Übertragungsmedien

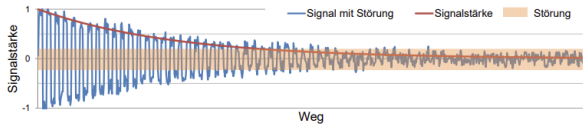
Ausbreitungsgeschwindigkeit

Lichtgeschwindigkeit im Vakuum: $c_0 = 299'792'458 \frac{m}{s}$

Daraus folgt die Ausbreitungsgeschwindigkeit im Medium: $\approx \frac{2}{3} c_0 \approx \mathbf{200'000 \frac{km}{s}}$

Signaldämpfung

Leistungsabnahme eines Signals auf einer Übertragungsstrecke.



$$\boldsymbol{Signaldämpfung\ (SNR)\ [dB] = 10 * \log\left(\frac{P1}{P2}\right)}$$

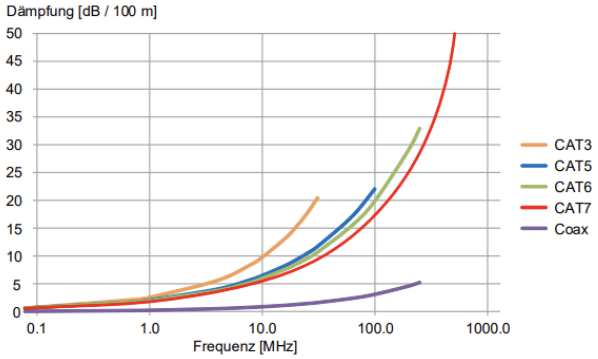
$P1: Eingangsleistung$
$P2: Ausgangsleistung$

$$= 10 * \log\left(\left(\frac{U1}{U2}\right)^2\right) = 20 * log\ \left(\frac{U1}{U2}\right)$$

- Eine Dämpfung von **6 dB** bedeutet eine **Leistungsabnahme um den Faktor 4** und **Spannungsabnahme um den Faktor 2**.

Dämpfungsbelag

Dämpfung pro Distanz; Typischerweise dB/100 m oder dB/km.



- ⇨ Je **kleiner die Dämpfung**, desto **grössere Distanzen** kann das Signal «leben».
- ⇨ **Senkt man Bitrate** (Bit/s), können **grössere Distanzen** erreicht werden.
- ⇨ Die Bandbreite (Frequenz) ist in der Grafik abhängig zum Dämpfungsbelag.
- ⇨ Die höheren Kabelkategorien brauchen, um höhere Dämpfung zu tolerieren, bessere Schirmungen, um das Übersprechen zu minimieren.

Kabeltypen

- **Koaxialkabel:** Geeignet für hochfrequente Signale. Besser als TP.
- **Twinaxial-Kabel:** Hoher Schutz. Geschirmt oder ungeschirmt. Allfälliger auf Störung.
- **Twisted Pair (TP):** Häufig im Einsatz.
- **Glasfaser:** Hohe Bandbreite, Geringe Dämpfung, zusätzlich:Dispersion(schlecht) ⇨ Wegen Totalreflexion. *Arten (aufsteigend nach Kosten): Multi Mode (MM) Stufenfasern, MM Gradientenfasern, Single Mode Fasern.* ⇨ Nehmen wenn zu grosses Rauschen

Störungen

- ⇨ Eine Verstärkung der Signale beim Empfänger möglich wenn Signal von der Störung (siehe Diagramm Signaldämpfung) abhebt.
- ⇨ Mögliche Störungen:
  - Übersprechen zwischen Leitungen.
  - Rauschen des Empfängers.
  - Einstreuungen durch andere Geräte.

> Übersprechen / Nebensprechen (crosstalk): Störungen von benachbarten Leitungen (kapazitiv oder induktiv).

- ⇨ Komplementäre Signale (Empfänger subtrahiert die Signale -> Störungen werden aufgehoben) und Schirmung gegen kapazitive Störungen.
- ⇨ Verdrillung gegen induktive Störungen.

Kabelschirmung Bezeichnung

xx/*y*TP worin TP für Twisted Pair steht:

xx steht für die Gesamtschirmung:	*y* steht für die Aderpaarschirmung:
U = ungeschirmt	U = ungeschirmt
F = Folienschirm	F = Folienschirm
S = Geflechtschirm	S = Geflechtschirm
SF = Schirm aus Geflecht und Folie	

Physical Layer (Schicht 1)

Verkehrsbeziehung und Kopplung

Arten der Kommunikation (*Verkehrsbeziehung*)

- Simplex — Ein Kanal, in eine Richtung
- Halbduplex — Ein Kanal, abwechslungsweise in zwei Richtungen
- Vollduplex — Ein Kanal pro Richtung

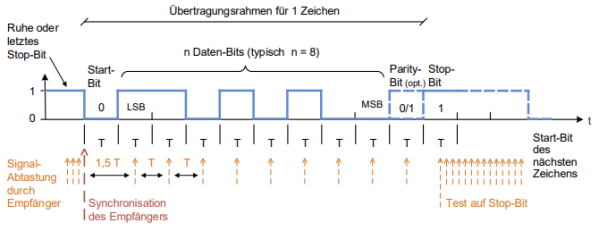
Arten der Verbindungen (*Kopplung*)

- Punkt-Punkt — Direkte Verbindung zweier Kommunikationspartner
- Shared Medium — Mehrere Partner verwenden das gleiche Medium

Serielle Asynchrone Übertragung

Kein Takt für Bitsynchronisation wird übertragen.

- Empfänger justiert seinen Übertragungsrahmen bei jedem übertragenen Zeichen von Neuem.



> Sender/Empfänger brauchen Abmachungen:

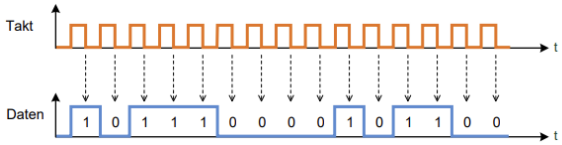
- Bitrate
- Anzahl Datenbits
- Anzahl Stoppbits

> Taktrückgewinnung: Möglich

Serielle Synchrone Übertragung

Empfänger arbeite mit Takt von Sender.

