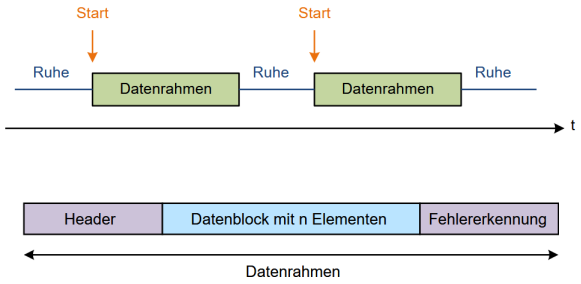
$$C_s = B \cdot \text{lb}\,(1 + \text{SNR})$$

5 Data Link Layer

Der Data Link Layer beschreibt:

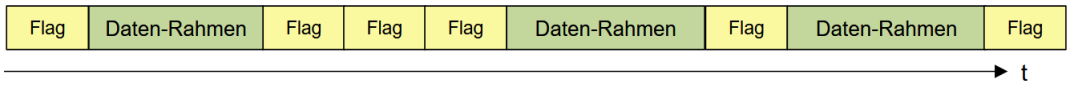
Framing von Daten, Bit- und Rahmenfehlerwahrscheinlichkeit, Fehlererkennung, Fehlerkorrektur, Flusskontrolle, Adressierung, Media access

5.1 Asynchrone Übertragung



5.1.1 Synchrone Übertragung

Bei einer synchronen point-to-point Übertragung werden durchgehend Flag Signale gesendet falls keine Daten gesendet werden (Kein unterbruch). Gesendete Frames werden somit durch Flag Daten eingeschlossen.



5.1.2 Bit-Stuffing

Falls eine Übertragung ein Bitmuster zur Detektion von Start und Ende einer Übertragung verwendet, muss sichergestellt werden, dass diese Bitmuster nicht in den zu senden Daten vorkommen. Dies wird mit Bit-Stuffing sichergestellt.

Bei einem Muster von 01111110 wird z.B. beim Sender nach 5 Einsen immer eine 0 eingefügt. Der Empfänger entfernt dann immer nach 5 Eines immer das nächste Bit immer.

5.2 Bit- und Restfehlerwahrscheinlichkeit

$$\text{BER} = \frac{B_E}{B_T},\ \text{FER} = \frac{F_E}{F_T},\ \text{RER} = \frac{F_R}{F_T}$$

BER → Bit Error Ration, B_E → Anzahl Fehlerhafte Bits, B_E → Totale Anzahl Bits

FER → Frame Error Ratio, F_E → Anzahl Fehlerhafte Frames, F_E → Totale Anzahl Frames

RER → Residual Error Ratio, B_E → Anzahl unentdeckter Fehlerhafter Frames, B_E → Totale Anzahl Frames

$$P_{Erfolg} = 1 - p_e$$
$$P_{Erfolg,Frame} = (1 - p_e)^N$$
$$P_{Fehler,Frame} = 1 - (1 - p_e)^N \ (= \text{FER})$$

$p_e \rightarrow$ Bitfehlerwahrscheinlichkeit, $N \rightarrow$ Anzahl Bits in einem Frame

Je grösser die Frame-Länge desto höher ist der Anteil der Nutzdaten, jedoch steigt die Fehlerwahrscheinlichkeit mit steigender Framelänge logarithmisch an. Daher existiert ein Optimum von Nettobitrate (Anzahl Bits ohne Header) und der Fehlerwahrscheinlichkeit. Für ein Frame mit Header Grösse 128 Bits und einem BER $= 10^{-4}$ bei 1197 Bits.

5.3 Fehlererkennung

Nach IEEE 802 (LAN-Standards) $\rightarrow$ RER $\leqslant 5 \cdot 10^{-14}$ und BER $\leqslant 10^{-8}$ wird vom Medium gefordert.

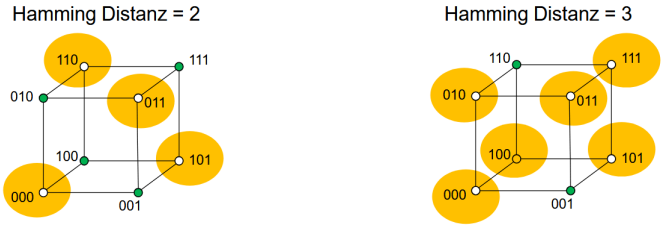
5.3.1 CRC-32 (nach IEEE 802.3)

$$N \leqslant 226 \implies \text{Hamming-Distanz} \geqslant 6$$
$$269 \leqslant N \leqslant 2974 \implies \text{Hamming-Distanz} = 5$$
$$2975 \leqslant N \leqslant 91607 \implies \text{Hamming-Distanz} = 4$$
$$91608 \leqslant N \leqslant 121072 \implies \text{Hamming-Distanz} = 3$$

CRC basiert auf der Polynomdivision. Die Bit-Folge wird eine zweite Bit-Folge dividiert. Die Bit-Folgen, stellen die Koeffizienten eines Polynoms mit Grad N dar (z.B. 1011 $\rightarrow 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$). Die originale Bit-Folge wird solange durch das Divisor-Polynom dividiert bis es einen Rest gibt. Dieser Rest wird mit der originalen Bit-Folge an den Empfänger übertragen indem der Rest an die Nachricht angehängt wird. Der Empfänger wiederholt dann diese Polynomdivision der empfangenen Bit-Folge und sollte keinen Rest erhalten. Falls der Rest ungleich Null ist, enthält die Bit-Folge einen Fehler.

5.3.2 Hamming-Distanz

Die Hamming-Distanz definiert den Abstand (Bit-Flips) eines validen Symbols zu einem anderen validen Symbol in einem bestimmten Code.



Mithilfe der Hamming-Distanz können Bit-Flips in einer Nachricht korrigiert werden. Dazu wird das nicht valide Symbol zum nächsten validen Symbol verändert. Die maximale Anzahl an detektierbarer Bit-Flips lautet $e = h - 1$, wobei h die Hamming-Distanz ist und e die Anzahl an detektierbaren Bit-Flips.

