OSI

#	OSI Layers	Devices	Implementation
7	Application		DNS
6	Presentation	Browser	HTTP, SMTP
5	Session		
4	Transport	Firewall, NAT	TCP, UDP
3	Network	Router	IP, ICMP
2	Data Link	Bridge, Switch	Ethernet, ARP
1	Physical	Hub,Repeater,Connector	100BASE-TX
0	Media	Kabel, Glasfaser	CAT7

- Zuverlässig = Quittung, Sequenznummer, Fehler wiederholen
- Zwischen Schichten: Dienst, Interface
- SAP = Dienst zur höchsten Schicht
- Innerhalb: Protokoll
- 1-4 = Transport
- 5-7 = Anwendung
- 1-2 = Network Access

Media

- Ausbreitungsgeschwindigkeit $c_{\text{Material}} = \frac{c_0}{\text{Brechungsindex}} \sim 200'000'000 \frac{m}{s}$
- Dämpfung $A = 10 \cdot \log\left(\frac{P_1}{P_2}\right) = 20 \cdot \log\left(\frac{U_1}{U_2}\right) \text{dB}$
- SNR = Signal-Noise Ratio = $10 \cdot \log\left(\frac{P_{\text{Signal}}}{P_{\text{Störung}}}\right) \text{dB}$

Kabel

- Koaxialkabel
  - Gut für hochfrequente Signale
  - Unempfindlich gegenüber elektromagnetischen Störungen
  - Mechanisch heikel im Umgang
- Paarsymmetrische Kabel (Twisted Pair)
  - Häufg benutzt
  - Gut für breitbandige Datenübertragung
  - Störungen kapazitiv oder induktive Störung, Crosstalk
  - Anfällig auf Störungen = Unshielded Twisted Pair, UTP
  - Weniger Störung = Shielded Twisted Pair, STP
- Twinaxial-Kabel
  - 2 Koxialkabel in einem
  - Bessere Schirmung
  - Einsatz bei hohen Datenraten
- Glasfaserkabel
  - Hohe Bandbreite -grosse Datenraten
  - Geringe Dämpfung -grosse Übertragungsstrecken
  - Resistent gegen elektromagnetische Einflüsse

Twisted Pair	xx = Gesamtschirmung	y = Adapterpaarschirmung
xx/yTP	U = ungeschirmt F = Folienschirm S = Geflechtschirm SF = Beides	U = ungeschirmt F = Folienschirm S = Geflechtschirm

Kategorien

- Cat 1-4: Billigkabel für analoge Sprachübertragung

- Cat 5: Frequenzen bis 100 MHz; z.B. für 100 Mb/s oder 1 Gb/s Ethernet bis 100 m
- Cat 6: 250 MHz, 1 Gb/s Ethernet und 10 Gb/s Ethernet (bis 55 m)
- Cat 7: 600 MHz, z.B. für 10 Gb/s Ethernet (bis 100 m)

Aufhebung von Störungen

- Zusäztliches Komplementäres Signal minimiert Störungen. Der Empfänger subtrahiert die beiden Signale.
- Elektrisch leitender Schirm leitet kapazitive Störung ab (Der Schirm muss gut geerdet sein)
- Verdrillte Aderpaare hebt induktive Störungen auf

Glasfaser

- Multimode: dicker Kern, billig -Signalverschmierung und Moden-Dispersion
- Gradientenfasern: weniger Moden-Dispersion
- Singlemode: dünn, teuer, keine Moden-Dispersion, weit unn viel

Totalreflexion

Eine Welle im Material A ändert beim Übergang in ein weniger Dichtes Material B den Winkel. Die Totalreflexion tritt ein wennn der Austrittswinkel β 90°. 90° wäre genau entlang der Grenze der Materialien. Der Winkel kann folgendermassen berechnet werden: $\beta = \sin^{-1}\left(\sin(\alpha)\frac{n_A}{n_B}\right)$

Physical Layer

Abtasten

Gegeben: 12000 bit und 100ppm Differenz = 0.0001 Fehler pro TBit

Abweichung = 12000 * 0.0001 = 1.2 TBit > 12000

Gleichspannungsfreiheit

→ AMI jedes 2. + zu - oder PAM3 4 Bits auf 3 Ternäre Symbole (-,0,+)

