

# Kommunikationstechnik Zusammenfassung Hofer

## 1 - OSI-Modell

*Reihenfolge der Daten bleibt erhalten*

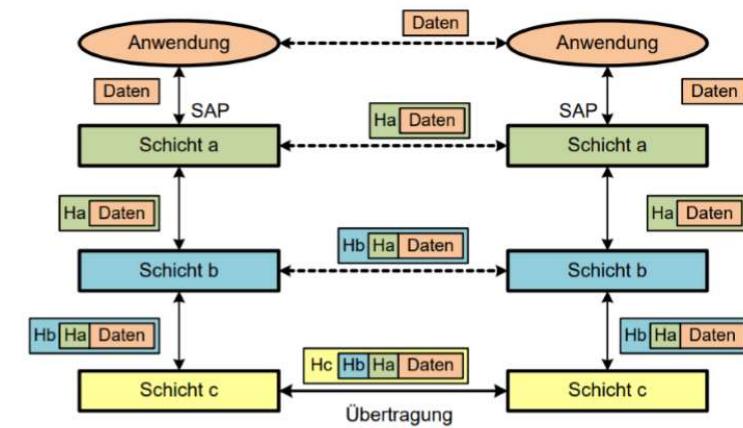
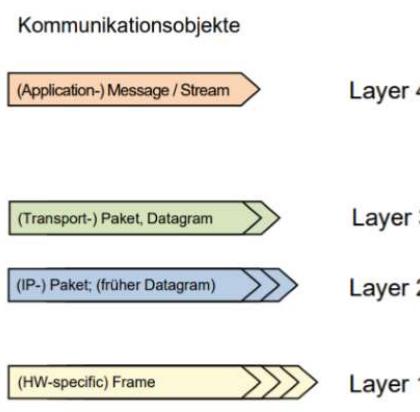
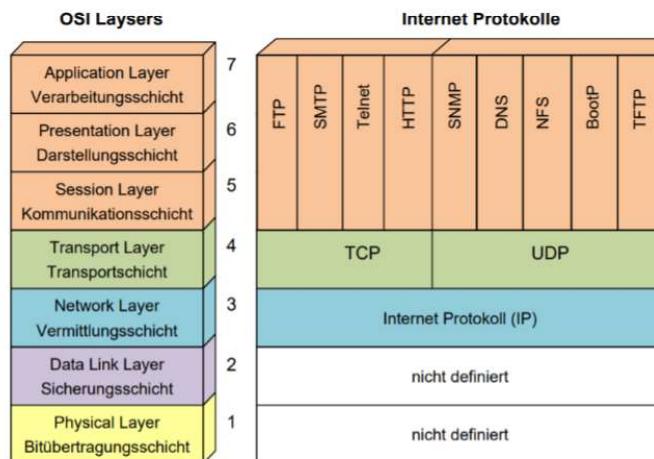
*Send and Forget*

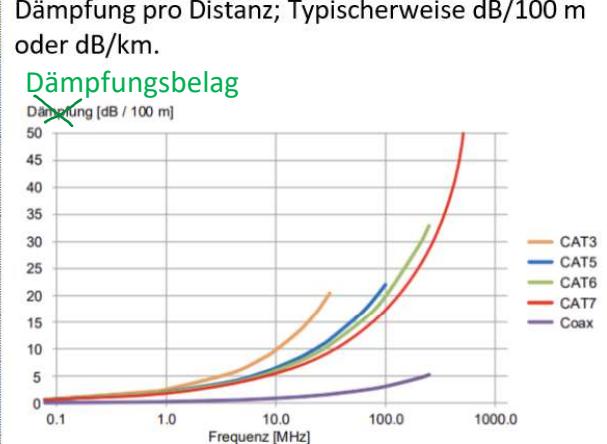
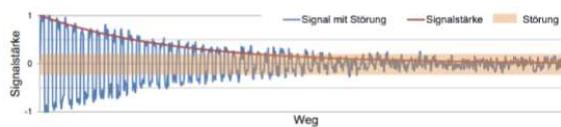
Ein Dienst sendet und empfängt bestätigte und unbestätigte Daten.  Klassifizierung von Diensten <ul style="list-style-type: none"><li>• Verbindungsorientiert oder verbindungslos</li><li>• Zuverlässig oder unzuverlässig</li></ul>	<b>Verbindungsorientiert</b> Verbindungs-Aufbau nötig Ziel muss bereit sein	<b>Verbindungslos</b> Jederzeit Nachrichten schicken Ziel muss nicht «bereit» sein
	<b>Zuverlässig</b> Kein Datenverlust Sicherung durch Fehler-Erkennung -/ Korrektur Text-Nachrichten	<b>Unzuverlässig</b> Möglicher Datenverlust Keine Sicherung Streaming

Eine Schicht hat die Aufgabe der darüberliegenden Schicht bestimmte Dienste zur Verfügung zu stellen. Die Schichten benötigen kein Wissen über die Realisierung der darunterliegenden Schicht.