- Keine Start- und Stoppbits notwendig.
- Neben Datensignal muss auch Takt übertragen werden.



Aufgabe vom Data Link Layer Grenzen der einzelnen Bytes zu ermitteln (Preamble etc.).

Leitungscodes und Taktrückgewinnung

Mittels Leitungscode ist es dem Empfänger möglich den Takt heraus zu extrahieren (sonst bräuchte er eine 2te Leitung für den Takt).

- Siehe Manchester Code.
- Regelmässige Zustandsänderungen auf der Übertragungsstrecke.

Formeln: Nutzung der Bandbreite

> Bitrate: Bit/s

> Baudrate: Symbol/s (Signaländerung)

> Symbolrate (Nyquist Rate):

$$f_s \leq 2B$$

f_s: Max. Symbolrate (Baud (Bd))

B: *Nutzbare Bandbreite (Hz)*

> Max. erreichbare Bitrate (Hartley's Gesetz):

$$R \leq 2B * ld(M)$$

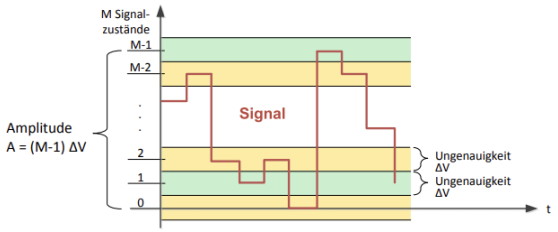
R: *Max. Bitrate (bit/s)*

M: *Unterscheidbare Signalzustände*

$$M = 1 + \frac{A}{\Delta V}$$

A: *Max. Grösse des Signals*

V: *Ungenaugikeit des Empfängers*



> Gesetz von Shannon-Hartley:

$$C = B * ld\left(1 + \frac{S}{N}\right)$$

C: *Kanalkapazität*

S: *Signalleistung*

N: *Rauschleistung*

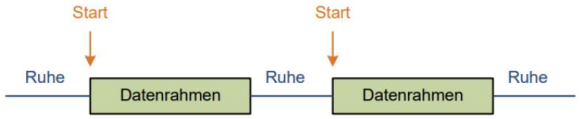
Data Link Layer (Schicht 2)

Datenraten – Framerate & Nutzbitrate

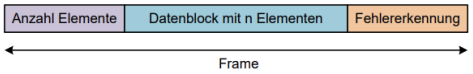
- $F_R = FrameRate,\ B = BitRate,\ F_L = FrameLength$
- $N = NutzBitRate, P = Payload$

$$F_R = \frac{B}{8 \cdot (F_L + IFG)}, \qquad N = F_R \cdot P \cdot 8$$

Framing (Asynchron)



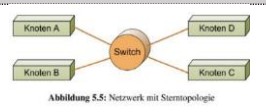
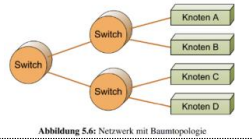
- Keine Daten: Nichts wird gesendet: Ruhe.
- Zu Beginn eines Frames wird ein Start Bit gesendet (ändern des Ruhezustands).
- Prüfbits am Ende eines Frames!
- Bspw. IP Pakete für unterschiedliche Routen.



Wahl der Frame-Länge

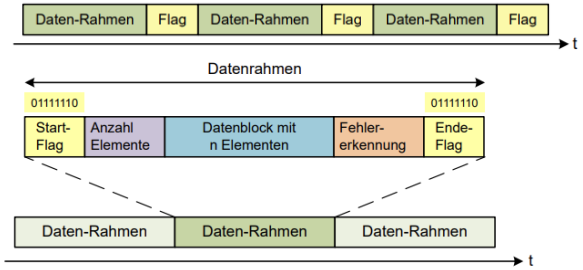
- Je länger die Frames desto besser wird die Nettobitrate.

$$\text{Nettobitrate} = \text{Bruttobitrate} * \frac{\text{Nutzdaten}}{\text{Nutzdaten} + \text{Header}}$$

Bild	Beschreibung
 Abbildung 5.5: Netzwerk mit Sterntopologie	> Zentraler Verteiler. > Wenig Störungsanfällig.
 Abbildung 5.6: Netzwerk mit Baumtopologie	> Weniger Last für die einzelnen Switches (Aufteilung).

Framing (Synchron)

- Frames werden dauernd gesendet (wenn kein Inhalt, dann leerer Frame).
- Start- und Stopflag.

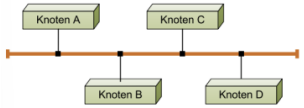
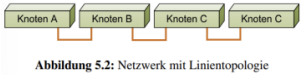
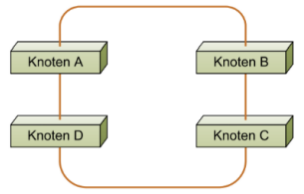


> Bitstopfen:

- Sender fügt im Datenstrom nach 5 Einsen immer einer 0 ein.
- Empfänger wirft nach 5 Einsen immer 1 Bit weg.
- Somit gibt es nie (ausser bei Flags) die Bitfolge 01111110

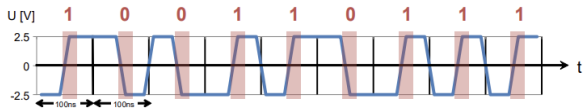
Lokale Netzwerke (Ergänzung 1 Schicht 2)

Topologien

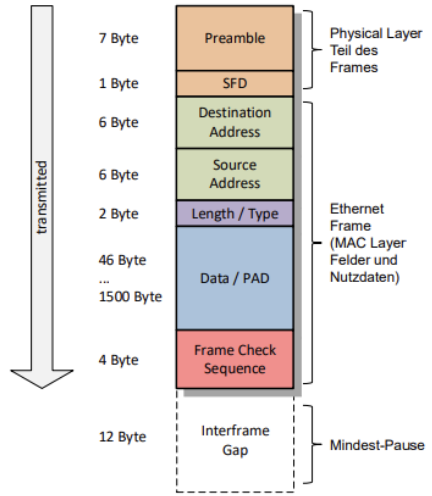
Bild	Beschreibung
 Abbildung 5.1: Netzwerk mit Bustopologie	> Passiv an Kabel. > Empfänger sieht anhand Adresse ob Daten relevant.
 Abbildung 5.2: Netzwerk mit Linientopologie	> Alle müssen Daten empfangen. > Ausfall: Segmentierung des Lan in 2 Teilen.
 Abbildung 5.3: Netzwerk mit Ringtopologie	> Benötigt Verfahren für Verhinderung von «endlosem Zyklus». > Ausfall: Jede kann immer noch erreicht werden.