Berechnungen

Gegeben: N Symbole, 1 Symbol dauert t Zeit, Bandbreite B

- Baudrate $f_s = \frac{1}{t}$
- Bitrate $R = \ln_2 \frac{N}{t}$
- Bits/Symbol = $\ln_2(N)$
- Maximale Baudrate $f_s = 2 \cdot \mathrm{B}$
- Maximale Bitrate(bps) $R = 2B \cdot ld(M)$
- $M = 1 + \frac{A}{\Delta V}$ = Unterscheidbare Signalzustände pro Symbole = Anzahl Stufen
- Kapazität(bps) $C_s = B \cdot ld\left(1 + \frac{S}{N}\right)$
- $\frac{S}{N}$ = Signal to Noise Ratio
- $M = \sqrt{1 + \frac{S}{N}}$

Serielle Asynchrone Übertragung

Gesamtzeit = (1.5 + n + (1) + 1) T

9.5 T müssen im Zeitfenster sein

1. Abtasten von Startbit "0" + 1.5T
2. n = 8 Datenbits lesen je + 1T (verkehrt)
3. (Parity Bit)
4. Stoppbit = 1

Serielle synchrone Übertragung

Taktgeber oder in Leitung codiert

Data Link Layer

Framing

- Asynchrone Übertragung ⇒ Start Bit
- Synchrone Übertragung ⇒ Flag wenn keine Daten (01111110). Bitstopfen = nach jedem 5. Bit eine 0 einfügen.
- Kleinere Frames = tiefere Fehlerwahrscheinlichkeit BER.
- Grössere Frames = Grösserer Anteil an Nutzdaten insgesamt / Nettobitrate. Datenverlust bei einem Fehler ist grösser.

Fehlerberechnung

- BER: Anteil fehlerhafter Bits = p_e
- Erfolg 1 Bit = $(1 - p_e)$
- Erfolg Frame = $(1 - p_e)^N$
- FER: Anteil fehlerhafter Frames = $1 - (1 - p_e)^N$, Annäherung: $N \cdot p_e$ für $p_e << 1$
- RER: Anteil unentdeckter fehlerhafter Bits = $P_{\leqslant F,N} = \Sigma_{t=0}^{F} \binom{N}{t} \cdot \varepsilon^t \cdot (1 - \varepsilon)^{N-t}$
- Bitfehlerrate: Bitfehler pro Zeit

Fehlererkennung

- CRC. 32-Bit
- Hamming Codes
- Quer, Längs, Checksum Parity. Even Parity→insgesamt gerade

Type	Erkennbare Fehler
32-Bit CRC	226 Bit 6, 2974 5, 91607 4, 3
Längs-/Querparität	4
16-Bit Check-Summe	1 ? 2
Even/Odd Parity RS-232	2
Hamming Code	h-1

Zugriffsmechanismen auf das Medium

- Leader/Follower-Verfahren
- Token Verfahren (deterministisch, aufwändig)
- Zeitsteuerung
- Carrier Sense Multiple Access: Bus frei? Daten senden. Abbruch bei Collision Detection. Collision Resolution. Collision Avoidance = request? clear.
- WLAN: Hidden Node Problem→Collision Avoidance

Flow Control

- Start-Stop
- Stop & Wait = Warten auf Quittung

Ethernet

MAC-Adresse

- Erste 3 Bytes: Hersteller
- Andere 3: Laufnummer
- Letzte 2 Bits des ersten Byte: 0/1 für individual/group address und universally/locally administered address

Ethernet Packet(PHY) + Frame(MAC) = 8 + 18 + 46

- **Preamble (7 Bytes)**
- **SFD (1 Byte)**
- **Destination Address (6 Bytes)**
- **Source Address (6 Bytes)**
- **Length/Type (2 Bytes)** <= 1500: Länge ohne PAD. >= 1536: DATA Type = Protokoll der nächsten Schicht.
  - 0×0800 für IPv4
  - 0×0806 ARP
  - 0×0001 ICMPv4, 58 ICMPv6
  - 0×86DD IPv6
- **Daten (46 - 1500 Bytes)** Wenn <= 46 dann PAD
- **Frame Check Sequence (4 Bytes)** IEEE CRC-32 Algorithmus
- (Interframe Gap 12 Bytes)