Mit der Hamming-Distanz können auch Bit-Flips korrigiert werden. Die maximale Anzahl von korrigierbaren Bit-Flips ist wie folt definieren:

$$k = \frac{h - 1}{2}$$

$k \rightarrow$ Anzahl korrigierbarer Bit-Flips, $h \rightarrow$ Verwendete Hamming-Distance

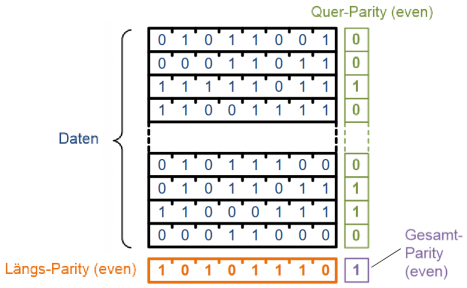
5.3.3 Even/Odd Parity

Even/Odd Parity fügt zu einer bestehenden Nachricht/Bit-Folge ein zusätzliches Bit hinzu, dass die Anzahl an 1 in der Nachricht/Bit-Folge gerade oder ungerade macht. Even/Odd Parity verfügt über eine Hamming-Distanz von $h = 2$

- **Even Parity:** Anzahl von 1 inkl. Parity-Bit ist gerade.
- **Odd Parity:** Anzahl von 1 inkl. Parity-Bit ist ungerade.

5.3.4 Längs- und Quer-Parity

Längs- und Quer-Parity basiert auf der Gleichen Idee wie Even/Odd Parity und ist lediglich eine Erweiterung dieses Prinzips.



5.3.5 Prüfsumme

$$P = \sum_{n-1}^{i=0} E\left(i\right)$$

$P \rightarrow$ Prüfsumme, $n \rightarrow$ Anzahl Datenelemente, $E\left(\right) \rightarrow$ Einzelnes Symbole/Elemente der Nachricht

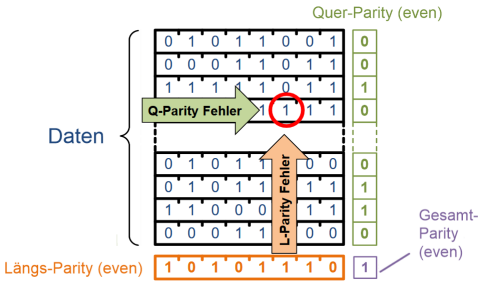
5.4 Backward Error Correction (BEC)

Bei der BEC muss jede Nachricht durch den Empfänger bestätigt werden, daher ist ein Rückkanal erforderlich. Bei fehlender Bestätigung, negativer Bestätigung oder Bestätigungs-Timeout wird die betroffene Nachricht erneut übermittelt bis die Nachricht erfolgreich empfangenen wird. BEC ist im Transport Layer genauer behandelt und definiert.

5.5 Forward Error Correction (FEC)

FEC ersetzt BEC nicht, sonder sollte die benötigten BEC minimieren. Bei fehlerhaften Nachrichten, wird die wahrscheinlich ungestörte Nachricht geschätzt (Hamming-Distanz). Falls Fehler korrigiert werden, wird die geschätzte Nachricht erneut mithilfe eines Fehlererkennungsverfahren geprüft. Falls weiterhin ein Fehler erkannt wird, kommt die BEC ins Spiel.

FEC kann auch mithilfe von Längs- und Quer-Parity durchgeführt werden.



5.6 Zugriffsmechanismen

- **Master-Slave Verfahren:** Master koordiniert Zugriff (Keine Konflikte), Single Point of Failure (Master)
- **Token Verfahren:** Knoten mit Token sendet und gibt Token weiter, Aufwändig (Startup, Token Verlust)
- **Zeitsteuerung:** Definiert wer sendet wann, Aufwändig in der Planung und schwer erweiterbar
- **Carrier Sense Multiple Access:** Knoten prüft ob Frei und sendet, Kollisionen möglich

5.6.1 Kollisionsbehandlung

- **CSMA/CD (Collision Detection):** Abbrechen und später nochmals Versuchen
- **CSMA/CR (Collision Resolution):** Hardware-unterstütze Arbitrierung
- **CSMA/CA (Collision Avoidance):** Prüfen, ob Medium frei ist (Listen before talk (LBT))

Knoten 2 wird seine Nachricht nach einer Pause erneut senden um eine erneute Kollision zu vermeiden.

5.7 Flow Control

Flow Control erlaubt dem Empfänger den Sender zu bremsen, falls der Empfänger durch den Sender überlastet wird.

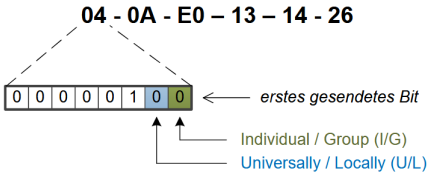
- **Explizit:** Empfänger kann Sender starten oder stoppen
- **Implizit:** Empfänger muss jede Nachricht bestätigen (Quittiert erst wenn Platz für nächste Nachricht)

6 Ethernet / LAN (Data Link Layer)

- **Topologie:** Bus, Linie (Point-to-Point), Ring, Vermascht (teilweise oder komplett), Stern, Baum
- **Übertragungsarten:** Unicast (1 Target), Multicast (Mehrere Targets), Broadcast (Alle im Subnetz)
- **Adressierung:** MAC (6 Bytes, fix zu jedem Gerät)

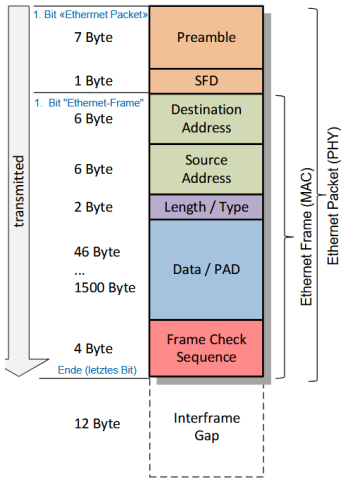
6.1 MAC Adressen im Detail

3 Bytes → OUI (Hersteller) / 3 Bytes → Laufnummer, ID



- **I/G:** 0 = individuelle Adresse, 1 = group address (z.B. Broadcast)
- **U/L:** 0 = universally administrated, 1 = locally administrated

