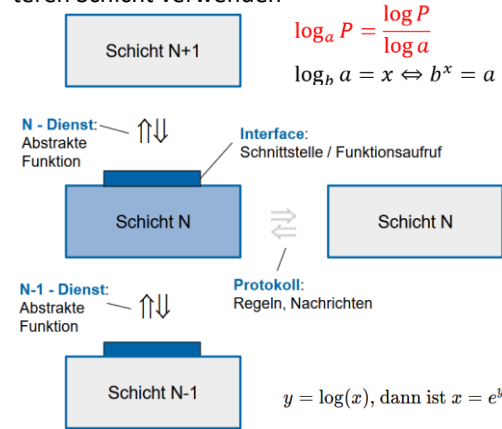


Schichtenmodell

Eine Schicht bietet nur der oberen Schicht ein Interface an, es kann nur das Interface der unteren Schicht verwenden



Dienst(Sendet und empfängt Daten)

Verbindungsorientiert	Verbindungslos
Session-Aufbau und -Abbau, Zustandsbehaftet	Keine Ressourcenreservierung, kein Gleicher Pfad

Zuverlässig	Unzuverlässig
Staukontrolle, Flusskontrolle, Reihenfolgegarantie, Fehlererkennung&Korrektur, Neuübertragungen	geringe Latenz, wenig Overhead, Broadcast/Multi, Best-Effort, Datenverlust möglich, Pfad dynamisch

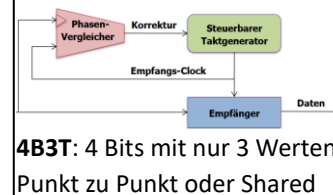
Physical Layer

Ungesicherte Strom Übertragung, seriell oder parallel
Verkehrsbeziehung: Simplex(Eine Richtung), Halbduplex(Zwei Richtungen), Vollduplex(Kanal pro Richtung)
Kopplung: Punkt-Punkt, Shared Medium
Bandbreite: In Hertz **Kanalkapazität:** Mit Rauschen

OSI-Modell

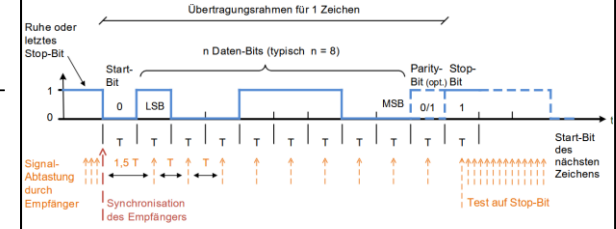
Serielle synchrone

Mit extra Leitung für Takt oder Codierung. Nachteil Codierung extra Logik. Mit Leitungscodes, sollen effizient und möglichst gleichspannungsfrei sein. Z.B. AMI Codes, braucht aber mehr als binär



Seriell asynchrone Übertragung

Letzte Abtastung muss noch im Zeitfenster liegen.

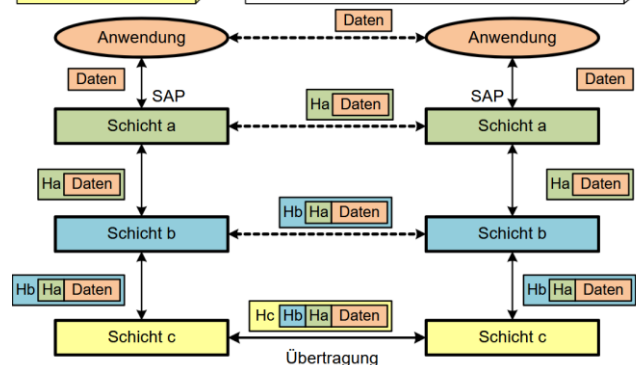
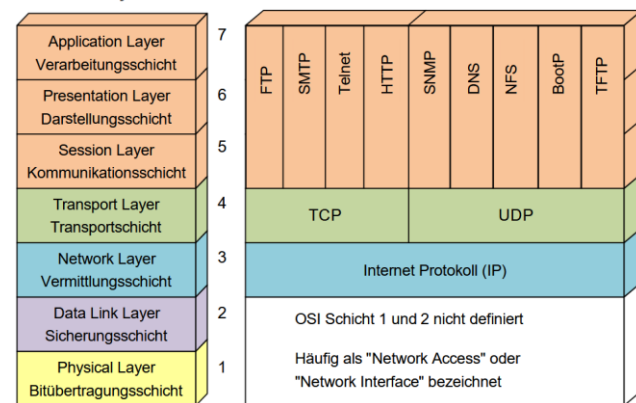


Datenübertragungsrate

Symbol: übertragenes physikalisches Signal
Bit: Informationsgehalt (Anzahl unique N in binär)
Max Symbolrate: $R_s = 2B$; **Zeichen:** «A» MBd
Baudrate: Leitungs-Symbole pro Sekunde (Hertz) B
Maximale Bitrate: $R_b \leq R_s * \log_2 M$
Unterscheidbare Signalzustände: $M = 1 + \frac{A}{\Delta V}$

OSI

beim Sender nach unten, und beim Empfänger nach oben
 OSI Layers



OSI - Layer

1. Übertragung von Rohdaten als elektrische Signale, Lichtimpulse oder Funkwellen. Medium z.B. Kabel.
2. Gesicherte Übertragungsstrecke zwischen direkt verbundenen Knoten. Framing, Fehlererkennung, Korrektur (bei Ethernet keine auf dem MAC-Layer) und Flusskontrolle; unterteilt in MAC- und LLC-Teile. Adressierung (genügend gültige MAC-Adressen), Media Access Control (CSMA/CD)
3. Routing, IP-Adressierung und Weiterleitung von Datenpaketen. Es gibt die **Diensttypen** Leitungsvermittelt und Paketvermittelt. **Leitungsvermittelt:** Es wird eine feste Verbindung zwischen Sender und Empfänger aufgebaut, die während der gesamten Kommunikation bestehen bleibt (z. B. klassische Telefonie). **Paketvermittelt:** Daten werden in einzelne Pakete aufgeteilt und über verschiedene Wege unabhängig zum Empfänger gesendet, wo sie wieder zusammengesetzt werden (z. B. Internet mit IP).
4. Bereitstellung Übertragungsdienste
5. Verwaltung von Sitzungen und Steuerung von Verbindungen.
6. Datenformatierung, Verschlüsselung, Komprimierung.
7. Benutzernahe Protokolle wie HTTP, SMTP, E-Mail.

Ausbreitungsgeschwindigkeit

Beispiel: **Licht in Glas** mit Brechungsindex $n \approx 1.5$

$$c_{\text{Glas}} = \frac{c_0}{n} = \frac{299'792'458}{1.5} \approx 200'000 \frac{\text{km}}{\text{s}}$$



Beispiel: **El. Signal in Leiter** mit Permittivität $\epsilon_r = 2.25$

$$c_{\text{Leiter}} = \frac{c_0}{\sqrt{\epsilon_r}} = \frac{299'792'458}{\sqrt{2.25}} = \frac{299'792'458}{1.5} \approx 200'000 \frac{\text{km}}{\text{s}}$$

Störungen in Übertragungsmedien

- Kapazitive Störungen:** Signalüberlagerung durch elektrische Felder benachbarter Leiter. Shielding als Lösung.
- Induktive Störungen:** Magnetische Wechselfelder verursachen unerwünschte Ströme in benachbarten Leitungen. Twisted Pair als Lösung
- Übersprechen (Crosstalk):** Störungen durch benachbarte Signale innerhalb eines Kabels. (NEXT- Sender, FEXT - Empfänger) Kabel und Steckerqualität als Lösung CAT 1-7
- Glasfaser:** Multimode(günstig mit begrenzter Reichweite) & Dispersion

Übertragungsmedien

Signaldämpfung: $dB = 10 * \log \frac{P_1(\text{Eingangsleistung})}{P_2(\text{Ausgangsleistung})} = 10 * \left(\log \frac{U_1}{U_2} \right)^2$

Beispiel: Dämpfung in Glasfaserkabeln

Gegeben: Dämpfung von 0.4 dB/km

Gesucht: Faktor für 2.5 km Glasfaserkabel

$$SNR = \frac{P_{\text{Signal}}}{P_{\text{Noise}}} = \frac{I_{\text{Signal}}}{I_{\text{Noise}}} = \frac{A_{\text{Signal}}^2}{A_{\text{Noise}}^2}$$

$$SNR_{dB} = 10 \cdot \log_{10}(SNR_{\text{linear}})$$

$$Q = 2.5 \times (-0.4) = -1.0 \text{ dB}$$

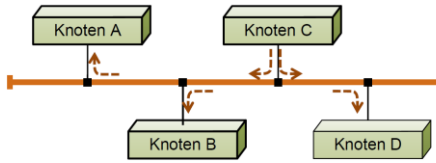
$$I_2 = I_1 \cdot 10^{-1/10} \approx 0.8 I_1$$

→ Nach 2.5 km bleiben noch ca. 80 % der Anfangsintensität übrig. $SNR_{\text{linear}} = 10^{(SNR_{dB}/10)}$

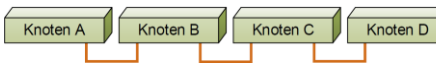
Charakteristika

Topologie:

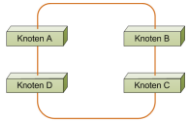
- **Bus:** Alle Stationen sind passiv und hören ab. Werden aktiv beim Senden.