Repeater, Hub(=Multiport)

- Verstärkt ankommende Signale auf einem Port und leitet sie "in bester Qualität" weiter
- Keine Fehlererkennung

Switch / Bridge

- Prüft zusätzlich die Checksum von Frames
- Merkt sich Sender in Filtering Database und schickt Pakete an diesen Sender zum richtigen Port
- Alte Einträge werden gelöscht, wenn kein Verkehr vom Absender mehr beobachtet wird (5-10min)
- Mehrere Ports → Bridge Matrix
- Übertragungszeit $\text{Latenz} = t_{\text{frame}} + \frac{\text{Distanz}}{200000\frac{\text{km}}{s}}$

Spanning Tree Algorithmus von Bridges

1. Initialisierung
   - Alle Ports für Nutzdaten blockiert
   - Annahme: "Ich bin Root"
   - Austausch BPDUs (Bridge Protocol Data Units) mit Nachbarn
   - Die tiefste Adresse wird Root
2. Aufbau des Spanning Tree
   - Aufdatieren der Info zu Root (kleinste ID) und Pfadkosten zu dieser
   - Austausch aufdatierter BPDUs bis Konvergenz
   - Die kürzesten Wege werden gewählt
   - Wenn es zwei Wege gibt, dann gewinnt der Weg, bei dem der nächste Knoten die tiefere Adresse hat.
3. Setzen der Port Roles
   - Freigeben für Nutzdaten von Root-Ports (diese führen zum Root) und Designated-Ports (diese führen vom Root weg)
   - Alle anderen Ports bleiben blockiert (Discarding)

BPDU

- Root-ID (aus lokaler Sicht): 8 Byte
- Root-Cost (aus lokaler Sicht): 2 Byte
- Bridge-ID ("Ich"): 8 Byte
- Port-ID (Sende-Port): 2 Byte

VLAN

- Der Tag wird vor dem Type/Length Feld eingefügt. Er besteht aus 2 Bytes 0×8100 = getagged und 2 Bytes VLAN-ID.
- Prio Wert befindet sich im VLAN-Tag am Anfang der VLAN-ID. Der Wert ist eine Zahl von 0-7, wobei 7 am wichtigsten ist.

LAN Monitoring

- Hub / Multiport Repeater, zu welchem alle Ports gehen
- Tap / Probe, der überall dazwischengehängt werden kann.
- Port-Mirroring leitet Daten zusätzlich auf einen anderen Port um

Kabel

- Bitrate(Mbit/s) + BASE oder BROAD + Codierung
- Codierungen Z.B:
  - T, TX, T1: Twisted Pair
  - SR, DR, LR: optisch
  - C: Twinax
  - K: Backplane
- Zwischen FLP: 10000 = Message Type Ethernet. Rest = Was kann die Station und was nicht
- Kompatibel durch:
  - Beibehaltung von Frame Format und Schnittstelle zwischen PHY und MAC
  - Autonegotiation mittels FLP bursts / NLP
- Vervielfachnugn der Datenrate heisst:
  1. Baudrate / Signalfrequenz
     - Höhere Datenrate bedeutet auch höhere Baudrate bzw. Bandbreite
     - Dämpfung nimmt mit steigender Signalfrequenz zu
     - Übersprechen (Crosstalk) nimmt mit steigender Frequenz zu
  2. Kompatibilität und Unterstützung von Systemen mit heterogenen Datenraten

- Möglichst keine Konfiguration
- Systemrelevante Parameter beibehalten

100BASE_TX

- 4 Bits werden zu 5 Bits Codiert
- Start-of-Stream Delimiter (J/K) ersetzt erstes Byte der Preamble
- End-of-Stream Delimiter (T/R) folgt nach dem Frame
- Idle (I) füllt die Leitung ununterbrochen zwischen Frames