Ein Protokoll ist eine Sammlung von Nachrichten, Nachrichtenformaten und Regeln zu deren Austausch. Im zwischenmenschlichen Bereich könnte man die Knigge als Protokoll bezeichnen. Sie legt einen gewissen «Verhaltens-Standard» nach welchem wir uns richten.

In der Technik ist ein Kommunikationsprotokoll eine Vereinbarung, die festlegt wie eine Datenübertragung zwischen Kommunikationspartnern abläuft.

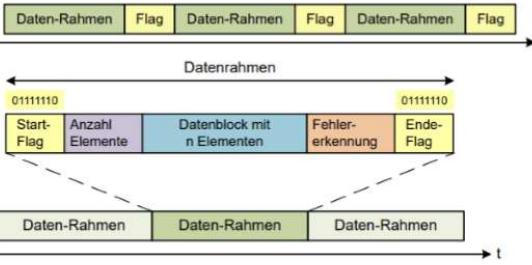
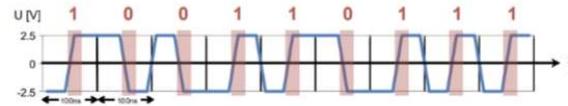
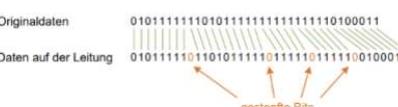