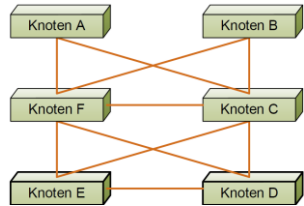
- **Linie:** Nachbarn leiten weiter. Bei Ausfall wird LAN aufgeteilt.



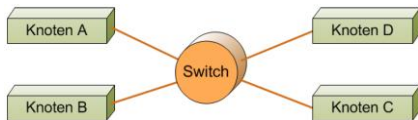
- **Ring:** Benötigt Verfahren um endlosen Kreisverkehr zu stoppen. Redundanz



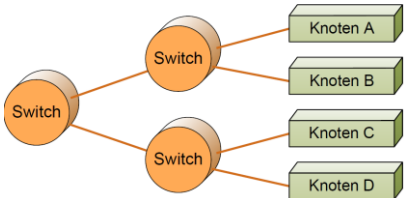
- **Vermascht:** Mehr Redundanz & Kosten



- **Stern:** Zentraler Verteiler



- **Baum:** Erweiterung von Stern, lokale Kommunikation (A->B) möglich



Übertragungsarten: Wird in Frame gesp.

- **Unicast:** Genau 1 Empfänger
- **Multicast:** Gruppe von Empfängern
- **Broadcast:** An alle Knoten

Adressierung MAC

IEEE MAC: 6 Bytes. Davon 3 OUI für Hersteller. Dann 3 als Laufnummer. **2 letztes Bit:** 0= universally administrated address (normal), 1 = local. **Letztes Bit:** 0 = individual, 1 = Group address (z.B. Broadcast).

Ethernet Format

Total Länge des Frames 64 bis 1518 Bytes also ohne 1, 2 und 8. 18 Bytes Frame-(MAC) Overhead. Pro Byte wird LSB (Rechts) zuerst Übertragen. Zahlenwerte mit MSB (Links)

$$\text{Sendedauer: } T_{\text{frame}} = \frac{N_{\text{bit}}}{\text{Bitrate}}$$

$$N_{\text{Bit}} = (\text{FrameSize} + 8) * 8$$

$$\text{Dauer Leitungsbelegung: } T = \frac{N_{\text{Bit}} + 96}{\text{Bitrate}}$$

$$\text{Latenz: } T_{\text{frame}} + t_{\text{transfer}}$$

$$t_{\text{transfer}} = \frac{d}{c_{\text{Leitung}}} \approx \frac{\text{Strecke}}{\text{Speed}}$$

1. Preamble (7 Bytes)

Synchronisationsmuster: 10101010 wiederholt, dient zur Taktsynchronisation.

2. Start Frame Delimiter – SFD (1 Byte):

10101011, den Beginn des Frames.

3. Destination MAC Address (6 Bytes)

4. Source MAC Address (6 Bytes) (HEX, LSB)

5. Ether Type / Length (2 Bytes)

Länge des Payloads (≤ 1500) oder Typ des darüberliegenden Protokolls an (≥ 1536)

6. Payload / Data (46–1500 Bytes)

Muss mindestens 46 Bytes lang sein (Padding falls nötig), maximal 1500 Bytes.

7. Frame Check Sequence – FCS (4 Bytes)

CRC32-Prüfsumme zur Fehlererkennung.

8. Interframe Gap: Zwischen den Frames, 12 Bytes (Kein Teil von Frame)

Ethernet-Geräte

Repeater/Hubs: Verstärkt alles (Fehler)

Switch: Auf Schicht 2. Können Filtern durch Address learning, zuerst beobachten dann filtern. Sollen unsichtbar sein für Endgeräte. Flooding für Multicast

LAN/Ethernet

Redundanz (Spanning Tree)

Wenn es einen Loop im Netzwerk gibt, zirkulieren Pakete mit unbekannter Adresse endlos, wenn es redundante Pfade gibt. Lösung durch Spanning Tree

1. Alle Ports gesperrt. Jeder Switch geht davon aus er ist Root. Start von BPDU-Austausch mit Nachbarn
2. Jeder Switch aktualisiert seine Info zur Root-Bridge (kleinste Bridge-ID) und berechnet die Pfadkosten dorthin. Erneut BPDU senden, wiederholt bis konvergiert
3. Freigabe folgender Ports für Nutzdaten: **Root Port:** Port eines Switches, der den kürzesten Weg zur Root-Bridge hat.

Designated Port: Je Segment der Port, der die beste Verbindung zur Root-Bridge bietet. Alle anderen Ports bleiben im Discarding-Zustand (keine Weiterleitung von Nutzdaten, nur BPDUs).

BPDU: Root-ID (8 Byte), Root-Cost (2 Byte), Bridge-ID des Senders (8 Byte), Port-ID des Senders (2 Byte)

VLAN-Tag

Vor 5. und ist 4 Byte lang (Frame wird länger). Type = 0x8100, 12 Bit für VLAN-ID, 3 Bit für Priority Code Point (QoS, Switches haben mehrere Ausgangs-Queues. Layer 2 unterstützt «Klassen»), 1 Bit für Drop Eligibility Indicator (Kann bei Überlastung zuerst verworfen werden bei 1)

Switched LAN Monitoring

Hub/Multiport Repeater: Hub nach Switch

Tap/Probe: Tap Zwischen Knoten, Low Level Analyse möglich, aber erhöht Latenz

Port Mirroring: Weiterleitung von Paketen auf extra Port. Port ist dann nicht mehr für normale Kommunikation verwendbar.

Leistungsmerkmale von Switches

Anzahl Ports	Steckergröße ist im Extremfall die Limitierung
Adressstabelle	Wie viele Stationen können im LAN existieren
Filterrate	Maximale Frames / s / Port (Empfangsrichtung)
Transferrate	Maximale Frames / s / Port (Senderrichtung)
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 ermittelt beste Betriebsart

Bezeichnung / Norm	Medium	Max. Distanz (Segmentlänge)	Topologie	Bemerkung
10BASE5	50 Ohm Koax	500 m	Bus	Thick Ethernet
10BASE2	50 Ohm Koax	185 m	Bus	Cheapernet
10BROAD36	75 Ohm Koax	3600 m	Bus	CATV-Technik
10BASE-T	2 Paar UTP Cat. 3	100 m	Punkt-Punkt	
10BASE-FL	2 MMF (62.5 µm)	2000 m	Punkt-Punkt	
10BASE-FP	2 MMF (62.5 µm)	500 m	Punkt-Punkt	Passiver Hub
10BASE-FB	2 MMF (62.5 µm)	2000 m	Stern	
10BASE-T1L	Single TP	1589 m	Punkt-Punkt	(2019): Feldbus-Nachfolge
10BASE-T1S	Single TP	25 / 40m	Punkt-Punkt / Multi-Drop	(2019): Automotive

Kabel

Ins Loss: Dämpfungsverlust, Siehe oben

NEXT: Near-End Crosstalk gibt an, wie stark ein Signal auf ein benachbartes Adern paar überspricht. Je höher der NEXT-Wert, desto geringer das Übersprechen

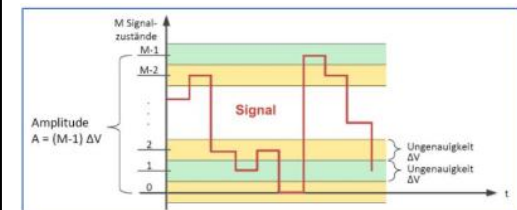
$$\text{NEXT (dB)} = 10 \cdot \log_{10} \left(\frac{\text{Signalstärke}}{\text{Störsignalstärke}} \right)$$

Koaxialkabel	Geeignet für hochfrequente Signale
Twinaxial-Kabel	Hoher Schutz
Twisted Pair (TP)	Häufig im Einsatz (Shielded / Unshielded)
Glasfaser	Hohe Bandbreite, Geringe Dämpfung, Resistent
Drahtgeflecht -> niederfrequente Einstreuungen	
Metallisch beschichtete Folien -> hochfrequente Störungen	

xxlyTP worin **TP** für Twisted Pair steht:

xx steht für die Gesamtschirmung:
U = ungeschirmt
F = Folienschirm
S = Geflechschirm
SF = Schirm aus Geflecht und Folie

y steht für die Aderpaarschirmung:
U = ungeschirmt
F = Folienschirm
S = Geflechschirm



Internet

Es braucht Adressierung, Router, Routing und Fragmentierung. Es soll jedes Netz für sich selber funktionsfähig sein, Kommunikation basiert auf best effort, Verbindung über Router, keine zentrale Einheit nötig

Internet Layer

Hält das virtuelle Netz von Teilnetzen zusammen, dafür leitet er IP Pakete zwischen zwei Hosts weiter. Kümmert sich nur um Transport, keine Fehlerkorrektur, keine feste Reihenfolge.