1000BASE-T

- 4 statt 2 Aderpaare, diese werden alle gleichzeitig in beide Richtungen verwendet
- 5-wertiger Leitungscode
- "Next Page" Mechanismen bei FLPs
- Vollduplexbetrieb mittels Gabelschaltung

10GBASE-T

- 16-wertiger Leitungscode
- Forward Error Correction, Scrambling
- neue Kabelkategorien CAT 6 bis 8

Bezeichnung	Medium	Max.Länge	Topologie
10BASE5	50 Ohm Koax	500 m	Bus
10BASE2	50 Ohm Koax	185 m	Bus
10BROAD36	75 Ohm Koax	3600 m	Bus
10BASE-T	2 Paar UTP Cat. 3	100 m	Punkt-Punkt
10BASE-FL	2 MMF (62.5 um)	2000 m	Punkt-Punkt
10BASE-FP	2 MMF (62.5 um)	500 m	Punkt-Punkt
10BASE-FB	2 MMF (62.5 um)	2000 m	Stern
10BASE-T1L	Single TP	1589 m	Punkt-Punkt
10BASE-T1S	Single TP	25 / 40m	Punkt-Punkt / Multi-Drop
100BASE-TX	2 TP CAT4-5		
1000BASE-T	4 TP CAT5	100m	
10GBASE-T	4 TP	100m	

Network Layer

IPv4

Insgesamt 20 Bytes:

- **Version (4 Bits)**: 4
- **Internet Header Length (IHL) (4 Bits)**: Länge = Wert * 4
- **Differentiated Services (DS) (1 Byte)**: Erlaubt Priorisierung, Delay, Jitter von IP-Datenpaketen. Der Wert ist eine Qualitätsklasse.
- **Total Length (2 Bytes)** (MTU 46..1500 Bit wenn in Ethernet Frame)
- **Identification Number (2 Bytes)** Erlaubt Identifikation zusammengehöriger Fragmente
- **Flags (4 Bits)** `0 DF MF` Do Fragments, More Fragments
- **Fragment Offset (12 Bits)**
- **Time to Live (TTL) (1 Byte)**: Dekrementierender Hop-Counter
- **Protocol (1 Byte)**: ZB 1 ICMP, 6 TCP, 17 UDP
- **Header Checksum (2 Bytes)**: Schützt nur den IP-Header selbst, In jedem Router neu berechnet, wegen TTL etc. 16-Bit Prüfsumme
- **Source Address (4 Bytes)**
- **Destination Address (4 Bytes)**
- **Options / Padding (variabel)**: muss immer ein vielfaches von 4 sein
  - Identification Number (2 Bytes)
  - Flags (3 Bits): 1 = Do/Dont Fragment, 2 = Last/More Fragments
  - Fragment Offset (13 Bits): Gibt an, wo in einem fragmentierten IP-Paket ein Fragment hingehört

IPv6

In der Praxis: 001 + 45 Bits Global Routing Index + 16 Bits Subnet ID + 64 Bits Interface ID. Insgesamt 40 Bytes:

- Version: 0.5 Byte = 6
- Traffic Class: 1 Byte
- Flow Label: 2.5 Bytes
- Nutzdatenlänge: 2 Bytes
- Next Header: 1 Byte
- Hop Limit: 1 Byte
- Source Address: 16 Bytes (8 Doppel-Bytes, :: = Restliche, :1 = :0001)
- Destination Address: 16 Bytes
- Extension Headers: Hop by hop, Destination, Routing, Fragmentation, Authentication, Security, Destination, Payload (Upper Layer)

Prefix	Bereich	RFC	Zum Vergleich bei IPv4
0000::FFFF:0:0/96	IPv4-Mapped Addresses	[RFC 4291]	
0064:FF9B::/96	IPv4-Translatable Addresses	[RFC 6052]	
2000:: /3	Global Unicast	[RFC 4291]	
FC00:: /7	Unique Local Unicast	[RFC 4193]	
FE80:: /10	Link Local Unicast	[RFC 4291]	Autoconfigured 169.254.0.0/16
FF00:: /8	Multicast	[RFC 4291]	Multicast 224.0.0.0/4
:: 1	Loopback		Localhost 127.0.0.1