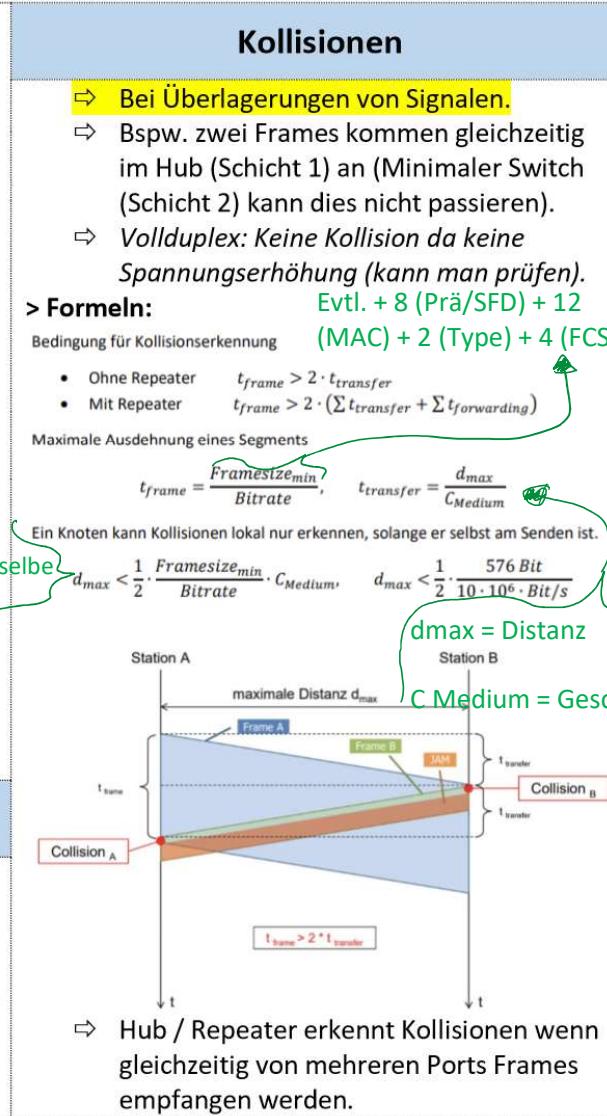
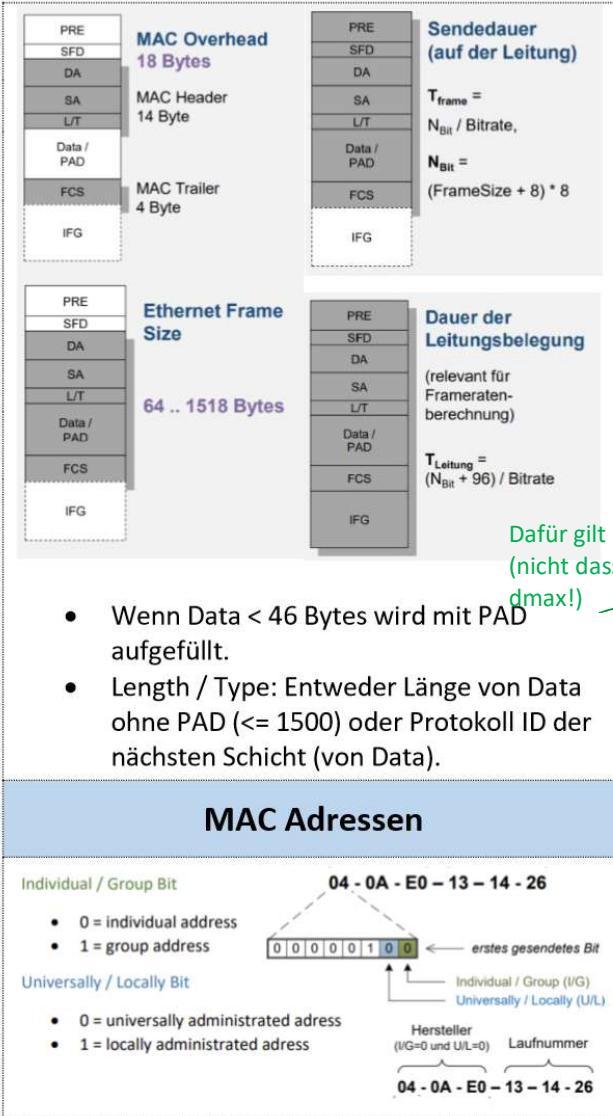
Übertragungsmedien	Dämpfungsbelag	Wegen Totalreflexion. Nehmen wenn zu grosses Rauschen
<b>Ausbreitungsgeschwindigkeit</b>	Dämpfung pro Distanz; Typischerweise dB/100 m oder dB/km. <b>Dämpfungsbelag</b> 	<ul style="list-style-type: none"> <li>• <b>Twisted Pair (TP):</b> Häufig im Einsatz.</li> <li>• <b>Glasfaser:</b> Hohe Bandbreite, Geringe Dämpfung, zusätzlich: Dispersion (schlecht)</li> </ul>
Lichtgeschwindigkeit im Vakuum: $c_0 = 299'792'458 \frac{m}{s}$		Arten (aufsteigend nach Kosten): Multi Mode (MM) Stufenfasern, MM Gradientenfasern, Single Mode Fasern.
Daraus folgt die Ausbreitungsgeschwindigkeit im Medium: $\approx \frac{2}{3} c_0 \approx 200'000 \frac{km}{s}$		
<b>Signaldämpfung</b>	<ul style="list-style-type: none"> <li>⇒ Je kleiner die Dämpfung, desto grössere Distanzen kann das Signal «leben».</li> <li>⇒ Senkt man Bitrate (Bit/s), können grössere Distanzen erreicht werden.</li> <li>⇒ Die Bandbreite (Frequenz) ist in der Grafik abhängig zum Dämpfungsbelag.</li> <li>⇒ Die höheren Kabelkategorien brauchen, um höhere Dämpfung zu tolerieren, bessere Schirmungen, um das Übersprechen zu minimieren.</li> </ul>	<b>Störungen</b> <ul style="list-style-type: none"> <li>⇒ Eine Verstärkung der Signale beim Empfänger möglich wenn Signal von der Störung (siehe Diagramm Signaldämpfung) abhebt.</li> <li>⇒ Mögliche Störungen: <ul style="list-style-type: none"> <li>- Übersprechen zwischen Leitungen.</li> <li>- Rauschen des Empfängers.</li> <li>- Einstreuungen durch andere Geräte.</li> </ul> </li> </ul> <p>&gt; <b>Übersprechen / Nebensprechen (crosstalk):</b> Störungen von benachbarten Leitungen (kapazitiv oder induktiv).</p> <ul style="list-style-type: none"> <li>⇒ Komplementäre Signale (Empfänger subtrahiert die Signale -&gt; Störungen werden aufgehoben) und Schirmung gegen kapazitive Störungen.</li> <li>⇒ Verdrillung gegen induktive Störungen.</li> </ul>
Leistungsabnahme eines Signals auf einer Übertragungsstrecke. 		
<b>Signaldämpfung (SNR) [dB] = <math>10 * \log \left( \frac{P_1}{P_2} \right)</math></b> P1: Eingangsleistung P2: Ausgangsleistung <b>3dB ≈ Faktor 1/2</b>		
$= 10 * \log \left( \left( \frac{U_1}{U_2} \right)^2 \right) = 20 * \log \left( \frac{U_1}{U_2} \right)$		
<ul style="list-style-type: none"> <li>• Eine Dämpfung von <b>6 dB</b> bedeutet eine <b>Leistungsabnahme um den Faktor 4</b> und <b>Spannungsabnahme um den Faktor 2</b>.</li> </ul>		
	<ul style="list-style-type: none"> <li>• <b>Koaxialkabel:</b> Geeignet für hochfrequente Signale. Besser als TP.</li> <li>• <b>Twinaxial-Kabel:</b> Hoher Schutz. Geschirmt oder ungeschirmt. Allfälliger auf Störung.</li> </ul>	<b>Kabeltypen</b>
		<b>Kabelschirmung Bezeichnung</b>
		<p>xx steht für die Gesamtschirmung: U = ungeschirmt F = Folienschirm S = Geflechtschirm SF = Schirm aus Geflecht und Folie</p> <p>y steht für die Aderpaarschirmung: U = ungeschirmt F = Folienschirm S = Geflechtschirm</p>