Broadcast Domain: Layer 2 Bereich

Router

Routing: Möglichst optimale Weiterleitung von Paketen. Statisch in kleinen Netzen. Aufbauen von Routingtabelle

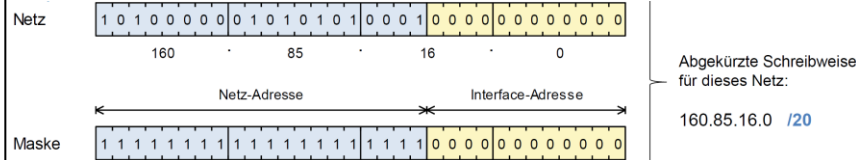
Forwarding: Datenpakete weiterleiten mit der Routingtabelle

IP-Adressen v4

Ist 32 Bit lang, wird unterteilt in «**Netz-Adresse**» und «**Interface-Adresse**».

Subnetzmaske: Bestimmt Grenze zwischen den 2 Teilen der Adresse^

Netzadresse und Broadcastadresse: Tiefste (Interface=0) und höchste Adresse



Rechnen mite Adressen: -2 Da tiefste und höchste reserviert sind!

	IP-Adresse	Subnetzmaske	Netzadresse	Broadcastadresse	Anzahl Adressen inkl. Netz- und Broadcastadresse
a	17.8.7.8	255.255.0.0 /16	17.8.0.0	17.8.255.255	65'536
b	11.7.177.4	255.255.224.0 /19	11.7.160.0	11.7.191.255	8'192
c	144.3.133.1	255.255.192.0 /18	144.3.128.0	144.3.191.255	16384
d	31.4.2.166	255.255.255.248 /29	31.4.2.160	31.4.2.167	8

Routing-Tabelle

Enthält Information wie jede **Netz-Adresse** erreicht werden kann

Flaches Routing: Router kennt jeden Weg zu jedem Ziel, Redundanz möglich durch mehrere Wege ins gleiche Netz. Für Backbone

Hierarchisches Routing: Router kennt die direkt angeschlossenen Netze und einen Router für den Rest. Für Hosts, Access Router

Fehlererkennung/Behebung Data Link Layer

Aus Physical Layer kommen **Bit Error Rate**, wenn nicht hier entdeckt wandern sie weiter nach oben als **Residual Error Rate**. Mit **Parity**, alle 1 mit Parity-Bit sind even/odd oder mit CRC. Error Correction:

Backward: Braucht Rückkanal, muss auf Quittung/Timeout warten

Forward: Empfänger schätzt was versendet wurde(Korrigiert selbst)

Network&Data-L Layer

CIDR

Früher IPs in Klassen aufgeteilt, aber nicht flexibel genug.

Subnetting: Aufteilung in mehrere Subnetze

Ausgangsnetz: 192.168.0.0/24 → 256 Adressen

Subnetting in 4 Subnetze:

- Neue Maske: /26 → je 64 Adressen

- Subnetze: 192.168.0.0/26, 192.168.0.64/26, 192.168.0.128/26, 192.168.0.192/26

Supernetting: Subnetze zusammenfügen

198.51.0110 0100	0000 0000	= C-Netz 198.51.100.0 /24
198.51.0110 0101	0000 0000	= C-Netz 198.51.101.0 /24
198.51.0110 0110	0000 0000	= C-Netz 198.51.102.0 /24
198.51.0110 0111	0000 0000	= C-Netz 198.51.103.0 /24

198.51.0110 01 00.0000 0000 = Subnetzmaske 255.255.252.0 oder /22

Zugriffsmechanismen Data Link Layer MAC

Leader: 1 Leader koordiniert alles, Keine Konflikte aber SPOF(Single Point of Failure)

Token: Ein Token wird in fester Reihenfolge weitergegeben. Ist deterministisch, aber Problem beim Token Verlust. Alternative wird ein Frame geschickt wo jeder Teilnehmer einen festen Platz drin hat

Zeitsteuerung: Wie Fahrplan, braucht genau Planung zwischen Knoten

Carries Sense Multiple Access: Vor senden wird abgehört ob frei. Bei Kollision: erneut versuchen(CSMA/CD) oder durch Hardware (CSMA/CR)

WLAN: Listen-while-talking nicht möglich, also kann Kollision durch Sender nicht erkannt werden. Es werden ACKs gesendet => dann bestätigt

Flow Control: erlaubt einem Empfänger den Sender temporär zu stoppen. Stop-and-Wait-Protokoll: Der Sender wartet auf eine Quittung (ACK), bevor er das nächste Paket sendet.

Clock Drift

Eigentaktabweichungen: Jeder Port hat eigene Clock =>

Temperatur, Alterung oder Toleranz ist anders

Damit der Sample-Zeitpunkt nicht um mehr als $\pm \frac{1}{2}$ Bit-Zeit verschoben wird gilt:

$$N \cdot \delta_{\text{rel}} \leq \frac{1}{2} \implies \delta_{\text{rel, max}} = \frac{1}{2N}$$

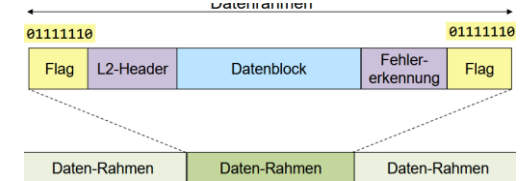
Beispiel 8 Datenbits + 1 Stoppbit $\rightarrow N = 9$:

$$\delta_{\text{rel, max}} = \frac{1}{2 \cdot 9} \approx 0,0556 = 5,56\%$$

Data Link Layer

Framing Async: Ruhezustand, Dann Start Bit. Header – Datenblock – Fehlererkennung

Framing sync: Immer Daten oder Flags



Bitstopfen: Um ein Bitmuster zu garantieren. z.B. Start flag ist sechs 1, dann wird nach fünf 1 eine 0 gestopft, wenn es keine Flag ist

Bit Error Ratio(BER): Anzahl Fehlerhafte Bits verglichen zu Gesamt Bits: Jedes 2. Flasch = BER 0.5

FER/RER: Frame Error Rate ist wie BER für Frames, RER = Residual/Unentdeckt FER=FER x (Frames/s)

Die Betrachtung der Erfolgswahrscheinlichkeit ist einfacher als die der Fehlerwahrscheinlichkeit:

- Um N Bit fehlerfrei zu empfangen, muss jedes einzelne Bit fehlerfrei empfangen werden

$$\text{Erfolgswahrscheinlichkeit für 1 Bit} \quad P_{\text{Erfolg}} = (1 - p_e)$$

$$\text{Erfolgswahrscheinlichkeit für den ganzen Frame (N Bit)} \quad P_{\text{Erfolg, Frame}} = (1 - p_e)^N$$

$$\text{Fehler-wahrscheinlichkeit für den ganzen Frame} \quad P_{\text{Fehler, Frame}} = 1 - (1 - p_e)^N$$

$$\text{Für } p_e \ll 1 \text{ gilt folgende Näherung: } (1 - p_e)^N \approx (1 - N \cdot p_e), \text{ also: } P_{\text{Fehler, Frame}} \approx N \cdot p_e (=FER)$$

Frame Länge: muss optimiert werden auf Nutz Bits und Fehlerwahrscheinlichkeit. Längere Frames: +Mehr Netto Bits, +weniger Overhead; -Mehr Fehler, -Datenverlust bei Fehler höher, -Mehr unentdeckte Fehler

Fehlererkennung: Ist abhängig von der Framelänge

5×10^{-14} unentdeckte Fehler / Frame-Byte

BER 10^{-8} (Maximal zulässiger Wert)

Maximale Frame-Länge: 1'500 Bytes = 12'000 Bit

Wahrscheinlichkeit für unerkannte fehlerhafte Frames oberhalb Data Link Layer

$$RER \leq 1'500 \frac{\text{Bytes}}{\text{Frame}} \cdot 5 \cdot 10^{-14} \frac{\text{Fehler}}{\text{Byte}} = 7,5 \cdot 10^{-11} \frac{\text{Fehler}}{\text{Frame}}$$

ca. jedes 13'000'000'000 Frame ist unerkannt fehlerhaft

Beispiel Backup 1.5 Tbyte:

$$1,5 \cdot 10^{12} \text{Byte} \cdot 5 \cdot 10^{-14} \frac{\text{Fehler}}{\text{Byte}} = 0,075 \frac{\text{Fehler}}{\text{Backup}}$$

Jedes 13. Backup defekt!

Beispiel Gigabit-Ethernet:

$$0,125 \cdot 10^9 \frac{\text{Byte}}{\text{s}} \cdot 5 \cdot 10^{-14} \frac{\text{Fehler}}{\text{Byte}} = 6,25 \cdot 10^{-6} \frac{\text{Fehler}}{\text{s}} = \frac{1 \text{ Fehler}}{44 \text{ h}}$$

Alle 44h ein unentdeckter Fehler!

Hamming-Distanz: Ist die minimale Anzahl Bits, in denen sich zwei beliebige gültige Codewörter eines Codes unterscheiden. Hamming-Distanz h erlaubt (h-1) Fehlererkennung oder h/2 Fehlerkorrektur.