6.2 Packet und Frame Format



- **Overhead:** 18 Bytes
- LSB first, ausser Length und Type sind MSB first
- $N \leqslant 1500 \implies$ Länge von DATA ohne PAD, $N \geqslant DATA \implies$ Type/Porto
- **Frame Check Sequence:** CRC-32

$$T_{Frame} = \frac{N}{R}$$
$$T_{Leitung} = \frac{N + 96}{R}$$
$$N = (\text{FrameSize} + 8) \cdot 8$$

$T_{Frame} \rightarrow$ Sendedauer, $T_{Leitung} \rightarrow$ Leitungsbesetzungszeit, $N \rightarrow$ Anzahl Bits im Frame

6.3 Ethernet-Geräte

- **Hub / Repeater:** Physical Layer, keine Fehlererkennung/Fehlerkorrektur, keine Packet Steuerung
- **Switch / Bridge:** Layer 2, Checksumme wird ausgewertet

6.3.1 Filtering Database (Switch)

Eine Liste von MAC Adressen von Geräten die an einem Switch angeschlossen sind. Wenn ein Switch ein Packet weiter leitet muss und die MAC Adresse in der Database zu finden ist, wird das Packet nur auf diesen Port ausgegeben. Falls kein Eintrag vorhanden ist, wird das Packet auf allen Ports ausgegeben. Einträge in dieser Database verfallen nach einer kongruierten Zeit.

6.3.2 Zeitverhalten

Hubs und Switched unterscheiden sich stark in Zeitverhalten. Ein Hub leitet Packets schneller weiter als eine Switch, da das Hub lediglich das Packet 1:1 wiedergibt und z.B. kein Error Checking durchführt. Somit hat ein Hub eine sehr kleine Latenz die durch das Einlesen und anschliessendes Ausgeben auf die anderen Ports ausgelöst wird. Ein Switch hingegen muss warten bis er das gesamte Packet empfangenen hat, führt dann Error Checking usw. durch und sendet erst dann das Packet weiter. Daher die grössere Latenz.

$t_{transfer}$ → Von Host A zu Switch/Hub, $t_{forwarding}$ → Zeit Eingang bis Ausgang Daten am Switch/Hub, t_{frame} → Sendezeit für Ganzes, $t_{processing}$ → Verarbeitungszeit im Switch

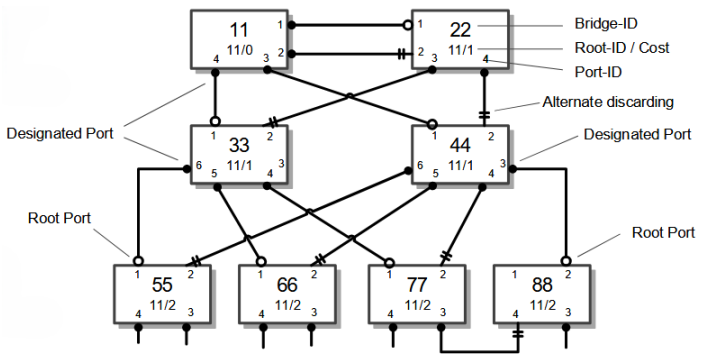
6.3.3 Spanning Tree

Ermöglicht schleifenfreie Topologie, Unterbrüche können ohne Eingriffe gelöst werden, Verschiedene VLAN's können unterschiedliche Spanning Trees besitzen, Problem: Während Aufbau oder Änderung ist Netzwerk für Nutzerdaten blockiert

BPDU Structure (Bridge Protocol Data Units)

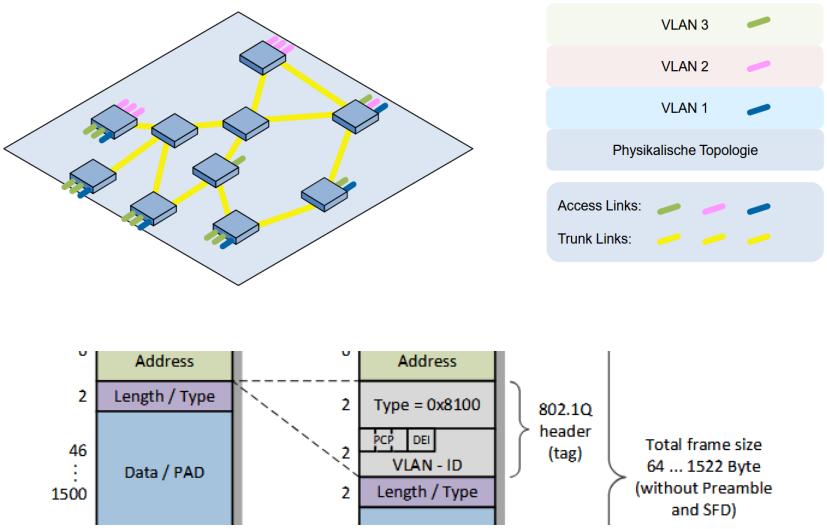
Root-ID (aus lokaler Sicht)	8 Bytes
Root-Cost (aus lokaler Sicht)	2 Bytes
Bride-ID (Eigene ID)	8 Bytes
Port-ID (Sende-Port)	2 Bytes

1. **Initialisierung:** Annahme: Ich bin Root, auf allen Ports BPDU senden
2. **Aufbau:** Austausch/Aufdatierung (Path-Cost) aller BPDU bis Root established (kleinste ID und/oder Path-Cost tief)
3. **Setzen der Port Roles:** Root-Ports (Port mit least Cost to Root), Designated-Ports (Ports zu andere Switches), Discarding (Unverwendete Ports)
4. BPDU's werden alle 2 sec erneut versendet um Unterbrüche zu erkennen und reparieren