▪ Das Signal-Rausch-Verhältnis (engl. Signal-to-Noise-Ratio) **SNR** ist definiert durch:

$$\text{SNR} = 10 * \log \left( \frac{P_{\text{Signal}}}{P_{\text{Störung}}} \right) \text{ dB}$$

<b>Physical Layer (Schicht 1)</b>		<b>Serielle Synchrone Übertragung</b>	<b>Data Link Layer (Schicht 2)</b>
<b>Verkehrsbeziehung und Kopplung</b>		<p>Empfänger arbeitet mit Takt von Sender.</p> <ul style="list-style-type: none"> <li>Keine Start- und Stoppbits notwendig.</li> <li>Neben Datensignal muss auch Takt übertragen werden.</li> </ul> <p>Aufgabe vom Data Link Layer Grenzen der einzelnen Bytes zu ermitteln (Preamble etc.).</p>	<p><math>M = 1 + \frac{A}{\Delta V}</math></p> <p>A: Max. Grösse des Signals V: Ungenauigkeit des Empfängers</p> <p>&gt; Gesetz von Shannon-Hartley:</p> $C = B * ld \left( 1 + \frac{S}{N} \right)$ <p>C: Kanalkapazität S: Signalleistung N: Rauschleistung</p>
<b>Serielle Asynchrone Übertragung</b>		<b>Leitungscodes und Taktrückgewinnung</b>	
<p>Kein Takt für Bitsynchronisation wird übertragen.</p> <ul style="list-style-type: none"> <li>Empfänger justiert seinen Übertragungsrahmen bei jedem übertragenen Zeichen von Neuem.</li> </ul> <p>&gt; Sender/Empfänger brauchen Abmachungen:</p> <ul style="list-style-type: none"> <li>- Bitrate</li> <li>- Anzahl Datenbits (norm. 1 Byte)</li> <li>- Anzahl Stoppbits (norm. 1 Bit)</li> </ul> <p>&gt; Taktrückgewinnung: Möglich <math>Ld() = \text{Informationsgehalt}</math></p>		<p>Mittels Leitungscode ist es dem Empfänger möglich den Takt heraus zu extrahieren (sonst bräuchte er eine 2te Leitung für den Takt).</p> <ul style="list-style-type: none"> <li>Siehe Manchester Code.</li> <li>Regelmässige Zustandsänderungen auf der Übertragungsstrecke.</li> </ul>	
<b>Formeln: Nutzung der Bandbreite</b>		<b>Datenraten – Framerate &amp; Nutzbitrate</b>	
<p>&gt; <b>Bitrate:</b> Bit/s</p> <p>&gt; <b>Baudrate:</b> Symbol/s (Signaländerung)</p> <p>&gt; <b>Symbolrate (Nyquist Rate):</b></p> $f_s \leq 2B$ <p><math>f_s</math>: Max. Symbolrate (Baud (Bd)) B: Nutzbare Bandbreite (Hz)</p> <p>&gt; <b>Max. erreichbare Bitrate (Hartley's Gesetz):</b></p> $R \leq 2B * ld(M)$ <p>R: Max. Bitrate (bit/s) M: Unterscheidbare Signalzustände</p>		<p><math>F_R = \frac{B}{B + (F_L + IFG)}</math>, <math>N = F_R \cdot P \cdot \theta</math></p> <p>Evtl. + 8 Bytes für Präambel und SFD</p> <p><b>Framing (Asynchron)</b></p>	