Internet-Protokolle

IP-Header

1. Byte (Oktett)								2. Byte (Oktett)								3. Byte (Oktett)								4. Byte (Oktett)							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL				DiffServ (DS)								Total Length															
Identification Number																Flags				Fragment Offset											
Time to Live								Protocol								IP Header Checksum															
IP Source Address																															
IP Destination Address																															
Optionen																/ Padding															

Version: 4/6, **IHL:** Anzahl Zeilen, max. 15, **DS:** 0-5: DSCP-Klassifizierung, 6-7 ECN: Router kann überlast kommunizieren, **TL:** Länge in Bytes von ganzem Paket max. 65535, **TTL:** Wird bei jedem Weiterleiten verkleinert meist 64/128, **Protocol:** Protokoll der Nutzdaten, **Checksum:** jeder Router berechnet neu, **Options/Padding:** Header muss immer Vielfaches von 4 Bytes sein **IN, Flags, Fragment:** Für Fragmentierung verwendet

Fragmentierung

Sollte im Sender passieren, MTU

IN: Ist für gleich für alle Fragmente, **Flags:**

Feld	Position	Werte	Funktion
	0	0	Reserved, must be Zero
DF	1	0 / 1	May / Don't Fragment
MF	2	0 / 1	Last / More Fragments

Fragment: Position im ganzen Paket

Kapselung

Das IP-Paket wird gekapselt für den Versand. Z.B. in Ethernet Frame für Ethernet, damit wird das IP-Paket nie verändert. Nur Kapselung

Internet Control Message Protocol

Für Fehler und Informationsaustausch. Wird in IP-Paket gekapselt. Nicht garantierte Ankunft.

ICMP-Typ	Bedeutung (Fehler)	ICMP-Typ	Bedeutung (Information)
3	Destination Unreachable	0	Echo Reply
5	Redirect	8	Echo
11	Time Exceeded	13	Timestamp
12	Parameter Problem: Bad IP Header	14	Timestamp Reply

1. Byte (Oktett)	2. Byte (Oktett)	3. Byte (Oktett)	4. Byte (Oktett)
0	1	2	3
Type (= 3)			
Code			
Checksum			
Depends on Code			
IP-Header + 64 Bits of Original Datagram			

Path MTU Discovery: Erkennung MTU auf Pfad

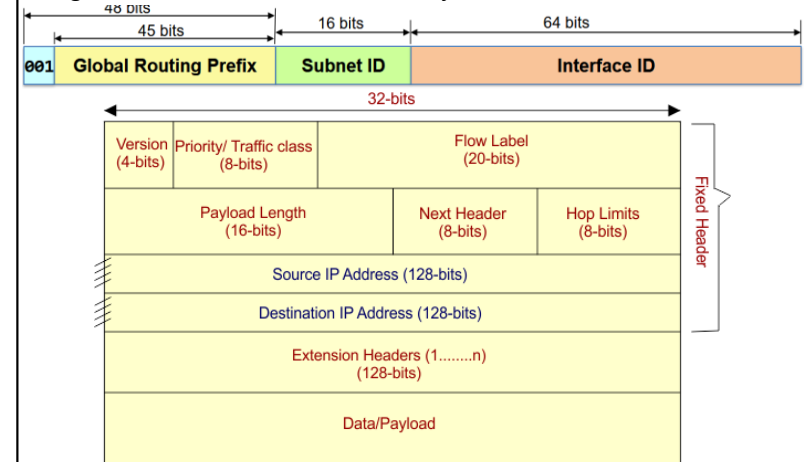
1. Annahme, PMTU = lokale MTU
2. Senden IP mit Länge=PMTU und mit DF=1
3. Empfang von «Destination Unreachable» mit Code 4 «fragmentation needed and DF set»
→ PMTU reduzieren auf «Next-Hop MTU»

Trace route: Diagnose Time Exceeded. Schickt Paket mit TTL=1, dann 2, usw. bis Ziel erreicht

Feld	Wert/Semantik
Type	3
Code	0 = net unreachable, 1 = host unreachable, 2 = protocol unreachable, 3 = port unreachable, 4 = fragmentation needed and DF set, 13 = communication administratively prohibited
Checksum	Prüfsumme über die ICMP Meldung
IP Header + 64 Bits of Original Datagram	Information für den Empfänger zur Zuordnung der Meldung zu einem gesendeten IP

IPv6

Länge von 16 Byte, in hex, linksstehende 0 können weggelassen werden, 0 folge nur durch ::. Anstatt Broadcast jetzt Multicast.



IPv6 Header

Basic Header 40 Byte, dann evtl. Extension Headers in Reihenfolge:

Hop by hop: Von jedem Router verarbeitet

Destination: Von Routern in «Routing extension» verarbeitet

Routing: Liste von Routern

Fragmentation: Von Empfänger für Zusammensetzung verarbeitet

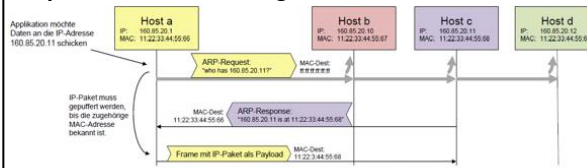
Authentication: Wie Fragmentation

Security: Verschlüsselung der Infos

Destination: Nur von Empfänger verarbeitet

Address Resolution Protocol (ARP)

ARP bleibt lokal, geht nicht Router weiter. Wenn Adresse nicht bekannt ARP-Request (Broadcast) an alle, Besitzer antwortet. Jeder Knoten hat ARP-Cache. Kann verwendet werden, um doppelte Adressen zu erkennen. Bei **Request** ist Target Mac Broadcast, bei **Response** dann die richtige Adresse

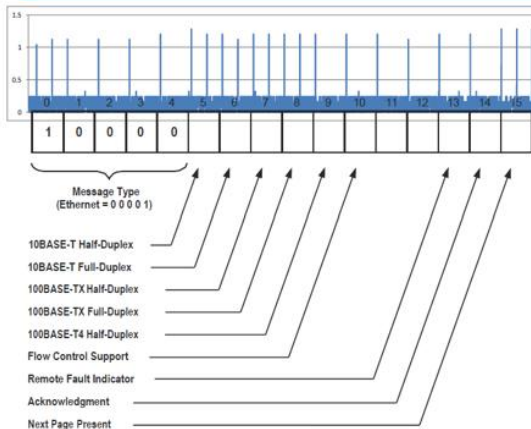


- Die ARP-Tabelle speichert bekannte <IP-MAC> Kombinationen für eine gewisse Zeit
- ARP-Request und ARP-Response sind je in genau einem Ethernet Frame enthalten mit Type 0806

- Beim Request ist die Destination Address FF-FF-FF-FF-FF-FF (Broadcast Frame) und die Hardware Address of Target ist 0

7	1	6	2	max. 1500	4
Präambel	SFD	Destination MAC Adresse	Source MAC Adresse	Protocol Type (= 0806 für ARP)	Daten (= eingebettete ARP Daten)
FCS					

Ethernet Auto-Negotiation



- Austausch der unterstützten 10 und 100 Mbit/s Optionen
- Höhere Datenraten werden über einen «Next Page» Mechanismus ausgehandelt
- Im Praktikum wird die Signalisierung mit FLPs für Performance Messungen explizit gesetzt
- Ein Gerät, das nur NLPs sendet, wird als 10Base-T, Half-Duplex identifiziert (Abwärtskompatibilität)

Nach erfolgreichem Austausch wird automatisch das höchstmögliche gemeinsame Betriebsprofil (Speed/Duplex) aktiviert. Über „Next Page“-Nachrichten lassen sich zudem optionale Features wie Energie-Effizienz (EEE), etc. aushandeln.

Was passiert bei IP-Paket Sendung genau?

Was geschieht bei der Übertragung genau?

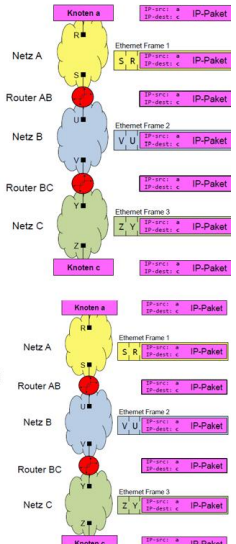
- Knoten a sendet ein IP-Paket an Knoten c → das Paket enthält die IP-Adressen von a und c
- Knoten a konsultiert die Routing Tabelle und sieht:
 - dass c über den Router AB erreicht werden kann, und
 - kennt nun die IP-Adresse von Router AB
- Knoten a generiert ein Ethernet Frame, welches an die Hardware-Adresse S von Router AB gesendet wird
- Router AB empfängt das Ethernet Frame, packt das IP-Paket aus und modifiziert den Header (TTL)
- Router AB konsultiert die Routing Tabelle und sieht:
 - dass c über den Router BC erreicht werden kann, und
 - kennt nun die IP-Adresse von Router BC
- etc.

Was geschieht bei der Übertragung GANZ genau?