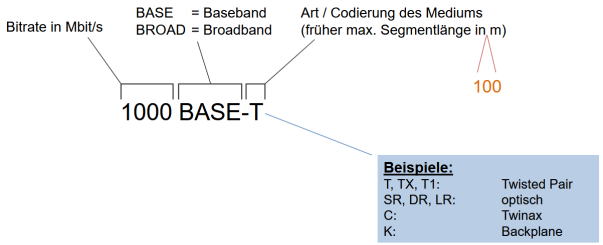


6.3.4 VLAN's und QoS

- Spart an Hardware (Mehrere getrennte Netze auf mit einer Infrastruktur)
- Anpassungen ohne zusätzliche Hardware möglich
- Network Segregation sichergestellt (Im Gegensatz zu Subnets)
- Transparent für Endnutzer
- **PCP (QoS):** Strict Priority ($0-7$, Prio 0 - Prio 7)
- **DEI (QoS):** Drop Eligible Indicator, ob ein Packet während Congestion verworfen werden darf



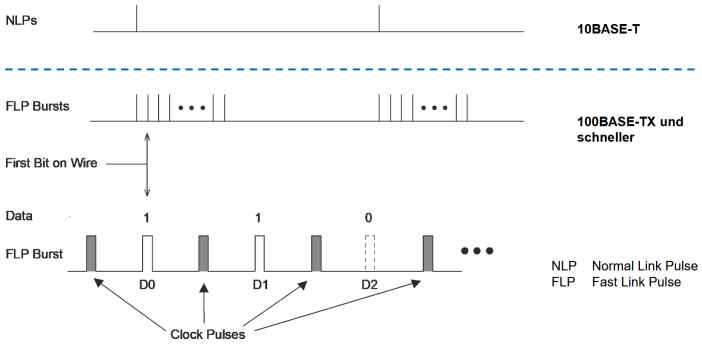
6.4 Bezeichnungs-Schema

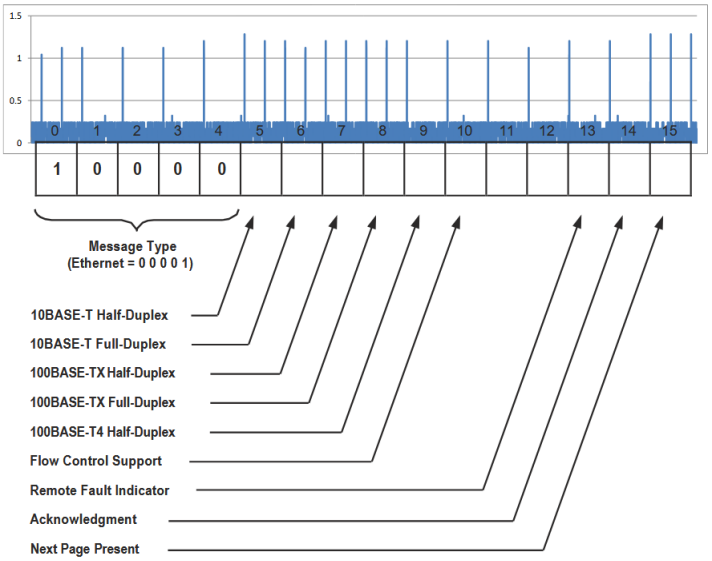


6.5 Autonegotiation

Bei Autonegotiation handeln zwei Geräte mit einander aus welche Ethernet Geschwindigkeit von beiden Geräten verwendet werden kann.

Auto-Polarity und Auto-Crossover ist Teil des Geräts das Second on Wire ist. Dabei versucht das Gerät zu identifizieren, welche Aderpaare zum Sende und Empfangen verwendet werden und wie diese polarisiert sind.





6.6 Übersicht Ethernet Evolution

	10BASE-T IEEE 802.3i	100BASE-TX IEEE 802.3u	1000BASE-T IEEE 802.3ab	10GBASE-T IEEE 802.3an
Kabelkategorie (für 100m Link Distanz)	CAT3 B = 16 MHz CAT5 B = 100 MHz	CAT5 B = 100 MHz CAT6 B = 250 MHz	CAT5 B = 100 MHz CAT6 B = 250 MHz	CAT6A B = 500 MHz CAT7/7A B = 600/1000 Mhz
Line Coding	Manchester 2 Aderpaare simplex	MLT-3 (synchron), 4B5B 2 Aderpaare simplex	PAM-5 (plus scrambling) 4 Aderpaare duplex	PAM-16, 64B/65B, FEC 4 Aderpaare duplex
Baudrate	10 MBaud	125 MBaud	4 x 125 MBaud	4 x 800 Mbaud
Link Pulses	NLP (Link Presence Detection)	FLP (Autonegotiation, Autopolarity)	FLP (Autonegotiation, Autopolarity, Next Page)	FLP (Autonegotiation, Autopolarity, NextPage)

7 Network Layer

Verbindet Teilnetze zu virtuellen grösseren Netzen, Nur zuständig für den Transport der IP-Pakete (keine Fehlererkennung oder Verlusterkennung)

7.1 Grundsätze Router, Routing & Forwarding

Verbindet verschiedene Netze mit potenziell verschiedenen Technologien (Ethernet & DSL), Verhält sich wie ein Konten im Netzwerk

Router müssen den optimalen Weg zu einem anderen Netz/Host kennen. Dies wird in kleinen Netzen eingesetzt und manuell konfiguriert. In grossen Netzen ermittelt der Router den optimalen Weg/Topologie selbst.

- **Innerhalb eines autonomous Systems:** Enhanced Interior Gateway Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System to Intermediate Systems (IS-IS)
- **Zwischen mehreren autonomous Systems:** Border Gateway Protocol (BGP)

Router gibt Packets an einen bestimmten Host an ein anderes Netz/Router weiter der/das auf dem Weg zum Host liegt.

7.2 IPv4

4 Bytes, IP-Adresse identifiziert Host-Interface, nicht Host selbst

7.2.1 Subnetzmaske

Gibt an welche Bits in einem Netzwerk frei wählbar sind. 192.168.50.0/XX → XX gibt an wie viele Bits fixiert sind (von links nach rechts aufgefüllt).