Manchester Leitungscode (10BASE-T)

- 1: Positive Flanke; 0: Negative Flanke
- Bei jedem Bit gibt es einen Signalwechsel
- Einfache Taktrückgewinnung

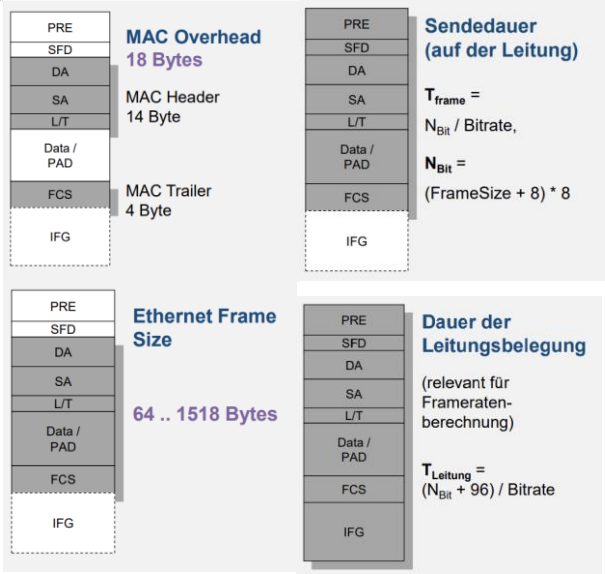


Ethernet Frame Format und Begriffe



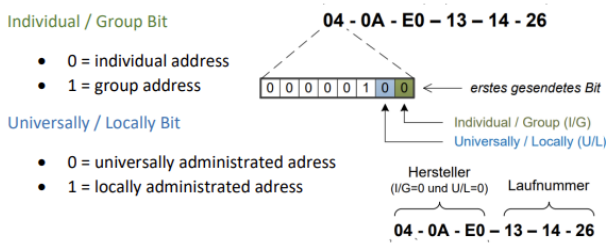
Zugriffsmechanismen (MAC):

- Master-Slave Verfahren
- Token-Verfahren
- Zeitsteuerung
- Carrier Sense Multiple Access (bei Ethernet inkl. CD (Collision Detection))



- Wenn Data < 46 Bytes wird mit PAD aufgefüllt.
- Length / Type: Entweder Länge von Data ohne PAD (<= 1500) oder Protokoll ID der nächsten Schicht (von Data).

MAC Adressen



⇨ Destination MAC Adresse wird vor Source MAC Adresse im Frame gesendet, da so ein Switch oder Router die Frames schneller auslesen kann und somit weiss wohin.

Kollisionen

⇨ Bei Überlagerungen von Signalen.

⇨ Bspw. zwei Frames kommen gleichzeitig im Hub (Schicht 1) an (Minimaler Switch (Schicht 2) kann dies nicht passieren).

⇨ *Vollduplex: Keine Kollision da keine Spannungserhöhung (kann man prüfen).*

> Formeln:

Bedingung für Kollisionserkennung

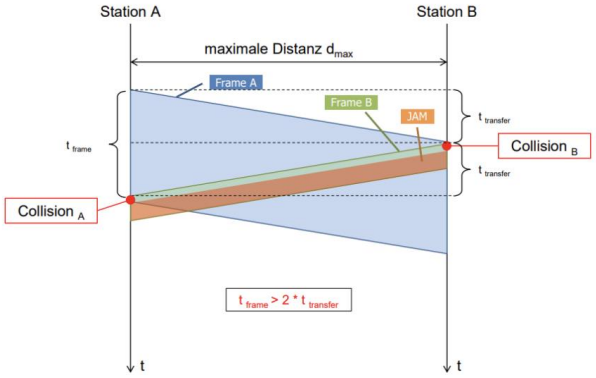
- Ohne Repeater $t_{frame} > 2 \cdot t_{transfer}$
- Mit Repeater $t_{frame} > 2 \cdot (\sum t_{transfer} + \sum t_{forwarding})$

Maximale Ausdehnung eines Segments

$$t_{frame} = \frac{Framesize_{min}}{Bitrate}, \quad t_{transfer} = \frac{d_{max}}{C_{Medium}}$$

Ein Knoten kann Kollisionen lokal nur erkennen, solange er selbst am Senden ist.

$$d_{max} < \frac{1}{2} \cdot \frac{Framesize_{min}}{Bitrate} \cdot C_{Medium}, \quad d_{max} < \frac{1}{2} \cdot \frac{576\ Bit}{10 \cdot 10^6 \cdot Bit/s}$$



⇨ Hub / Repeater erkennt Kollisionen wenn gleichzeitig von mehreren Ports Frames empfangen werden.

Switched LAN und Ethernet (Ergänzung 2 Schicht 2)

Switch / Bridge

⇨ Verwenden «Filtering Database».

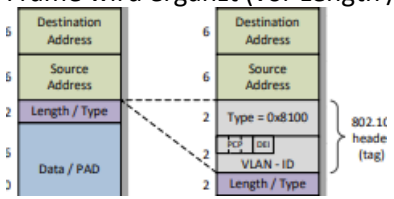
⇨ Switch lernt nur die Senderadressen nicht den Empfänger.

⇨ Unbenutzte Einträge werden nach einer gewissen Zeit gelöscht.