<ul style="list-style-type: none"> <li>Keine Daten: Nichts wird gesendet: Ruhe.</li> <li>Zu Beginn eines Frames wird ein Start Bit gesendet (ändern des Ruhezustands).</li> <li>Prüfbits am Ende eines Frames!</li> <li>Bspw. IP Pakete für unterschiedliche Routen.</li> </ul> 	<h3>Wahl der Frame-Länge</h3> <ul style="list-style-type: none"> <li>Je länger die Frames desto besser wird die Nettobitrate.</li> </ul> <p><b>Norm = 79%</b></p> $\text{Nettobitrate} = \text{Bruttobitrate} * \frac{\text{Nutzdaten}}{\text{Nutzdaten} + \text{Header}}$ 	<table border="1"> <thead> <tr> <th>Bild</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td></td> <td>&gt; Zentraler Verteiler. &gt; Wenig Störungsanfällig.</td> </tr> <tr> <td></td> <td>&gt; Weniger Last für die einzelnen Switches (Aufteilung).</td> </tr> </tbody> </table>	Bild	Beschreibung		> Zentraler Verteiler. > Wenig Störungsanfällig.		> Weniger Last für die einzelnen Switches (Aufteilung).		
Bild	Beschreibung									
	> Zentraler Verteiler. > Wenig Störungsanfällig.									
	> Weniger Last für die einzelnen Switches (Aufteilung).									
<h3>Framing (Synchron)</h3> <ul style="list-style-type: none"> <li>Frames werden dauernd gesendet (wenn kein Inhalt, dann leerer Frame).</li> <li>Start- und Stopflag.</li> </ul> 	<h3>Lokale Netzwerke (Ergänzung 1 Schicht 2)</h3> <h4>Topologien</h4> <table border="1"> <thead> <tr> <th>Bild</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td></td> <td>&gt; Passiv an Kabel. &gt; Empfänger sieht anhand Adresse ob Daten relevant.</td> </tr> <tr> <td></td> <td>&gt; Alle müssen Daten empfangen. &gt; Ausfall: Segmentierung des Lan in 2 Teilen.</td> </tr> <tr> <td></td> <td>&gt; Benötigt Verfahren für Verhinderung von «endlosem Zyklus». &gt; Ausfall: Jede kann immer noch erreicht werden.</td> </tr> </tbody> </table>	Bild	Beschreibung		> Passiv an Kabel. > Empfänger sieht anhand Adresse ob Daten relevant.		> Alle müssen Daten empfangen. > Ausfall: Segmentierung des Lan in 2 Teilen.		> Benötigt Verfahren für Verhinderung von «endlosem Zyklus». > Ausfall: Jede kann immer noch erreicht werden.	<h3>Manchester Leitungscode (10BASE-T)</h3> <ul style="list-style-type: none"> <li>1: Positive Flanke; 0: Negative Flanke</li> <li>Bei jedem Bit gibt es einen Signalwechsel</li> <li>Einfache Taktrückgewinnung</li> </ul> 
Bild	Beschreibung									
	> Passiv an Kabel. > Empfänger sieht anhand Adresse ob Daten relevant.									
	> Alle müssen Daten empfangen. > Ausfall: Segmentierung des Lan in 2 Teilen.									
	> Benötigt Verfahren für Verhinderung von «endlosem Zyklus». > Ausfall: Jede kann immer noch erreicht werden.									
<p><b>&gt; Bitstopfen:</b></p> <ul style="list-style-type: none"> <li>Sender fügt im Datenstrom nach 5 Einsen immer eine 0 ein.</li> <li>Empfänger wirft nach 5 Einsen immer 1 Bit weg.</li> <li>Somit gibt es nie (ausser bei Flags) die Bitfolge 01111110</li> </ul> 		<p><b>Ethernet Frame Format und Begriffe</b></p> <p>Anzahl fehlerhafte Bits im Verhältnis zu Gesamtzahl der Bits: • Alle Bits falsch: BER = 1 • Kein Bit falsch:</p>								
<p><b>Zugriffsmechanismen (MAC):</b></p> <ul style="list-style-type: none"> <li>- Master-Slave Verfahren</li> <li>- Token-Verfahren</li> <li>- Zeitsteuerung</li> <li>- Carrier Sense Multiple Access (bei Ethernet inkl. CD (Collision Detection))</li> </ul>	<p>Im LAN-Bereich gibt es drei Übertragungsarten</p> <ul style="list-style-type: none"> <li>• Unicast</li> <li>• Broadcast</li> <li>• Multicast</li> </ul>	<ul style="list-style-type: none"> <li>an einzelne Stationen</li> <li>an alle Stationen</li> <li>an eine Gruppe von Stationen</li> </ul>								