IP Adressen

- 4 Byte
- Netzadresse = Interface 0
- Broadcast Adresse = Alles 1
- Loopback-Adressen: Das Netz 127.0.0.0/8 wird and emuliertes Loopback-Gerät geschickt (braucht kein Netz)
- Private Adressbereiche: Werden nicht weitergeleitet: 10.0.0.0 /8, 172.16.0.0 – 172.31.0.0 /16, 192.168.0.0 – 192.168.255.0 /24
- Autoconfig-Adressen: 169.254.0.0 /16

Netzmaske	Alternative	Interfaces
255 (1111'1111)	/24	256 - 2
254 (1111'1110)	/23	512 - 2
252 (1111'1100)	/22	1'024 – 2
248 (1111'1000)	/21	2'048 - 2
240 (1111'0000)	/20	4'096 - 2
224 (1110'0000)	/19	8'192 - 2
192 (1100'0000)	/18	16'384 - 2
128 (1000'0000)	/17	32'768 – 2
0 (0000'0000)	/16	65'536 – 2

Klasse	Adressbereich	Anzahl Netze	Interfaces pro Netz	/?	Präfix
A	1.0.0.0 - 127.255.255.255	127	16'777'214	/8	0
B	128.0.0.0 - 191.255.255.255	16'384	65'534	/16	10
C	192.0.0.0 - 223.255.255.255	2'097'152	254	/24	110
D	224.0.0.0 - 239.255.255.555	Multicast Adressen			1110
E	240.0.0.0 - 255.255.255.255	Reserviert für zukünftige Nutzung			1111

Aufteilung von Netzen

???

Router

1. Netze verbinden, ZB LAN und Internet
2. Netze segmentieren um die Broadcast Domain zu limitieren oder
3. Netze mit einer Firewall voneinander schützen.

Routing

- = Aufbau und Update von Routingtabellen in den Knoten
- Tabelle: Netzadresse Netzmaske Port Gateway
- default 0.0.0.0 eth0 160.85.16.1
- Flach = Jeder kennt jeden
- Hierarchisch = Router kennt direkt angeschlossenen Netze seiner Interfaces und 1 anderen Router

Übertragung eines IP-Pakets

1. A fragt mit ARP Ip für nächsten Router B
2. Ethernet Paket von A zu B
3. B macht das ganze erneut
4. Im letzten Netz gibt ARP die tatsächliche IP des Ziels zurück

ARP (Ethernet Layer, In Ethernet Paket)

ARP-Tabelle speichert bekannte IPv4 MAC Kombination.

1. Broadcast "who has (IP)"
2. "(IP) is at (MAC)"

NDP

- Request ist Multicast
- Neighbor Cache speichert IPv6 MAC Kombination

ICMP (In IP Paket)

- 1 Byte Type
- 1 Byte Code
- 2 Bytes Checksum
- 2 Bytes Identifier
- 2 Bytes Sequence Number
- Weitere Bytes abhängig vom Code

Type	Code	Usage
0 Echo		ping
3 Destination Unreachable	4 fragmentation needed and DF set	Path MTU discovery
8 Echo reply		ping
11 Time Exceeded		traceroute antwort (TTL war 0)

Transport Layer

TCP Header

Verbindungsorientiert, Insgesamt 20 Bytes ohne Optionen/Padding:

- **TCP Source Port (2 Bytes)**
- **TCP Destination Port (2 Bytes)**
- **Sequence number (4 Bytes)**
- **Acknowledgement Number (4 Bytes)**
- **Header Length (4 Bits)** (Faktor 4 Bytes)
- **Unused (4 Bits)**
- **ECN Flags (2 Bits)** 8 = Congestion Window Reduced, 9 = ECN-Echo
- **Control Bits (6 Bits)** URG,ACK,PSH,RST,SYN,FIN. PSH=OhnePuffer
- **Window (2 Bytes)** Verfügbarer Puffer
- **Checksum (2 Bytes)** Über TCP-Header und Daten
- **Urgent Pointer (2 Bytes)** Falls URG, gibt Position von Urgent Data an
- Options/Padding (4 * n Bytes) ZB MSS (Maximum Segment Size)