⇨ *Port Mirroring möglich.*

VLAN

Bildet eine Grenze für eine Broadcast-Domain (Grenze für Verteilung von Broadcast-Frames).
Ethernet Frame wird ergänzt (vor Length / Type):



⇨ Maximale Framelänge wird um 4 Bytes auf 1504 erhöht.

⇨ *Switches besitzen Ingress/Egress.*

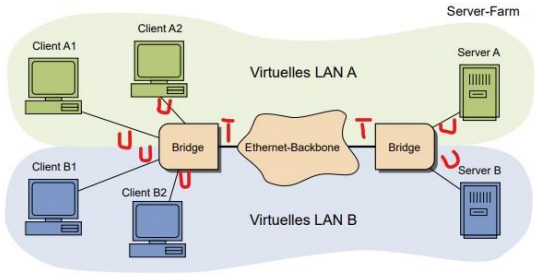
- **PCP:** Frame mit Priorität (8 Stufen). Achtung: Dadurch könnte es sein, dass gewisse Frames nie weiter gesendet werden!
- **DEI:** Frames mit 0 markieren, welche bei Überlastung zuerst verworfen werden.

⇨ Wenn Buffer von Switch voll.

⇨ Theoretisch Max. 2^12 – 2 VLANS möglich.

⇨ VLAN mit ID 1: Default (für untagged Frames).

> VLAN Tagging:
Wird von den Switches gemacht. Frames werden aber inkl. Tagging zum Empfänger gesendet (müssen daher fähig sein zu entschlüsseln).



⇨ Hier wäre Ethernet Backbone = Trunk

- Egress: An welchen Ports kann mit welchem VLAN gesendet werden. Zusätzlich wird bestimmt ob getagged.
- Ingress: Legt fest, welche VLAN ID für eingehende Pakete von einem Port zugewiesen werden.

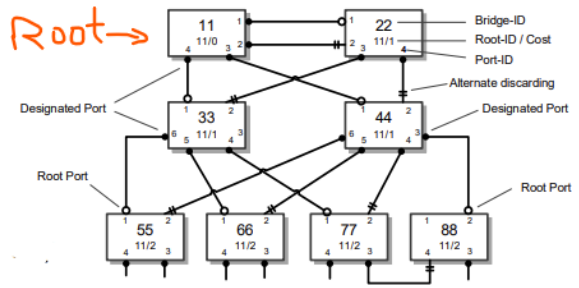
Spanning Tree (Redundanz Protokoll)

Ziel: Alle Segmente in einem Netzwerk loop-frei.
Redundanz (anders wie INCO): Keine mehreren Wege zum gleichen Empfänger.

⇨ Sperrt alle Wege ausser einen.
⇨ Fehlerfall: Wenn möglich ein neuer Weg, welcher gesperrt war, öffnen (Algorithmus wiederholen).
⇨ Alle Knoten werden einmal verbunden.

> Ablauf:

1. Root bestimmen mittels *Bridge-Identfier* (Priorität, MAC-Adresse)
2. Direkt angeschlossene Bridges bestätigen (verbinden)
3. Weitere Verbindungen abhängig von *Kosten* und *Bridge-Identifier* eintragen



Leistungsmerkmale von Bridges

Anzahl Ports	Steckergrösse ist im Extremfall die Limitierung
Adresstabelle	Wie viele Stationen können im LAN existieren
Filterrate	Maximale Frames / s / Port (Empfangsrichtung)
Transferrate	Maximale Frames / s / Port (Senderichtung)
Backplane / Fabric Kapazität	Maximaler Gesamtdurchsatz zwischen allen Ports
Architektur	**Store-and-Forward**: Frame wird komplett empfangen und dann weitergeleitet **Cut-Through**: Frame wird schon nach Decodierung der Zieladresse weitergeleitet. Leitet auch korrupte Frames weiter, in der Regel aber kein Problem **Adaptive Cut-Through**: Schaltet bei hoher Fehlerrate automatisch auf Store-and-Forward um
Konfigurierbarkeit	Unmanaged (keine Möglichkeit z.B. VLANs einzurichten) oder Managed (via Konsole oder Web Interface)
Energieverbrauch	Wird zunehmend wichtiger in Data Center Anwendungen

Ethernet Systeme

- *Autonegotiation* Ermittlung der besten Betriebsart durch Austausch der Leistungsmerkmale zweier Netzwerkkomponenten. →XBASE-T?
- *Link Pulses* NLP = Link Presence Detection
  FLP = Autonegotiation, Autopolarity

	10BASE-T	100BASE-TX	1000BASE-T	10GBBASE-T
Kabelkategorie	CAT3 - 16 MHz CAT5 - 100 MHz	CAT5 - 100 MHz CAT6 - 250 MHz	CAT5 - 100 MHz CAT6 - 250 MHz	CAT6A - 500 MHz CAT7 - 600 MHz CAT7A – 1000 MHz
Line Coding	Manchester 2 Aderpaare simplex	MLT-3, 4B5B 2 Aderpaare simplex	PAM-5, 8B/10B 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	FLP	FLP	FLP

Kompatibilität 10/100/1000BASE-T wird erreicht durch

- **Beibehaltung** von Frame Format und Schnittstelle zwischen PHY und MAC
- **Autonegotiation** mittels FLP bursts / NLP

Internet Protokolle (Schicht 3)

Router

⇨ Routing: Durch statische Konfiguration oder dynamisch durch Routing-Protokolle.
⇨ Forwarding: Durch Routing Tabellen.

- Kümmert sich nicht um retransmit!
- Reihenfolge von Paketen kann sich ändern wenn Pakete unterschiedliche routen nehmen.
- Beim Router gehen Datalink und Physical Layer Komponenten eines Frames weg! (Fügt neue hinzu)!

Adressierungsschema / Routing

> Flaches Adressraum / Routing:

- Einfach ein paar Bits/Bytes (Bspw. AHV).
- Führt zu grossen Adresstabellen.
- Routingtabelle hat alle bekannten Netze.

> Hierarchisches Adressraum / Routing (Default):

- Man soll bei den Adressen erkennen können zu welchem Netz sie gehören (Bspw. Postanschrift).
- Arbeitet mit Defaulteinträgen.