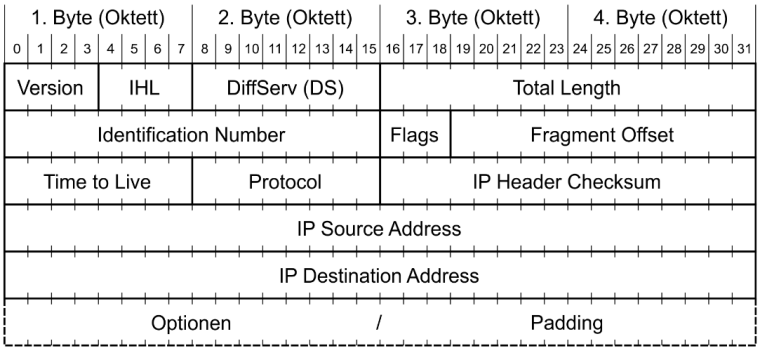
7.2.2 Netzadresse

Die Netzadresse ist keine Adresse die ein Host verwenden kann. Die Netzadresse wird ermittelt indem alle frei wählbaren Bits (definiert durch Subnetzmaske) auf 0 gesetzt werden.

7.2.3 Broadcast-Adresse

Die Broadcast-Adresse adressiert alle Adressen in einem Subnet und kann nicht von einem Host verwendet werden. Die Broadcast-Adresse ist die höchste Adresse in einem Subnetz und wird ermittelt indem alle frei wählbaren Bits (definiert durch Subnetzmaske) auf 1 gesetzt werden und MAC ist 6x FF.

7.2.4 Header Format



Version	4 (IPv4) oder 6 (IPv6)
IHL (Internet Header Length)	Länge des Headers als vielfaches von 4 Bytes (Header ohne Optionen 20 Bytes $\implies$ IHL = 5)
DS (Differentiated Services)	Erlaubt Priorisierung von IP-Datenpaketen **Bit 0-5** sind DSCP (Differentiated Services Codepoints) oder auch Prio **Bit 6-7** sind ECN (Explicit Congestion Notification) und wird verwendet um bevorstehende Überlastungen mitzuteilen
Total Length (TL)	Länge inklusive Header und Nutzdaten in Bytes
Identification Number (ID)	Unique ID des ursprünglichen Packets (zur zusammensetzung bei Fragmentierung)
Flags	**Bit 0** ist Reserved und muss 0 sein **Bit 1** ist DF (Don't Fragment) 1 = Don't Fragment, 0 = May Fragment **Bit 2** ist MF (More Fragments) 1 = More Fragments to come 0 = Packet is last Packet
Fragment Offset (FO)	Gibt an wo das Fragment in die originale Nachricht gehört
TTL	Verbleibende Hop Anzahl des Packets (Jeder Router dekrementiert Wert beim Routing)
Protocol	Protokoll der Nutzdaten (Porto der übergeordneten Schicht)
Header Checksum	Prüfsumme nach definition (5.3.5), bei jeder Route neu berechnet weil TTL verändert
Source Address	IP-Adresse der Source
Destination Address	IP-Adresse der Destination
Options	Selten verwendet
Padding	Auffüllen mit 0 bis Header vielfaches von 32 Bits = 4 Bytes

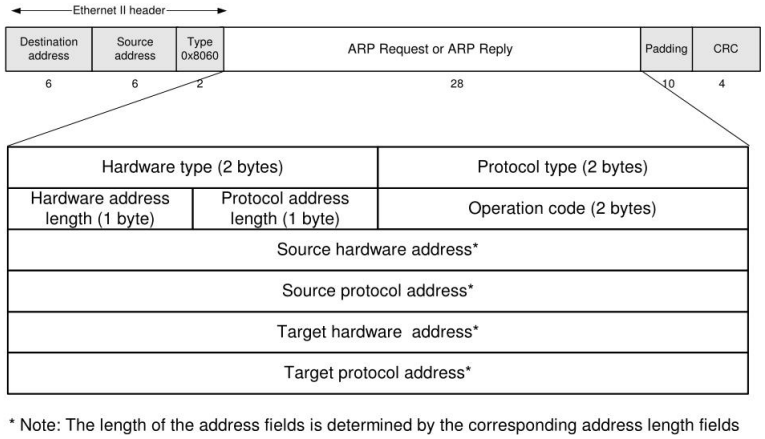
7.2.5 Fragmentierung

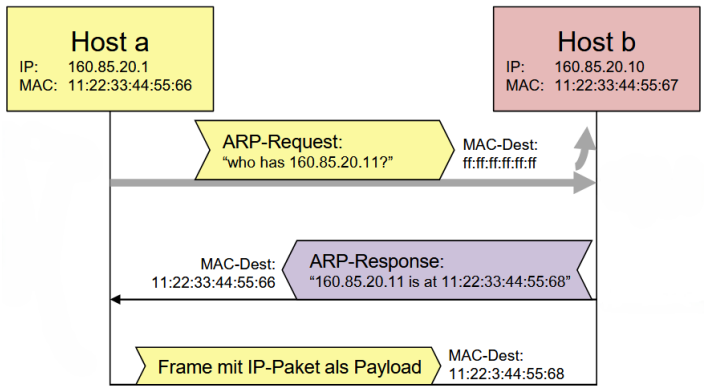
Wenn ein Packet beim Routing die MTU (Maximum Transfer Unit) des Pfads, dass das Packet nehmen muss, überschritten wird, muss ein Packet Fragmentiert werden (aka. in mehrere kleine Packets aufgeteilt werden). Die Fragmentierung wird durch den Sender durchgeführt und das Packet wird erst beim Target wieder reassembled (Dadurch Entlastung von Routern). Fragmentierung ist nur Teil von IPv4, IPv6 ist keine Fragmentierung vorgesehen.