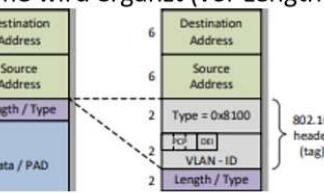
## Switched LAN und Ethernet (Ergänzung 2 Schicht 2)

### 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.

- ⇒ 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.

Store and Forward Switches senden empfangene Daten erst weiter wenn alle erhalten

- ⇒ Theoretisch Max.  $2^{12} - 2$  VLANS möglich.
- ⇒ VLAN mit ID 1: Default (für untagged Frames).

Seite 4 von 10

## Grundsätze des Internets

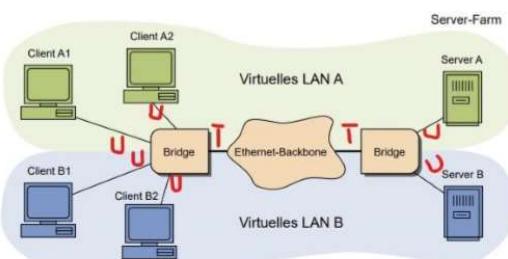
### KT Zusammenfassung

- 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

### Luca Marcea

#### > 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.

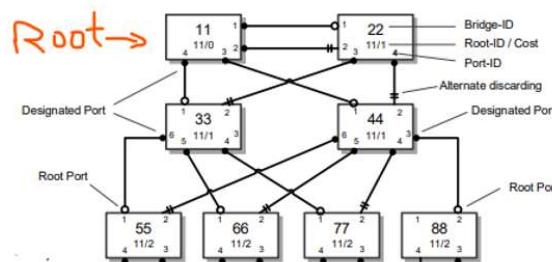
#### Spanning Tree (Redundanz Protokoll)

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



#### Leistungsmerkmale von Bridges

Anzahl Ports	Steckergroesse ist im Extremfall die Limitierung
Adressstabelle	Wie viele Stationen können im LAN existieren
Filtriere	Maximale Frames / s / Port (Empfangsrichtung)
Transferrate	Maximale Frames / s / Port (Sendedrichtung)
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 = Verbindungslos und unzuverlässig

#### Ethernet Systeme

- *Autonegotiation*: Ermittlung der besten Betriebsart durch Austausch der Leistungsmerkmale zweier Netzwerkkomponenten. → XBALE-T2
- *Link Pulses*: NLP = Link Presence Detection  
FLP = Autonegotiation, Autopolarity

	10BASE-T	100BASE-TX	1000BASE-T	10GBASE-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 Adernpaare simplex	MLT-3, 4B5B 2 Adernpaare simplex	PAM-5, 8B/10B 4 Adernpaare duplex	PAM-16, 64B/65B, FEC
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

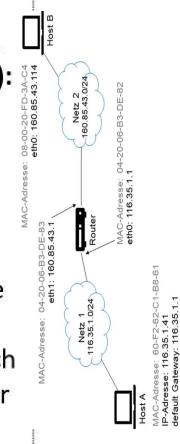
#### > Flaches Adressraum / Routing:

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

Netzwerk	MAC-source	MAC-destination	IP-source	IP-destination
Netz 1	BB-61	DE-82	116.35.1.41	160.85.43.114
Netz 2	DE-83	3A-C4	116.35.1.41	160.85.43.114