⇨ IP-Adresse identifiziert ein Host-Interface (nicht Host).
⇨ Netzadressen in einer Routingtabelle nach der Länge sortiert (0.0.0.0 = default daher zu unterst).

Grundsätze des Internets

- Jedes Netzwerk soll für sich selbst funktionsfähig sein
- Die Kommunikation basiert auf «best effort»
- Die Verbindung der Netze erfolgt durch Black Boxes
- Keine zentrale Funktionssteuerung wird benötigt

Subnetting (IPv4)

Netzadresse «Netz|0*» und Broadcastadresse «Netz|1*» steht für einen Host nicht zur Verfügung!

> Adressbereich Klassen:

Klasse	Adressbereich	Anzahl Netze	Interfaces pro Netz
A	1.0.0.0 – 127.255.255.255	127	16'777'214
B	128.0.0.0 – 191.255.255.255	16'384	65'534
C	192.0.0.0 – 223.255.255.255	2'097'152	254
D	224.0.0.0 – 239.255.255.555	Multicast Adressen	
E	240.0.0.0 – 255.255.255.255	Reserviert für zukünftige Nutzung	

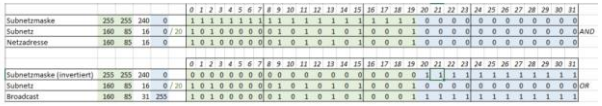
Private Adressbereiche (werden im Internet nicht weitergeleitet):

Klasse	Netzadresse(n)	Anzahl Netze	Subnetzmaske
A	10.0.0.0	1	255.0.0.0
B	172.16.0.0 – 172.31.0.0	16	255.255.0.0
C	192.168.0.0 – 192.168.255.0	256	255.255.255.0

- ⇨ Maske alleine nicht möglich eine Klasse zu definieren (Bspw. 255.255.255.255 nicht nur in Klasse C)
- ⇨ 127.0.0.0/8 ist für Loopback Test reserviert (localhost).

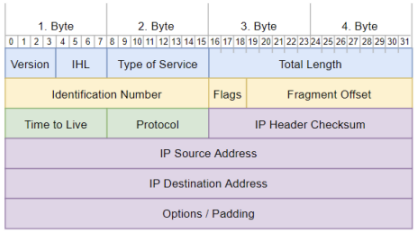
> Beispiel:

- Interface 000…000 32 – Länge vom Subnetz
- Subnetzmaske 255.255.240.0 1111'1111.1111'1111.1111'0000.0000'0000
- Subnetz 160.85.16.0/20 20 = Länge



IP Paket

⇨ Verbindungslos und unzuverlässig.



0	00000000
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

Ein IP-Packet besteht aus einem Header (min. 20 Byte) und Nutzdaten.

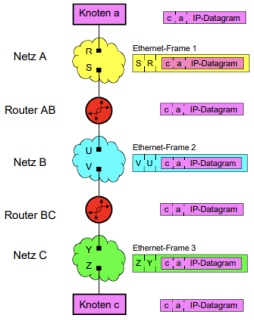
- Version IPv4 / IPv6
- IHL Header Length in 4-Byte (20 Byte → IHL = 5)
- Type of Service Erlaubt Priorisierung
- Total Length Länge des IP-Packets (Header + Nutzdaten)
- ID Number Identifikation des IP-Pakets / Fragmente
- Flags Kontroll-Flags für Fragmentierung
- Fragment Offset Gibt an, wo ein Fragment hingehört
- Time to Live Hop-Counter, 0 → Paket wird verworfen
- Protocol Übergeordnetes Protokoll

IP Paket Übertragung

⇨ Ethernet Frames werden bei jedem Router erneuert!

⇨ Router erneuert im IP Paket nur die TTL und somit auch die Prüfsumme.

Bemerkungen:
(1) Knoten a hat auch als Host eine IP Tabelle.
(2) Router haben pro Port separate Netzadressen.
(3) Wenn TTL = 0 wird ICMP an Sender geschickt.

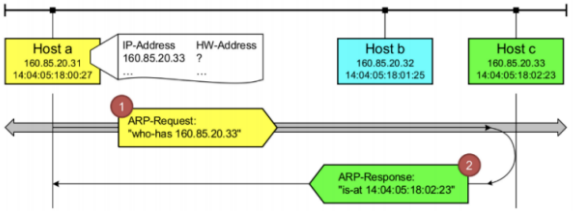


Adressauflösung

> ARP (Address Resoultion Protocol):

- Fragt im eigenen (lokalen) Netz mittels Broadcast, wer die entsprechende IP Adresse hat – *ohne IP Header* (Sender IP/HW und Empfänger IP/HW im Paket).

⇨ Der Host mit der angefragten IP Adresse sendet dann seine MAC Adresse zurück.



⇨ **Spezielle Request ARP Komponenten:**

- **Dest. Adresse vom Ethernet Header:** FF-FF-FF-FF-FF-FF
- **Ziel-HW-Adresse vom ARP Header:** 00-00-00-00-00-00

> ICMP (Internet Control Message Protocol):

- Prüft Verbindung zu einem Router/Host und misst die Round-Trip-Time (Zeitdifferenz zwischen Senden und wieder Empfangen der Ping Antwort).

IP Paket Header enthält ungültigen Wert.
Bspw. Don't Fragment (DF) Bit gesetzt, aber MTU zu klein.
Beinhalten die gleichen Daten.

ICMP-Typ	Bedeutung (Fehler)
3	Destination Unreachable
4	Source Quench
5	Redirect
11	Time Exceeded
12	Parameter Problem

ICMP-Typ	Bedeutung (Information)
0	Echo Reply
8	Echo Request
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

TTL abgelaufen oder reassemblieren innerhalb einer Zeit nicht möglich.

Wenn Host H ein IP Paket an einen Router R1 sendet und dieser feststellt dass der nächste Router R2 im gleichen Netz wie H ist und im nächsten Mal direkt an R2 senden soll.