- Knoten a sendet ein IP-Paket an Knoten c → das Paket enthält die IP-Adressen von a und c
- Knoten a konsultiert die Routing Tabelle und sieht:
 - dass c über den Router AB erreicht werden kann, und
 - kennt nun die IP-Adresse von Router AB
- Knoten a generiert ein Ethernet Frame, welches an die Hardware-Adresse S von Router AB gesendet wird
- a muss aus der IP-Adresse von Router AB die Hardware-Adresse S herausfinden
- **Adressauflösung**

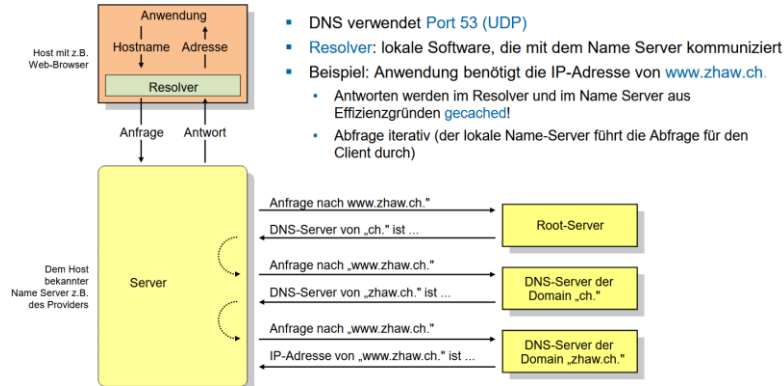


- Die IP-Adressen a und c bleiben während der gesamten Übertragung unverändert



DNS

Namen werden in Bäumen gespeichert. FQDN muss eindeutig sein, alles erlaubt ausser Geschwisterknoten dürfen nicht gleichen Namen haben. Es wird in Zones aufgeteilt, jede Zone hat min. 2 Server.



DNS kann auch andere Daten liefern, es gibt Record Types:

Type	Beschreibung / Funktion	Definiert in
A	IPv4 Adresse des gesuchten Hosts (32 Bit)	RFC 1035
AAAA	IPv6 Adresse des gesuchten Hosts (128 Bit)	RFC 3596
MX	Mail Exchange (Mail Server)	RFC 1035 / 7505
NS	Name Server (Name Server Name für eine Zone)	RFC 1035
CNAME	Canonical Name (primärer Name) für einen Alias zum Host	RFC 1035
TXT	Text Record, in Antworten für verschiedenste Angaben verwendet	RFC 1035

Generische, weltweite Domains:

- **com**: Kommerzielle Unternehmen, sehr gross (ibm.com)
- **edu**: Bildungseinrichtungen, vor allem U.S. Universitäten (mit.edu)
- **net**: Internet (Service) Providers (ripe.net)
- **org**: „Was nirgends oben hineinpasst“, non-Profit Organisation (un.org, wireshark.org)
- **int**: Internationale Bündnisse (nato.int, eu.int)

Generische Domains in den USA:

- **gov**: US Bundesregierung (whitehouse.gov)
- **mil**: US Militär (darpa.mil)

Landesspezifische Domains (ISO 3166):

- **ch, li, de, us, uk...**
- Registrare: RIPE NCC (Europa), APNIC (Asia-Pacific), ARIN (North-America), ...

Neue Top Level Domains:

- Neue Regeln haben thematische und markenspezifische TLDs ermöglicht, so dass die Anzahl TLDs auf weit über 1'000 angestiegen ist
- **aero, biz, coop, info, museum, name, pro...**

TCP-Probleme

Problem	Schicht 2	Schicht 4	Massnahmen bei TCP
Nachrichtenverlust	Pverlust = FER	Pverlust >> FER	Positives ACK
Telegramm-Reihenfolge	fix	kann variieren	Sequenznummern
Round Trip Time	konstant, µs .. ms	variabel, ms .. s	Adaptiver Retransmission Timeout
Überlast des Empfängers	kommt vor	kommt vor	Sliding Window mit dynamischer Fenstergrösse
Überlast des Netzwerks	direkt beobachtbar (Medium)	nur indirekt beobachtbar	Slow Start (Congestion Window)
Neustart von Hosts	direkt beobachtbar	nur indirekt beobachtbar	3 Weg Handshake, Initialisierung Sequenznr.

Application Layer

Network Address Translation (NAPT)

1. Private Hosts (192.168.0.x) kommunizieren über ein gemeinsames Gateway (192.168.0.1), das über eine globale IP (160.85.17.11) verfügt.
2. Beim Verlassen des privaten Netzes: Die private IP-Adresse wird durch die globale IP des Gateways ersetzt. Der private Source-Port (56777) wird durch einen neuen eindeutigen Port ersetzt (52345).
3. Das Gateway speichert eine Verbindungstabelle: (192.168.0.10:56777) → (160.85.17.11:52345)
4. Antwortpakete werden mit dieser Tabelle zurückgeleitet im privaten Netz.

Hauptschwierigkeit: Zustandserhaltung

Statisch (NAT): Es werden manuelle Einträge in einer DB gemacht für jeden Host.

OSI-Verletzung: NAT arbeitet auf der **Network-Schicht**, verändert jedoch Inhalte des **Transport-Headers**. Dadurch müssen **Checksummen** neu berechnet werden. Wenn Verschlüsselung unterhalb Transport-Layer passiert, ist NAPT nicht mehr möglich. Kann umgangen werden mit **NAT-T**, das anstatt Pakete verändern sie in UDP-Pakete verpackt oder mit IPv6

HTTP

Mit TCP auf Port 80, zustandlos, Transaktionsbasiert, ASCII-basiert, MIME-Typen

TCP-Massnahmen

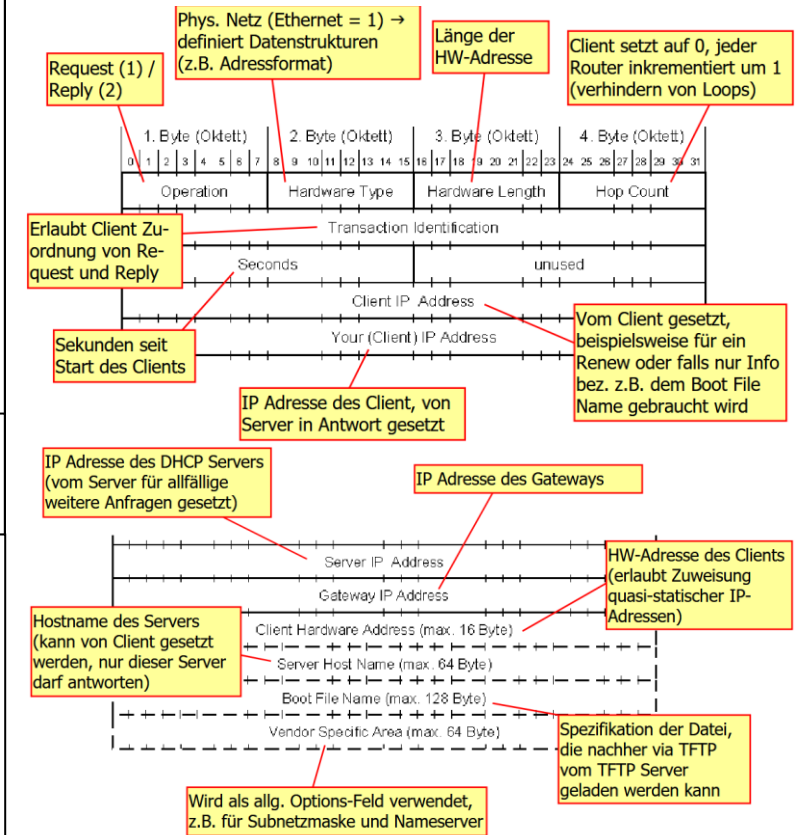
- 32-Bit Sequenznummern – jedes Byte im Datenstrom ist eindeutig identifiziert
- 3-Wege Handshake beim Verbindungsaufbau mit zufälliger Initialisierung der Sequenznummern
- Kontrollierter Verbindungsabbau mit der Möglichkeit, ausstehende Daten zu senden
- Adaptive Timeouts basierend auf Wert und Varianz der gemessenen Round-Trip Zeiten
- Schutz des Empfängers vor Überlast durch dynamische Anpassung der Fenstergrösse beim Sliding Window Protokoll (Advertised Window, wird dem Sender vom Empfänger mitgeteilt)
- Schutz des Netzwerks vor Überlast durch Congestion Control (im Sender) mit dem Slow Start Algorithmus

Dynamic Host Configuration Protocol

Verwendet Port 67(Server) und 68(Client) mit UDP. Client fordert IP und DHCP liefert sie mit einer Lease Time, diese muss immer wieder vom Client erneuert werden, sonst wird IP neu verteilt. Es kann auch andere Daten als IP-Adressen verteilen:

Code	Label	Description
1	Subnet	Subnet mask IP address
3	Router	IP address(es) for routers on the subnet
6	DNSserv	IP address(es) for DNS servers
12	Hostname	Text string for the client host name
15	DNSdomain	DNS domain name

1. Client sucht DHCP-Server mittels Broadcast
2. DHCP-Server antwortet (DHCP offer)
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.