TCP Eigenschaften

- **Verbindungsorientierte Übertragung**: Zuerst wird eine Verbindung zwischen Client- und Serveranwendung aufgebaut

- **Zuverlässiger Verbindungsaufbau**: Bevor eine TCP-Verbindung steht, muss dies von beiden Endpunkten aktiv bestätigt werden
- **Hohe Zuverlässigkeit**: Die Daten kommen ohne Datenverlust und in der richtigen Reihenfolge auf der anderen Seite an
- **Vollduplexübertragung**: Gleichzeitige, voneinander unabhängige, Übertragung in beiden Richtungen möglich
- **Stream-Schnittstelle**: Die Anwendung sendet/empfängt eine unstrukturierte Byte-Folge
- **Graceful Termination** (Verbindungsabbau): TCP gewährt die Zustellung aller Daten auch beim Verbindungsabbau
- **Punkt-zu-Punkt Kommunikation**: Zwei Applikationen tauschen Daten aus. Konzepte wie Multicast oder Broadcast existieren nicht.

TCP Verbindung

Aufbau

1. Der Server "horcht" (LISTEN) auf einer bestimmten Port Nummer
2. Der Client sendet **SYN=1, ACK=0** und zufälliger initialer Sequenznummer **SEQ=a** (Bsp. 15'000)
3. Server bestätigt Sequenznummer mit **ACK=a+1 (15'001), SYN=1** und wählt zufällige initiale Sequenznummer **SEQ=b** (Bsp. 42'300)
4. Client bestätigt b mit **ACK=b+1** (42'301) und **SEQ=a+1**
5. Wenn nun vom Client bei SEQ=15001 1000 Bytes Daten gesendet werden, sendet der Server ACK=16001

Abbau

1. A sendet FIN
2. B sendet ACK=ack+1 um FIN zu bestätigen
3. Der Verbindungszustand wird als Half-Closed bezeichnet, B könnte also immer noch Daten schicken.
4. B sendet auch FIN
5. A sendet ACK=ack+1 um FIN zu bestätigen

RTT

- BPD = RTT (s) * Bandbreite (bps)
- minimal benötigte TCP Fenster = BPD / 8
- ???

Sliding Window

Daten senden um Window zu füllen. Dann auf Quittung warten.

Congestion Control

- **Slow Start**: Senderateexponentiell erhöhen Schwelle. Dann linear. Problem = tiefere Schwelle und Neustart.
- **Congestion Window**: Ein Überlastfenster limitiert zusätzlich die Grösse des Sendefensters. Dies ist eine lokale Variable.

UDP Header

Verbindungslos, Insgesamt 8 Bytes:

- UDP Source Port (2 Bytes)
- UDP Destination Port (2 Bytes)
- UDP Message Length (2 Bytes)
- Checksum (2 Bytes)

Ports

- Standardisierte System Ports (Bereich 1 - 1'023)
- HTTP 80(TCP), DNS 53, SSH 22(TCP), HTTPS 443
- User Ports (Bereich 1'024 - 49'151) (Reserviert für Applikationen)
- Dynamic / Private Ports (Bereich 49'152 - 65'536)

NAT (Network greift auf Transport zu)

Alle Hosts im privaten Netz 192.168.0.0/8 verwenden 192.168.0.1 als Default-Gateway.

NAPT-Gateway-Funktion:

- Er ersetzt im IP-Header der ausgehenden Pakete die lokale Source-Adresse 192.168.0.10 durch die globale Gateway- Adresse 160.85.17.11
- Er ersetzt im Transport-Layer-Header der ausgehenden Pakete das Source-Port 56777 durch eine eindeutige / freie Port- Nummer.
- Er legt die Verbindungsinformation dynamisch in einer Verbindungstabelle ab.
- Er sucht bei eingehenden Paketen die Verbindung in der Tabelle und setzt die ursprüngliche IP-Adresse/Port wieder ein
- Portnummern und IP-Adressen werden verändert → Prüfsummen müssen angepasst werden.