Ports gewürfelt (sonst blockiert)

Beispiel: Ein Client (C) kontaktiert einen DNS-Server (S) via UDP:
- Anfrage C → S: Source Port: 59327 Destination Port: 53
- Antwort S → C: Source Port: 53, Destination Port: 59327

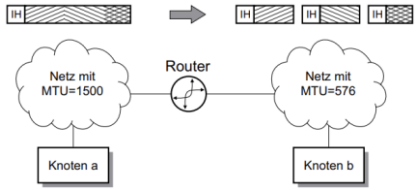
Transport Layer (Schicht 4)

Fragmentierung und Reassembly

⇨ Sender kennt die zu durchlaufenden Netz MTUs nicht. Daher werden die IP Pakete (max. 65535 Byte) falls nötig fragmentiert.

- Wichtig: Jede Fragmentierung ist in einem eigenständigen IP Paket.

> Fragmentierung (Beim Sender oder Router):

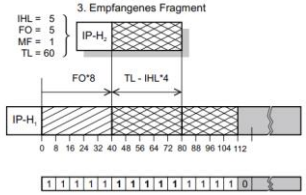


IP Paket Header Komponenten:

- **Total Length:** Länge des Fragments.
- **ID Number**: Eindeutige Kennung des ursprünglichen IP Pakets.
- **Flags: 1:** Immer 0, **2 (DF):** 0=May/1=Don't Fragment, **3 (MF):** 0 = Last/1=More Fragm.
- **Fragment Offset:** Gibt in Bytes an wohin (bis zu 8'192 Fragmente möglich).

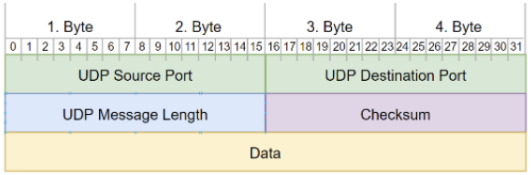
1. Länge der Nutzdaten = Vielfaches von 8 Bytes
2. Die Pakete haben die gleiche und grösstmögliche Länge

> Reassembly (Beim Empfänger / Endknoten):



UDP (User Datagram Protocol)

⇨ Multiplexen und Demultiplexen von Datagramme zu den Applikationen *(wenn Paket an Host angekommen ist, braucht es noch Information um es der richtigen App/Prozess zu geben (mittels Port)).*



⇨ Verbindungslos und unzuverlässig.

TCP (Transmission Control Protocol)

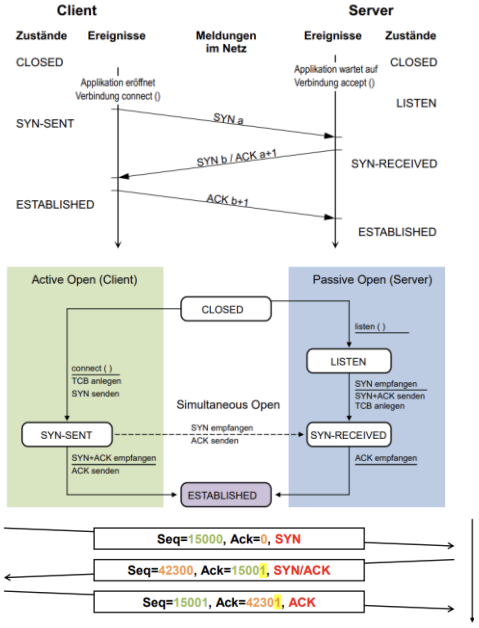
- Sequence-Nr. — Nummer zur Ordnung der Segmente
- Acknowledgement-Nr. — n + 1 → Daten korrekt und vollständig
- Data Offset — Gibt an wo Daten beginnen / enden
- ECN-Flags — Explicit Congestion Notification
- Control Bits — URG, ACK, PSH, RST, SYN, FIN
- Window — Verfügbare Puffergrösse
- Urgent Pointer — URG = 1 → Position der wichtigen Daten
- Options — Häufigste Verwendung: MSS

⇨ Verbindungsorientiert und zuverlässig.

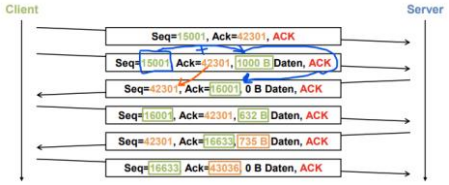
⇨ Min. 20 Bytes, Max. 60 Bytes

TCP Verbindungsphasen

> Verbindungsaufbau:



> Datenaustausch:



⇨ ACK Flag immer gesetzt.

⇨ Sender nimmt die Nr. die er als Seq. Nr. bekommen hat, addiert diese mit den Anzahl Datenbytes die er bekommen hat und setzt diese als Ack.

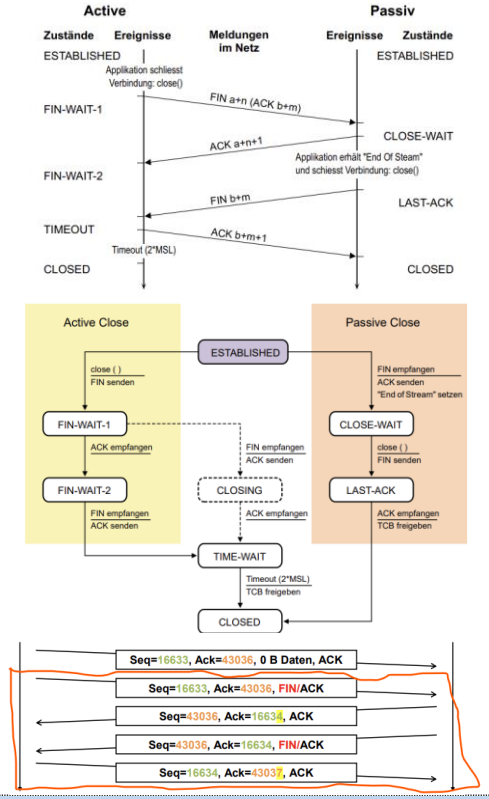
LISTEN — Auf Anforderung warten
SYN-SENT — Anforderung geschickt
SYN-RECEIVED — Anforderung erhalten
ESTABLISHED — Verbindung besteht

System Ports (*Well-Known*) — **Feste Port**-Nummern, für bekannte Appl. reserviert
User Ports (*Registered*) — Reservierter Bereich für herstellerspezifische Appl.
Dynamic / Private Ports — **Frei verfügbare** Ports

System Ports	User Ports	Dynamic Ports
0 - 1023	1024 - 49'151	49'152 - 65'535

⇨ Seine Nr., die er als Ack Nr. bekommen hat, nimmt er und setzt sie als Seq. Nr.