Berechnung

Im Folgenden wird eine asynchrone serielle Schnittstelle mit 115'200 Baud; 8 Dat einem Stop-Bit verwendet (siehe auch Abbildung 6):
Q02 Wie lange ist die Zeit für die Übertragung eines Bits?

$$1/115200=8.68\mu s$$

0,000008681 s oder 8,681 μs

- Zeichnen Sie eine Signalfolge ein, bei der sich logische Signale 1 und 0 abwechseln.



Q03 Welche Frequenz hat das Rechtecksignal ausgedrückt durch T und als numerischer Wert in Hertz?

$$1/8.68 = 0.1152 (115.200 \text{ Hz}) \text{ also etwa } 115.2\text{kHz}, 56000\text{kHz}$$

Q04 Welchem Zeichen entspricht diese Signalfolge?

1,0,1,0,1,0,1,0 -> Der Wert 0x55 (dezimal 85) im ASCII-Code ist der Buchstabe 'U'.

Die Bits werden umgekehrt gesendet:
1 0 0 0 0 0 1 0
Also mit Start- und Stopbit:
0 1 0 0 0 0 1 0 1
(Startbit -> Daten (LSB-MSB) -> Stopbit)

Berechnung von Datenraten

$$\text{Total Bits pro Frame} = 8 \times [(P + 26)] + 96 \cdot \frac{B}{8(P + 26) + 96}$$

Formel für t_{delay} bei Store-and-Forward Switching:

$$t_{\text{delay}} = \frac{L \cdot 8}{R}$$

Dabei ist:

- L = Frame-Länge in Byte
- 8 = Umrechnung von Byte in Bit
- R = Datenrate in Bit/s (hier z.B. 10 Mbit/s = 10 000 000 bit/s)
- Ergebnis in Sekunden

Grundformel bei 10 Mbit/s:

$$\text{Switch Delay (theoretisch)} = \frac{\text{Frame-Länge [Byte]} \times 8}{10\,000\,000} \times 10^6 = \text{Frame-Länge} \times 0,8 \mu s$$

(da 1 Byte = 8 Bit, und 1 Sekunde = 10^6 Mikrosekunden)

HEX Mac

Unten ist der Hex-Dump eines MAC-Frames dargestellt, wie er mit Wireshark aufgezeichnet worden ist.

```
0000: 08 00 2B C3 AC A5 00 00 F8 1A 84 1A 08 00 45 00
0010: 00 2C 1B 31 40 00 08 06 99 5E A0 55 82 2A A0 55
0020: 83 67 04 1A 12 67 00 00 C0 C5 00 00 00 60 02
0030: 20 00 5A A3 00 00 02 04 05 B4 00 00 A3 7C 51 FB
```

a) Markieren und benennen Sie die einzelnen Felder.

Oktett 0-5: Destination MAC-Address (08-00-2B-C3-AC-A5)
Oktett 6-11: Source MAC-Address (00-00-F8-1A-84-1A)
Oktett 12/13: Length / Type -> hier Type = 0x0800
Oktett 14-59: Data / padding
Oktett 60-63: Frame Check Sequence

Beispiele

IP-Adressen

Schritt 3: Netzadresse = IP AND Maske
Nur die ersten 16 Bits bleiben erhalten ->
maske: 11111111.11111111.00000000.00000000
IP: 00010001.00001000.00000111.00001000
Maske: 11111111.11111111.00000000.00000000
-> 00010001.00001000.00000000.00000000
-> 17.8.0.0

Schritt 4: Broadcastadresse
Alle Hostbits (die letzten 16) auf 1:
-> 17.8.255.255

Schritt 5: Anzahl Adressen
 $2^{32-16} = 2^{16} = 65536$

Von IP und Netzadresse auf Subnetmaske:

Schritt 1: Erkenne Präfix / Subnetzmaske
-> IP: 177 im dritten Oktett
-> Netzadresse beginnt bei 160 -> Abstand = 16 -> Blockgröße = $2^4 = 16$
-> $\Rightarrow /20 \rightarrow 255.255.240.0$

Schritt 3: Broadcastadresse
-> Alle Hostbits (12) auf 1 -> 160.0 + 4095 = 175.255
-> Broadcast = 17.7.175.255

Schritt 4: Anzahl Adressen
 $2^{32-20} = 2^{12} = 4096$

Hostbits ergeben sich aus $32 - 20$ (von subnetmaske)

1. Subnetzmaske ermitteln
Schreibe die beiden Adressen binär (nur 3. Oktett wird spannend):
177 = 1011 0001
160 = 1010 0000
-> Bis zum 3. Bit stimmt alles überein.
-> 16 (Netz-/Voll-Bits + 3 Bits im 3. Oktett = /20)
-> Subnetzmaske: 255.255.224.0 (224 = 1110 0000)

Variante 1: Broadcast = Netzadresse + ($2^h - 1$)
Bedeutung:
Du nimmst die Netzadresse als Startpunkt (die erste Adresse im Subnetz) und addierst alle möglichen Host-Adressen drauf - das ergibt die letzte Adresse - Broadcast.
-> $h = 32 - \text{Prefix} = \text{Anzahl Host-Bits}$
-> $2^h = \text{Anzahl aller IPs im Subnetz}$
-> $2^h - 1 = \text{letzte Adresse} - \text{Broadcast}$
Beispiel:
Netzadresse: 192.168.10.0 /24 -> $h = 8$
 $2^8 = 256 \Rightarrow \text{Broadcast} = 192.168.10.0 + 255 = 192.168.10.255$

Netzadresse: hostbits anzahl also z.B. 13 -> 31.255 + netzadresse (255 irrelevant)

a) Betrachtung / Eckdaten eines IP Netzes

Gegeben ist das Netz 172.30.10.0/25.

- Geben Sie in der folgenden Tabelle die Eckdaten für das gegebene Netz an:

Netzadresse:	172.30.10.0
Broadcast-Adresse:	172.30.10.127
Nutzbarer Host-Adressbereich:	172.30.10.1 - 172.30.10.126

- Geben Sie die **Netzmasken** für die drei Subnetze an (kurze Schreibform mit « / » genügt):

Subnetz 1 (für 50 IP-Hosts):	/26 (oder 255.255.255.192)
Subnetz 2 (für 25 IP-Hosts):	/27 (oder 255.255.255.224)
Subnetz 3 (für 25 IP-Hosts):	/27 (oder 255.255.255.224)

- Geben Sie je die **Netzadresse**, die **Broadcastadresse** und die **Anzahl adressierbarer Hosts** der drei Subnetze an:

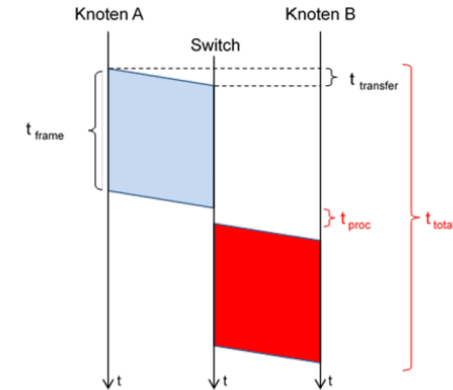
	Netzadresse	Broadcastadresse	Anzahl Hosts
Subnetz 1 (für 50 IP-Hosts):	172.30.10.0	172.30.10.63	62
Subnetz 2 (für 25 IP-Hosts):	172.30.10.64	172.30.10.95	30
Subnetz 3 (für 25 IP-Hosts):	172.30.10.96	172.30.10.127	30

Variante 2: Broadcast = Netzadresse OR (NOT Maske)
Bedeutung:
Du setzt alle Host-Bits auf 1.
Denn die Subnetzmaske ist z.B.:
-> /24 = 11111111.11111111.11111111.00000000
-> NOT (Maske) = 00000000.00000000.00000000.11111111
Dann machst du:
test: 192.168.10.0 OR 00000000.00000000.00000000.11111111
=> Maske: 00000000.00000000.00000000.11111111
Broadcast: 192.168.10.11111111 = 192.168.10.255

c) Gegeben IP + Broadcastadresse
IP: 144.3.133.1 Broadcast: 144.3.191.255
1. Subnetzmaske + Präfix herausfinden
Vergleiche IP & Broadcast Oktett für Oktett:
Oktett IP Broadcast Gleich?
1. 144 144 ✓
2. 3 3 ✓
3. 133 (1000 0101) 191 (1011 1111) X ab Bit 3
4. 1 255 X
-> Im 3. Oktett sind die ersten 2 Bits identisch (10¹), danach variabel = /18.
Maske /18 = 255.255.192.0 (192 = 1100 0000)

Delay

Die Leitungslänge zwischen Switch und den Knoten sei je 50 m, Ausbreitungsgeschwindigkeit $2 \cdot 10^8$ m/s; Bitrate: 10 Mbit/s; Länge der Nutzdaten (im Ethernet Frame): 974 Byte



Bei allen folgenden Berechnungen muss der Rechenweg klar ersichtlich sein!