Fragment Offset wird in Anzahl 8 Bytes grossen Packets angegeben. (FO = 100 $\implies$ 800 Bytes Offset)

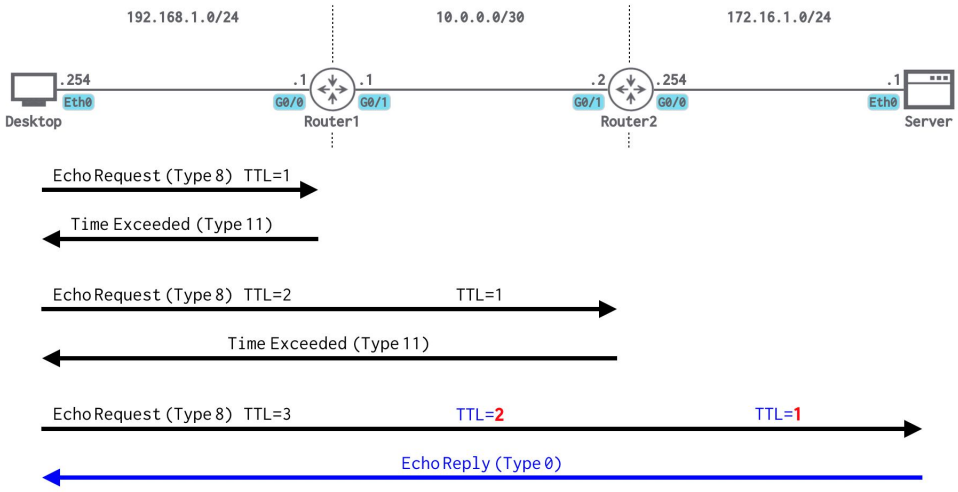
7.2.6 ARP (Address Resolution Protocol)

ARP löst IP-Adressen zu MAC Adressen auf. Dazu broadcasted der Host, der eine IP-Adresse auf eine MAC-Adresse auflösen möchte, eine ARP-Request in sein gesamtes Netzwerk (Broadcast an MAC 6x FF). Alle Hosts auf dem Netzwerk erhalten diesen Broadcast, jedoch antwortet nur der Host mit der IP-Adresse die in der ARP-Request verlangt ist mit einer ARP-Response. Der Anfragende Host speichert dann diese MAC-IP Kombination in seinem ARP Cache für eine bestimmte Zeit ab. **Wichtig: ARP basiert nicht direkt auf IP, wird jedoch oft mit dem Network Layer verbunden.**



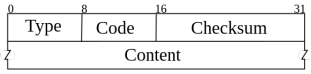


7.2.7 Traceroute



7.2.8 ICMP (Internet Control Message Protocol)

Verwendet IP-Layer, Unzuverlässig, Informationelle Nachrichten



Type	Bedeutung	Type	Bedeutung
0	Echo Reply (Ping Reply)	11	Time Exceeded
3	Destination Unreachable	12	Parameter Problem: Bad IP Header
5	Redirect	13	Timestamp
8	Echo (Ping)	14	Timestamp Reply

7.3 Spezielle Adressen/Netze

- 127.0.0.0/8 → Loopback-Netz
- 10.0.0.0/8 → Privater Adressbereich
- 172.16.0.0 - 172.31.0.0/16 → Privater Adressbereich
- 192.168.0.0 - 192.168.255.0 → Privater Adressbereich
- 169.254.0.0/16 → Autoconfig-Adressen

7.4 Klassifizierung von Subnets

- **Class A:** 255.0.0.0 (/8)
- **Class B:** 255.255.0.0 (/16)
- **Class C:** 255.255.255.0 (/24)

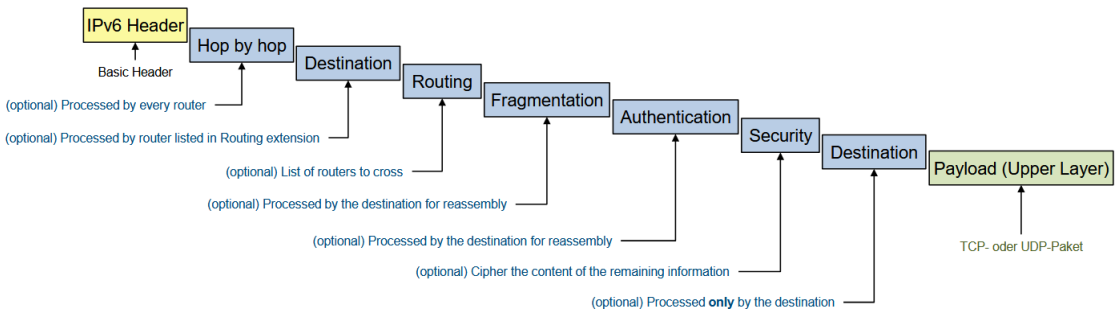
7.5 Supernetting / Subnetting

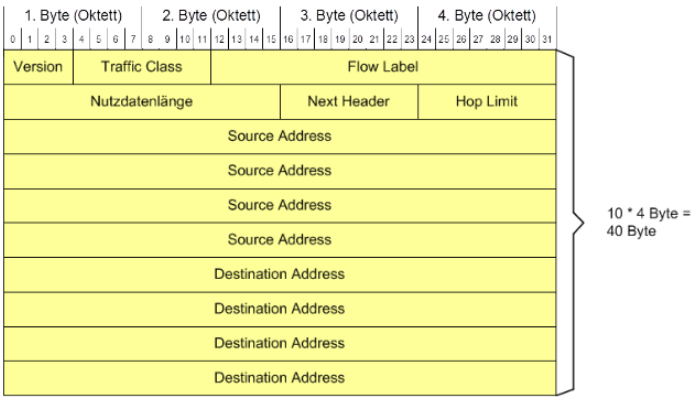
Supernetting beschreibt das zusammenfassen von mehreren kleinen Netzen in ein grösseres Subnetz. Kann helfen Routing-Tabelle zu verkleinern.

Subnetting beschreibt das Aufteilen eines grossen Subnetz in mehrere kleinere Subnetze.

7.6 IPv6

- 16 Bytes dargestellt als HEX in 2 Bytes grossen Blöcken abgetrennt durch :
- Leading 0 können in einem Block weggelassen werden
- 2^{218} Adressen $= 3.4 \cdot 10^{38}$ Adressen in Vergleich zu 2^{32}
- ICMPv6 ersetzt ARP, RARP und IGMP (ICMPv6 Proto Type ist 58)
- Ethertype für IPv6 0x86dd
- Header 40 Byte IPv6 + Extension Header
- Fragmentierung wird in Extension Headers definiert
- Extension Header werden nur bei Bedarf eingefügt und der Typ des folgenden Headers wird durch das Next-Header-Feld definiert





7.7 Routing

Jeder Router verfügt über eine Routing-Tabelle. In dieser ist beschrieben wie ein bestimmtes Netz/Host erreicht werden kann. Ein solcher Routing-Eintrag kann auch auf weitere Router verweisen. In den meisten fällen verfügt eine Routing-Tabelle über einen default Eintrag. Dieser Eintrag wird verwendet falls das gesuchte Netz/Host über keinen anderen Eintrag erreichbar ist (Hierarchisches Routing). Falls kein solcher Eintrag vorhanden ist und ein Netz/Host über keinen Eintrag verfügt wird das Paket im Router verworfen (Flaches Routing).