> Verbindungsabbau:



Abbauanforderung geschickt
Abbauanforderung bestätigt
Auf Lokale Verbindung warten
Verbindungsabbau bestätigt
Letzte Bestätigung gesendet

FIN-WAIT-1 FIN-WAIT-2 CLOSE-WAIT LAST-ACK TIME-WAIT

TCP: Erkennen verlorener Nachrichten

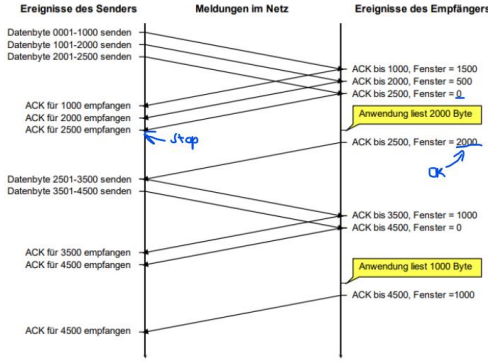
Pakete werden nach einer bestimmten Zeit erneut übertragen, wenn keine Bestätigung (Nachricht mit Ack. Nr.: Die gesendete Seq. Nr. + Anzahl Bytes) kommt.

Gewichteter Mittelwert *SRTT (Smoothed Round-Trip Time)*
Streuung RTTVAR des *SRTT* der Abweichungen
Retransmission Time-Out RTO

$\alpha = 0.125$: $SRTT_n = (1-\alpha)\cdot SRTT_{n-1} + \alpha \cdot RTT_n$
$\beta = 0.25$: $RTTVAR_n = (1-\beta)\cdot RTTVAR_{n-1} + \beta \cdot |SRTT_n - RTT_n|$
$RTO_n = SRTT_n + 4 \cdot RTTVAR_n$

TCP: Fluss-Steuerung (Sliding Window)

- Überlast des Empfängers
- Stop-and-Wait (Sender wartet bis Empfänger Bestätigung schickt) sehr ineffizient. **Daher «Sliding Window».**



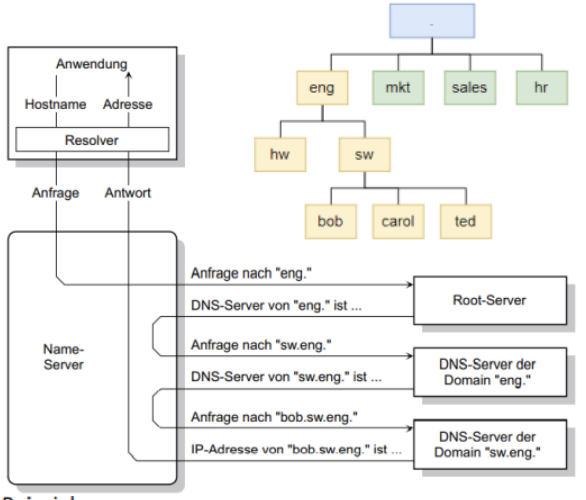
Fenstergrösse im Window Feld des TCP Headers.

TCP: Überlast Steuerung (Congestion Control)

⇨ *Fluss-Steuerung schütz nur Empfänger vor Überlast.*
⇨ Sender schickt Daten bis min{Congestion Window, Advertised Window} erreicht.
⇨ Verwendet den Paketverlust als Masseinheit der Überlastung. Reagiert durch Absenken der Übertragungsrate.
⇨ Ist eine lokale Variable beim Sender.

Application Layer (Schicht 5-7)

DNS (Domain Name Space)



Beispiel

- *bob.sw.eng.* Fully Qualified Domain Name
- *.* Root
- *eng* Top Level Domain
- *sw* Second Level Domain

- Name Server kennt die IP Adressen zu den Hostnamen in seiner Zone.
- Gleiche Domänenamen nicht erlaubt.

DHCP (Dynamic Host Configuration Protocol)

- ⇨ Basiert auf UDP
- ⇨ Dynamische Zuweisung von IP-Adressen.
- ⇨ BootP: Fixe Zuordnung MAC <-> IP Manuel

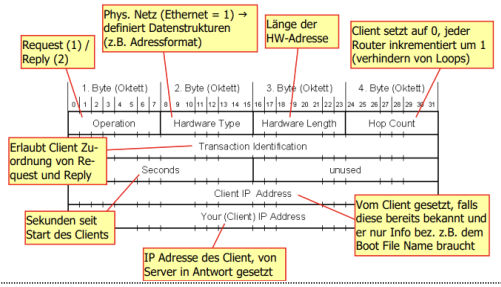
> Ablauf:

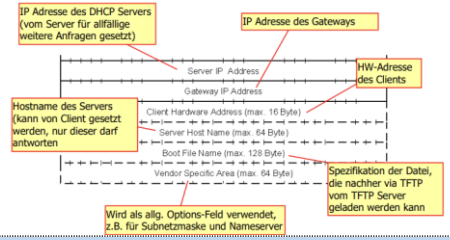
(1) Client sucht DHCP Server mittels Broadcast:

L5	⇨ Offer
L4	SP: 68 DP: 67
L3	SIP: 0.0.0.0 DIP: 255.255.…
L2	SMAC: Eigene MAC DMAC: FF:FF:…

(2) DHCP Server antworten mit offers.
(3) Der Client wählt einen Server und fordert eine Auswahl der angebotenen Parameter (DHCP request).
(4) Der Server bestätigt mit einer Message, welche die endgültigen Parameter enthält.
(5) Vor Ablauf der Lease-Time erneuert der Client die Adresse. Clients die offline gehen werden die Lease-Time nicht erneuern (darum dann automatische Freigabe).