- Geben Sie hier gemäss Weg/Zeit-Diagramm die Berechnungen an für:

$$t_{\text{frame}} =$$

$$[974 + 8 (\text{Prä-/SFD}) + 12 (\text{MACs}) + 2 (\text{Type}) + 4 (\text{FCS})] \cdot 8 / 10^7 = 8/10^4 = 800\mu s$$

- Geben Sie hier gemäss Weg/Zeit-Diagramm die Berechnungen an für:

$$t_{\text{transfer}} = 50[m] / 2 \cdot 10^8 [m/s] = 2.5 \cdot 10^{-7} = 250\text{ns}$$

- Der Switch hat eine Verarbeitungszeit (t_{proc}) von 10 μs . Ergänzen Sie im obigen Diagramm t_{proc} , und grafisch die Übertragung des Frames vom Switch zum Knoten B.

siehe Grafik (in Rot)

- Geben Sie hier die gesamte Übertragungszeit (Senden des ersten Bits an der Quelle bis zum Empfang des letzten Bits am Ziel) an. Zeichnen Sie t_{total} ebenfalls im obigen Diagramm ein.

$$t_{\text{total}} = 2 \cdot 800 \mu s + 2 \cdot 250\text{ns} + 10\mu s = 1610.5 \mu s$$

Einheit	Symbol	in Sekunden	in Mikrosekunden	in Nanosekunden
1 Sekunde	s	1 s	1 000 000 μs (10^6)	1 000 000 000 ns (10^9)
1 Mikrosekunde	μs	0.000 001 s (10^{-6})	1 μs	1 000 ns (10^3)
1 Nanosekunde	ns	0.000 000 001 s (10^{-9})	0.001 μs (10^{-3})	1 ns

Kabel Protokolle

Standard	Kodierung	1000Base-SX	8b/10b
10Base-T	Manchester NRZ		
100Base-TX	4B/5B + MLT-3	1000Base-LX	8b/10b
100Base-FX	4B/5B + NRZI	10GBase-T	PAM-16
1000Base-T	PAM-5	10GBase-SR	64b/66b
1000Base-SX	8b/10b	10GBase-LR	64b/66b

Subnetze

IP-Subnetz Aufteilung

Sie bekommen von Ihrem Internet Service Provider (ISP) ein privates Klasse-C Netz zugeteilt. In Ihrem Haus befinden sich 4 Parteien, welche sich den Internet-Anschluss teilen. Sie geben jeder Partei **ein gleich grosses Subnetz**, indem sie das Klasse-C Netz 192.168.1.0/24 in 4 Subnetze aufteilen. Geben Sie für alle 4 Subnetze die Netzadresse, die Netzmaske, die Broadcast-Adresse, den Default Gateway sowie die Anzahl adressierbarer Hosts an.

W – DCN/KT Übungsaufgaben Klassifizierung: "Intern"

Subnetz 1	
Netzadresse	192.168.1.0
Netzmaske	/26 oder 255.255.255.192 (letztes Byte: 11000000)
Broadcast-Adresse	192.168.1.63
Anzahl adressierbarer Hosts	62 (64 – 2)

Subnetz 2	
Netzadresse	192.168.1.64
Netzmaske	/26 oder 255.255.255.192 (letztes Byte: 11000000)
Broadcast-Adresse	192.168.1.127
Anzahl adressierbarer Hosts	62 (64 – 2)

Subnetz 3	
Netzadresse	192.169.1.128
Netzmaske	/26 oder 255.255.255.192 (letztes Byte: 11000000)
Broadcast-Adresse	192.168.1.191
Anzahl adressierbarer Hosts	62 (64 – 2)

Subnetz 4	
Netzadresse	192.168.1.192
Netzmaske	/26 oder 255.255.255.192 (letztes Byte: 11000000)
Broadcast-Adresse	192.168.1.255
Anzahl adressierbarer Hosts	62 (64 – 2)

Leitungscode

Welche Eigenschaft muss ein Leitungscode aufweisen, dass der Empfänger den Takt aus dem Datenstrom extrahieren kann?

Der Bitstrom muss so codiert werden, dass er - unabhängig von den übertragenen Daten - genügend häufige Pegeländerungen (Signalfanken) aufweist.

Nennen Sie zwei Codes, welche die Bedingung unter a) erfüllen.

Manchester (10Base-2, 10BASE-T), dreiwertiger NRZI (100Base-TX), 4B3T (10BASE-T1L)

Aus welchen Gründen kann es notwendig sein, dass ein Leitungscode gleichstromfrei ist?

Wird das Signal galvanisch getrennt über einen Transformator geführt wird, dann geht der Gleichstromanteil verloren.

Nennen Sie zwei Codes, welche gleichstromfrei sind.

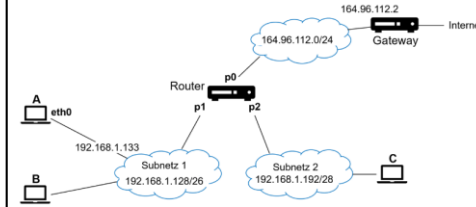
AMI, 4B3T (10BASE-T1L), dreiwertiger NRZI (100Base-T)

Welche Aufgaben hat der Data Link Layer generell? Nennen Sie 4 Funktionen und zu jeder ein treffendes Beispiel, wie die Aufgabe bei Ethernet gelöst wird (Stichwort genügt).

- Frame Delineation → Präambel und SFD
- Fehlererkennung → CRC
- Fehlerkorrektur → bei Ethernet keine auf dem MAC Layer
- Adressierung → global gültige MAC-Adressen
- Media Access Control → CSMA/CD

Routing

Drei Subnetze sind wie in der Figur dargestellt über einen Router verbunden und über die Default Gateway-Adresse 164.96.112.2 ans Internet angeschlossen. Die Router-Ports p0, p1, p2 belegen die tiefste Adresse im jeweiligen Subnetz.



- Wie sieht die Routing-Tabelle für den Router aus? Geben Sie die Einträge in der Reihenfolge an, wie diese beim Forwarding berücksichtigt werden. Die Routing-Tabelle soll möglichst wenig Einträge beinhalten. Geben Sie die Netzmaske in der Kurznotation /nn an.
Anmerkung: Es werden evtl. nicht alle Zeilen der Tabelle benötigt

Netzadresse	Netzmaske	Port	Gateway
192.168.1.192	/28	p2	direkt
192.168.1.128	/26	p1	direkt
164.96.112.0	/24	p0	direkt
default	/	p0	164.96.112.2

- Wie sieht die Routing-Tabelle für den Linux-Host A aus, wenn er Ziele in allen diesen Subnetzen und auch im Internet erreichen können muss? Die Routing-Tabelle soll möglichst wenig Einträge beinhalten.
Hinweis: Es werden evtl. nicht alle Zeilen der Tabelle benötigt

Netzadresse	Netzmaske	Port	Gateway
192.168.1.128	/26	eth0	direkt
default	/	eth0	192.168.1.129

Übertragung

Wir betrachten eine asynchrone Schnittstelle, welche mit folgenden Parametern betrieben wird
Bitdauer T ist 1 ms, 8 Bit/Zeichen, 1 Stopp-Bit.

a) Welche maximale Zeichenrate lässt die Schnittstelle zu?

1000 Bits / 10 Bit/Zeichen = 100 Zeichen/s

- b) Um wieviel darf die Frequenz des Empfängertaktgebers von dem des Senders maximal abweichen, ohne dass das einen Übertragungsfehler bewirkt? Relative Angabe in Prozent.
Zeitmessung startet mit der fallenden Flanke des Start-Bits nach 9.5 * T ist man im Idealfall in der Mitte des letzten Datenbits

Fehlablesung entsteht dann, wenn man um 0.5 * T daneben liegt
→ 0.5 * T / 9.5 * T = 1/19 = 5.26%

- c) Wir betrachten den Fall, bei dem die Frequenz des Empfängertaktgebers geringfügig höher ist, als der unter b) errechnete Wert. Es wird das Zeichen 10101010 gesendet. Welches Zeichen detektiert der Empfänger?

Das zuletzt übertragene Bit wird nicht abgetastet, dafür das vorhergehende zweimal. Weil das letzte Bit das MSB ist, wird das Zeichen 00101010 empfangen.

Bit stuffing

der synchronen Datenübertragung werde das Flag 01111110 und Bit-Stuffing (B) wendet.

Wozu verwendet man hier Bit-Stuffing?

Start-/Ende-Flags dürfen nicht in den eigentlichen Daten vorkommen, da dies vom Empfänger als Flag detektiert würde

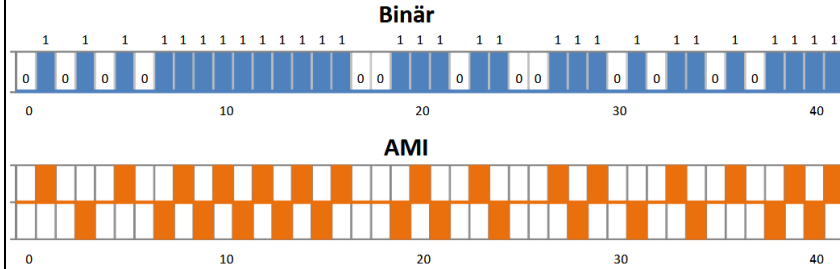
Wie sieht der folgende gesendete Bitstrom auf der Leitung aus?