Diese fix definierten Netze sind teilweise nicht passend für bestimmte Anwendungen (C zu klein und B zu gross). CIDR (Classless Inter-Domain Routing) erlaubt Subnetzmasken von beliebiger Länge.

7.8 Verwaltung von IP-Adressen

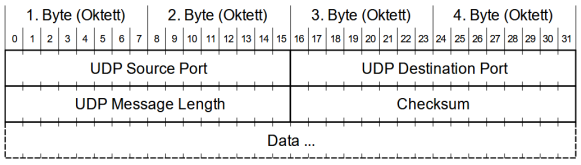
Verwaltung/Vergabe durch IANA im Auftrag der ICANN (Internet Corporation for Assigned Names and Numbers), IANA delegiert an Regional Internet Registries (RIR) (Europa: RIPE-NCC), RIRs delegieren an Local/National Internet Registries (LIR, NIR), LIR/NIR delegieren an ISP

8 Transport Layer

Schnittstelle für Applikationen und Netzwerk, Implementiert TCP und UDP, Einführung von Ports, Flow-Control (Sliding Window), Congestion Control, TCP Proto Type ist 06, UDP Proto Type ist 17

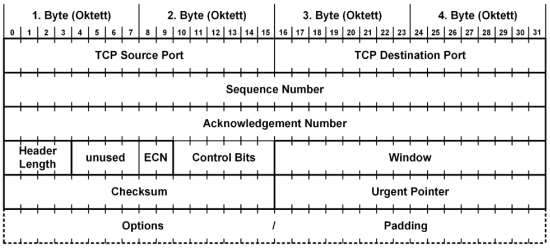
8.1 UDP (User Datagram Protocol)

Verbindungslose Unzuverlässige Kommunikation. (Checksum wird über Source-, Destination-IP, Protocol, Length aus IP-Header, UDP-Header und Daten berechnet)



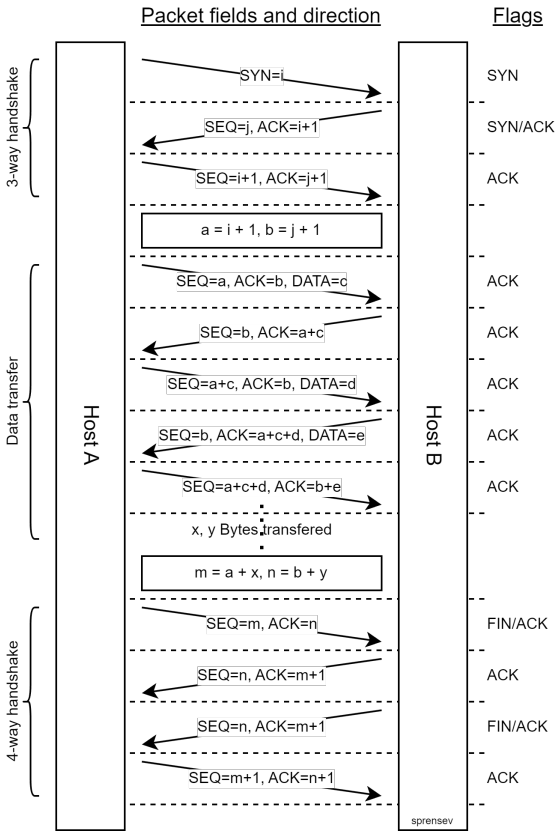
8.2 TCP (Transmission Control Protocol)

Bidirektionale zuverlässige stream-basierende Kommunikation. (Checksum wird über Source-, Destination-IP, Protocol, Length aus IP-Header, TCP-Header und Daten berechnet)



Source Port	Die Portnummer auf der die Antwort erwartet wird.
Destination Port	Die Portnummer an die das Packet versendet wird.
Sequence Number	Sequenznummern der Daten des gesendeten Packets.
Acknowledgment Number	Sequenznummern die als nächstes erwartet wird.
Header Length	Länge des Headers.
ECN Flags	Congestion Window Reduced (CWR) und ECN-Echo (ECE).
Control Bits	URG (urgency), ACK (is ACK Number valid?), PSH (direkte Weiterleitung an APP), RST (reset connection), SYN (Verbindungsaufbau), FIN (Verbindungsabbau).
Window	Grösse des Buffers des Empfängers.
Checksum	Checksum über Pseudo-Header, TCP-Header und Daten.
Urgent Pointer	URG-Flag gesetzt bedeutet UP den Bytes Offset der Urgend Data.
Options	Repräsentiert die verschiedenen TCP-Optionen.

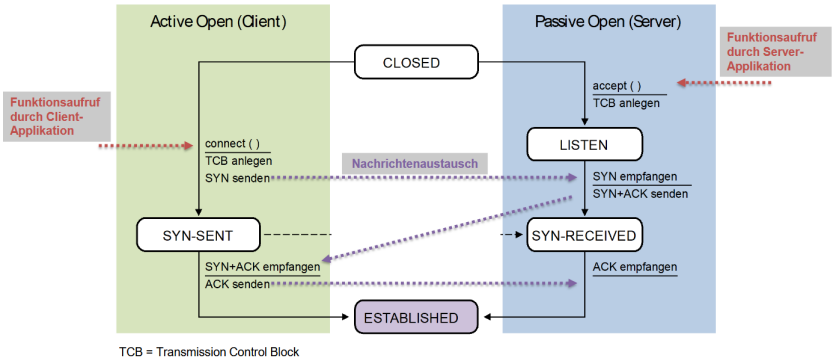
1. **Verbindungsaufbau:** Initialisierung von Sequenznummern, Aushandeln von Optionen, Initialisierung und Reservation von Ressourcen (Buffer, Variablen)
2. **Nachrichtenaustausch:** Übertragung von Nutzdaten, Sequenznummern sichern korrekte Reihenfolge, Explizite Bestätigung empfangener Daten, Wiederholte Übertragung verlorener Nachrichten
3. **Verbindungsabbau:** Sicherstellen des geordneten Austausches bis zum Ende, Freigabe der allozierten Ressourcen