> Header:

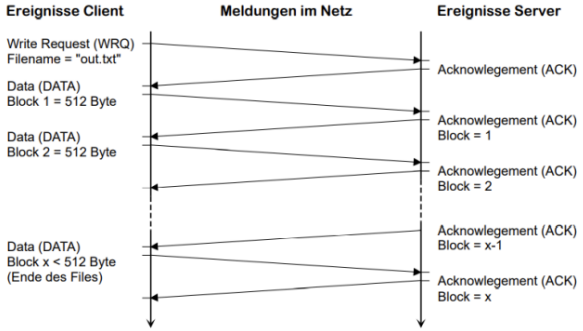




TFTP (Trivial File Transport Protocol)

- ⇨ Basiert auf UDP (Port 69) trotz (eigener) Zuverlässigkeit, da entwickelt für Gerät mit minimalen Möglichkeiten und UDP einfacher.
- ⇨ Zuverlässigkeit durch Stop-and-Wait.

> Senden einer Datei:

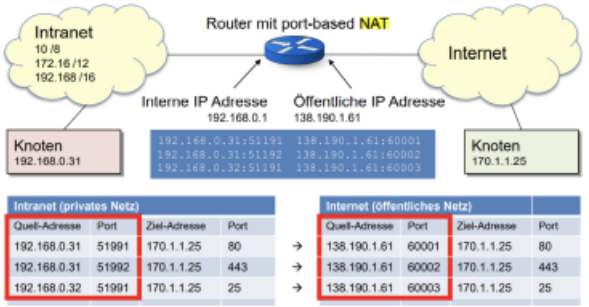


- ⇨ Lesen genau gleich einfach anders herum (mit RRQ) (Client macht dann immer ACK).

HTTP (Hypertext Transfer Protocol)

- ⇨ Basiert auf TCP (Port 80)
- Ist Zustandslos (Nachfolgende Transaktionen sind unabhängig).
- Wenn html Seite geladen werden Links
  - wie Bilder nicht geladen und müssen dann nochmals (in der gleichen TCP Verbindung oder neuen bei HTTP 1) angefragt werden.
- Werden mittels URL eindeutig lokalisiert.
- GET Request mittels «\r\n» Zeilen einteilen und leere Zeile beendet Request.

NAT (Network Address Translation)



Intranet (privates Netz)

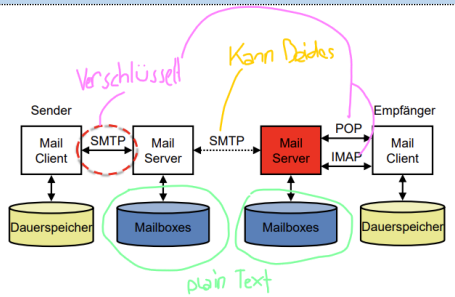
Quell-Adresse	Port	Ziel-Adresse	Port
192.168.0.31	51991	170.1.1.25	80
192.168.0.31	51992	170.1.1.25	443
192.168.0.32	51991	170.1.1.25	25

Internet (öffentliches Netz)

Quell-Adresse	Port	Ziel-Adresse	Port
138.190.1.61	60001	170.1.1.25	80
138.190.1.61	60002	170.1.1.25	443
138.190.1.61	60003	170.1.1.25	25

- Router mit NAT ändert bei ausgehenden Paketen die Src-IP-Adresse und die Src-Port Adresse (und Prüfsummen!) und speichert diese in einer Tabelle (kann auch statisch).
- ⇨ Statisch: Kann eine private IP Adresse fix an eine öffentliche (Port) binden!
- Extern verwendete Ports können frei gewählt werden.
- Pro Dienst/Port Nr. nur einen lokalen Server.
- ⇨ Wird gemacht, um mehr IPv4 Adressen «zu bekommen» (privat -> öffentlich).

E-Mail Protokolle (SMTP & POP3)



> SMTP: (Mails senden)

- Basiert auf TCP (Port 25)
- Definiert wie E-Mail msg gesendet werden

> POP: (Mails empfangen)

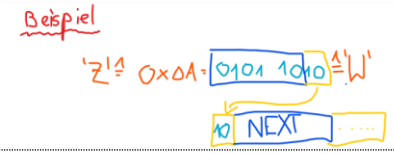
- Können Mails aus den Mailboxes geholt werden und in den Dauerspeicher gelagert werden.

> Mail Erweiterungen:

- SMTP basiert auf 7-Bit ASCII Zeichen.
- ⇨ Daher Codierung von 8-Bit mittel Base64
- ⇨ Info nötig, wo neue Komponenten in Mail beginnen und welchen Typ mittels MIME.

Nur E-Mail Client interpretiert MIME TYPEN.

Value	Binary	Encoding	Value	Binary	Encoding	Value	Binary	Encoding	Value	Binary	Encoding
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/



OSI-Modell Informationen

Verbindungslos / -orientiert

> Verbindungslos:

- Lediglich Datenaustausch (send & forget).
- Darum möglich jederzeit Daten zu senden.
- Man kann hierbei theoretisch einfach nochmals senden wenn kein Response (Protokollabhängig).
- Einfach umsetzbar.

> Verbindungsorientiert:

- Reihenfolge der Daten bleibt erhalten.
- Verbindungsaufbau, Datenaustausch, Verbindungsabbau
- => Ziel muss bereit sein.
- Bspw. HTTP

Zuverlässig / Unzuverlässig

> Zuverlässig:

- Kein Datenverlust.
- Sicherung durch Fehlererkennung und Fehlerkorrektur.
- Bspw.: Datei (Filetransfer, Backup, Datenbank-Transaktionen).

> Unzuverlässig:

- Möglicher Datenverlust.
- Keine Sicherung (keine Fehlererkennung).
- Bspw.: Audio, Video (schlecht bei Audio-Video-Sync).

OSI-Modell