1010111110100111111111110000001010111101111101

Sender	Empfänger	Daten	Sequenznummer	Acknowledgenummer
A	B	0	1000	30000
B	A	1000	30000	1000
B	A	1000	31000	1000
A	B	500	1000	32000
B	A	1000	32000	1500
A	B	0	1500	33000

Leitungscode

Beispiel: 3-wertiger AMI-Code (Alternate Mark Inversion)



Sehen Sie Nachteile dieses Leitungscode?

- Auf der Übertragungsstrecke drei Zustände benötigt → rein binäre Medien genügen nicht

Eignet sich dieser Code gut für die Taktrückgewinnung im Empfänger?

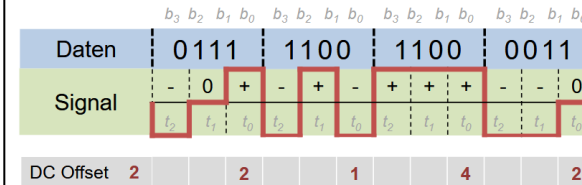
- Bei einer längeren Folge von "0" in den Daten ist keine Taktrückgewinnung mehr möglich

Anwendung: 10 Mbit/s Ethernet über Single Pair bis 1.2km (10BASE-T1L)

4B3T-Codierung: 4 Bit $2^4 = 16$ Symbole ($b_3b_2b_1b_0$) → 3 ternäre Symbole $3^3 = 27$ Symbole ($t_2t_1t_0$)

- Der kumulierte DC Offset (1 .. 4) wird bei der Codierung berücksichtigt und so Gleichspannungsfreiheit erreicht

- Beispiel: 1100_{binär} wird auf "- + -" oder "+ + +" abgebildet



		MMS 43 coding table ^[1]			
		Accumulated DC offset			
Hex	Binary	1	2	3	4
0	0000	+0 + (+2)		0-0 (-1)	
1	0001		0 - + (+0)		
2	0010		+ - 0 (+0)		
3	0011		0 0 + (+1)		- - 0 (-2)
4	0100		- + 0 (+0)		
5	0101	0 + + (+2)		- 0 0 (-1)	
6	0110	- + + (+1)		- - + (-1)	
7	0111		- 0 + (+0)		
8	1000		+ 0 0 (+1)		0 - - (-2)
9	1001		+ + + (+1)		- - - (-3)
A	1010	+ + - (+1)		+ - - (-1)	
B	1011		+ 0 - (+0)		
C	1100	+ + + (+3)		- - - (-1)	
D	1101		0 0 + (+1)		- 0 - (-2)
E	1110		0 + - (+0)		
F	1111	+ + 0 (+2)		0 0 - (-1)	

MLT-3 (Multi-Level Transmission, 3-Pegelsystem) – kompakt

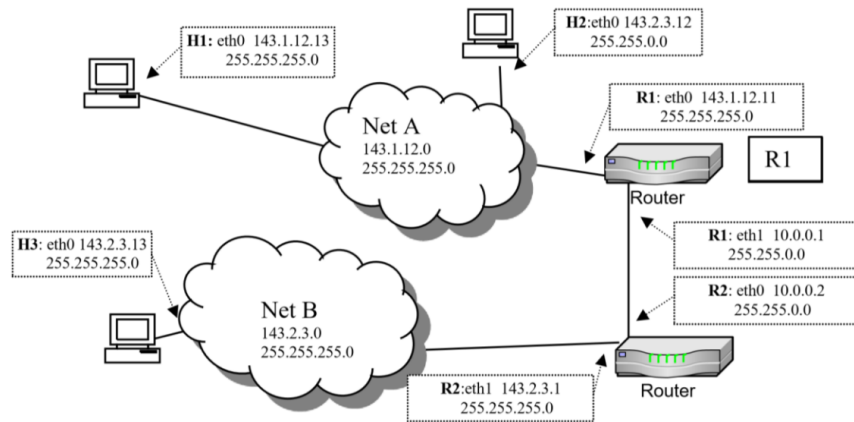
- Pegel: +V, 0 und -V
- Regel:
 - Bei Bit=0 → kein Pegelwechsel (bleibt auf dem bisherigen Pegel)
 - Bei Bit=1 → nächster Pegel im Zyklus +V → 0 → -V → +V ...
- Vorteile:
 - Halbierte höchste Frequenz gegenüber binärem NRZ → geringere Bandbreite
 - DC-frei durch symmetrische Pegelverteilung
 - Reduzierte elektromagnetische Emissionen
- Anwendung: 100 Mbit/s Ethernet über Kupfer (100Base-TX)

So liefert MLT-3 eine einfache, effiziente Multi-Level-Kodierung, die bei 125 MBaud nur eine Grundfrequenz von ca. 31,25 MHz benötigt.

PAM (Pulse Amplitude Modulation) – Kurz erklärt

- Prinzip
Bei PAM wird jedes Symbols durch eine von M möglichen Amplitudenstufen repräsentiert. Man unterscheidet:
 $M = \{2, 5, 16, \dots\} \Rightarrow \log_2(M)$ Bit pro Symbol
– Beispiel: PAM-5 hat 5 Stufen und trägt $\log_2(5) \approx 2,32$ Bit pro Symbol.
– In der Praxis kodiert man bei nicht-poten M ganze Bitgruppen (z. B. 3 Bit a 8 Stufen, 4 Bit a 16 Stufen).
- Ablauf
 1. **Bit-Gruppierung:** Rohdaten werden in Blöcke zu $\log_2(M)$ Bit aufgeteilt (oder in nächsthöheres Integer umgerundet).
 2. **Zuordnung:** Jedes Bit-Kombination wird einer Amplitudenstufe zugewiesen.
 3. **Signalformung:** Die gewählte Amplitude wird je Symbolzeit auf der Übertragungsleiter gegeben.
 4. **Empfang:** Pegel wird abgetastet und in das zugehörige Bitmuster rückgewandelt.

Routing Tabelle



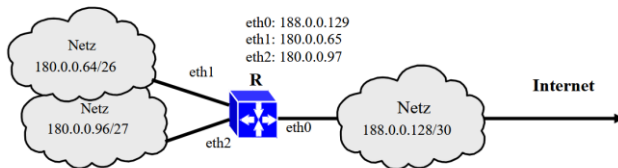
Routing-Tabelle von Host H1:

Netzadresse	Netzmaske	Interface	Gateway
143.1.12.0	255.255.255.0	eth0	(direkt)
default		eth0	143.1.12.11

Routing-Tabelle von Router R1:

Netzadresse	Netzmaske	Interface	Gateway
143.1.12.0	255.255.255.0	eth0	(direkt)
10.0.0.0	255.255.0.0	eth1	(direkt)
143.2.3.0	255.255.255.0	eth1	10.0.0.2

Der Router R verbindet die 3 abgebildeten Subnetze. Alle Stationen sollen über den Internetanschluss mit dem Rest der Welt kommunizieren können.



Mit welchen Einträgen muss der Router konfiguriert sein?
Wählen Sie für den Anschluss „Internet“ eine bei dieser Konfiguration mögliche IP-Adresse.

Netzadresse	Maske	Port	Gateway
188.0.0.128	255.255.255.252	eth0	(direkt)
180.0.0.96	255.255.255.224	eth2	(direkt)
180.0.0.64	255.255.255.192	eth1	(direkt)
default		eth0	188.0.0.130

Es kommt nur 188.0.0.130 für Internet in Frage, da .129 für eth1 und .131 für Broadcast verwendet wird.

Bit stuffing

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	1	0	1	0	1	0	1									1	1	1	1	1	1	1	1	1	1	1	1	1	1	
0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1							0	0	0	1	0	0	0	0
0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	1														
1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	1	0	0	0	0	1	0
1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	1	1	0	1	0	0	1	1	1	1	1	1	0

Hinweis: Für jedes Feld gilt: Das LSB steht rechts.

a) Was ist in diesem IP-Header alles falsch? (leere Felder nicht beachten!)

IP-Version muss 4 statt 5 sein!

TL+FO*8>64k → ungültiges IP-Paket Buffer overflow

b) Welches Protokoll wird mit diesem IP-Paket transportiert?

1 = ICMP

c) Wie heisst die IP-Adresse des Senders?

130.15.129.5

d) Wie heisst die IP-Zieladresse?

160.85.116.252

e) Sind bei diesem IP-Header Optionen vorhanden? Begründung verlangt!

Nein, IHL=5 = Minimum

f) Über wie viele Router wird dieses Paket im Maximum noch geleitet?

Über 6 bis zum 7-ten

TCP Schiebefensterprotokoll

Zwei Hosts sind mit einem Duplex-Übertragungskanal von 1 GBit/s verbunden. Welche Übertragungsrate kann man mit einer TCP-Verbindung maximal erreichen, falls die Window Size auf 64 kByte begrenzt ist und die Round Trip Time 2 ms beträgt.

Der Overhead der Protokoll-Header kann bei dieser Betrachtung vernachlässigt werden. Unter welchen Bedingungen wird diese maximale Rate auch erreicht?

Übertragungsrate = 64 kByte alle 2 ms = 64 kByte * 8 Bit/Byte / 2 ms = 256 Mbit/s Damit ist der Kanal nur zu ca. ¼ der Zeit genutzt.