8.2.1 Flags

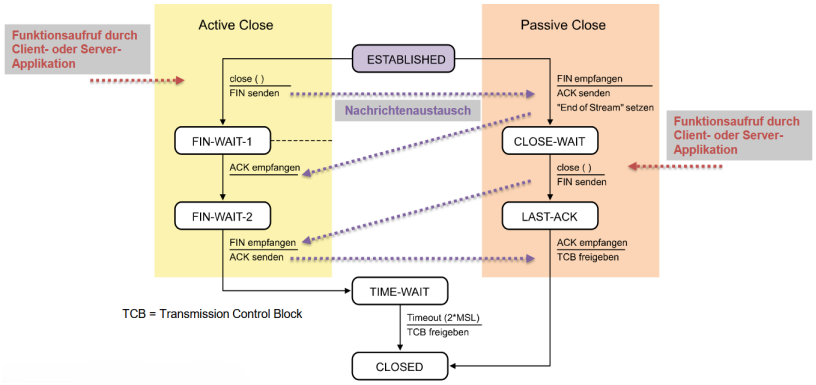
- **SYN/FIN:** Verbindungsauf- und -abbau
- **ACK:** Acknowledge Number im empfangenen Segment ist gültig
- **PSH:** Daten sollen schnellstmöglich an Applikation weitergegeben werden

8.2.2 Verbindungsaufbau State-Machine



8.2.3 Verbindungsabbau State-Machine

Eine Verbindung kann auch nur einseitig geschlossen werden, dieser Verbindungszustand wird als Half-Closed bezeichnet.



8.2.4 RTO (Retransmission Time-Out)

$$\begin{aligned} \text{SRTT}_{new} &= (1-\alpha)\cdot \text{SRTT}_{old} + \alpha \cdot \text{RTT}, \alpha = 0.125 \\ \text{RTTVAR}_{new} &= (1-\beta)\cdot \text{RTTVAR}_{old} + \beta \cdot |\text{SRTT} - \text{RTT}|, \beta = 0.25 \\ \text{RTO} &= \text{SRTT} + 4 \cdot \text{RTTVAR} \end{aligned}$$

SRTT → Smoothed Round-Trip Time, RTTVAR → Gewichteter Mittelwert der Abweichungen

8.2.5 Flow-Control

- **Stop-and-Wait-Verfahren:** Packet senden, warten auf ACK, nächstes senden
- **Sliding Window:** Empfänger teil Sender mit wie viele Bytes noch im Buffer platz haben

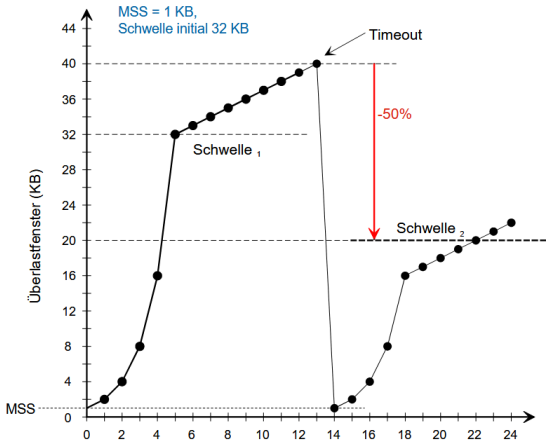
$$\text{BDP} = \text{RTT} \cdot B$$

BDP → Bandwidth-Delay-Product (Optimale Buffer Size um Verbindung nicht auszubremsen)

8.2.6 Congestion Control

Sicher stellen, dass das Netz über das Daten ausgetauscht werden nicht überlastet wird.

MSS → Maximum Segment Size (Anzahl Nutzdaten bei bestimmter MTU)

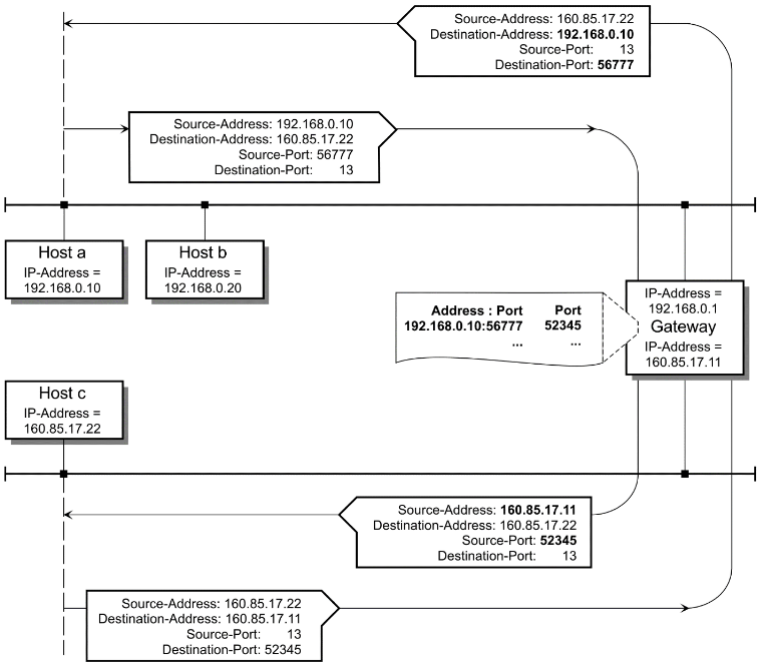


8.3 Ports

- System Ports: 1 – 1023
- User Ports: 1024 – 49151
- Dynamic / Private Ports: 49152 – 65536

9 Network-Applications & Protocols

9.1 NAT (Network Address Translation)



ISCHES DIE GANZ FUCKING ZIIT WERT GSI DIE ZF SCHRIIBE, NEIIIIIIIIII