#### > Hierarchisches Adressraum / Routing (Default):

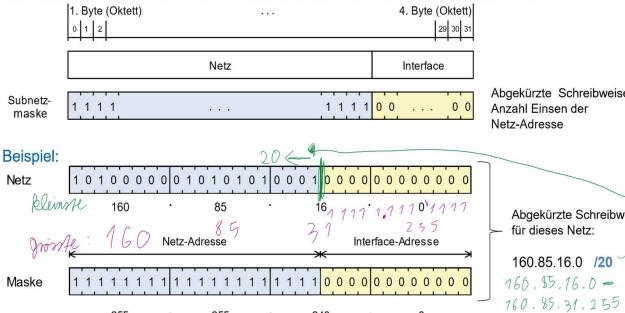
- Man soll bei den Adressen erkennen können zu welchem Netz sie gehören (Bspw. Postanschrift).
- Arbeitet mit Defaulteinträgen.



## Subnetting (IPv4)

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

Die Subnetzmase bestimmt die Grenze zwischen Netz- und Interface-Adressbits:



Die Maske ist eine AND Verknüpfung mit der IP

Gegeben ist das Netz 172.30.10.0/25.

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

## IP Paket

⇒ Verbindungslos und unzuverlässig.

1. Byte	2. Byte	3. Byte	4. Byte
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	0 00000000	128 10000000	192 11000000
	Identification Number	Flags	Fragment Offset
Time to Live	Protocol	IP Header Checksum	
		IP Source Address	
		IP Destination Address	
		Options / Padding	

Ein IP-Paket 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

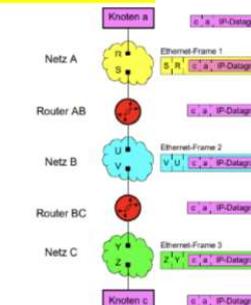
## IP Paket Übertragung

⇒ Ethernet Frames werden bei jedem Router erneuert!

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

Bemerkungen:

- Knoten a hat auch als Host eine IP Tabelle.
- Router haben pro Port separate Netzadressen.
- Wenn TTL = 0 wird ICMP an Sender geschickt.

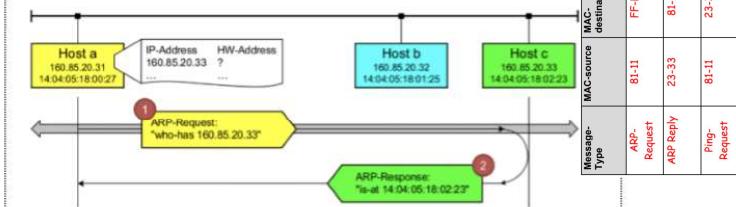


## Adressauflösung

> ARP (Address Resolution 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.

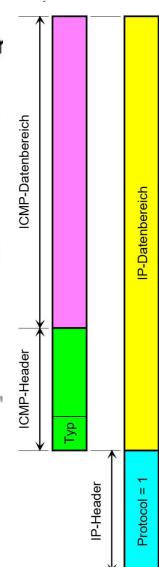
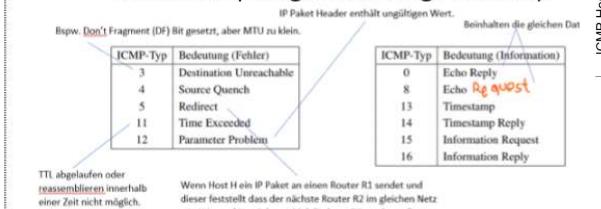


⇒ Spezielle Request ARP Komponenten:

- 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).



## 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. → Header + Daten

> Fragmentierung (Beim Sender oder Router):

IP Paket Header Komponenten: Header + Daten

- 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 woher (bis zu 8'192 Fragmente möglich).

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

> Reassembly (Beim Empfänger / Endknoten):

Bsp. Ein IP Paket 1500 Bytes lang (bestehend aus 20 Header und 11480 Daten) wird über eine MTU von 580 gesendet

Fragment Offset FO	Total Length TL	More Fragments MF
0	580	560+20 1
70	580	560+20 1
140	380	0

## Transport Layer (Schicht 4)

### 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.
- Acknowledgement-Nr.
- Data Offset
- ECN-Flags
- Control Bits
- Window
- Urgent Pointer
- Options

Nummer zur Ordnung der Segmente  
n + 1 → Daten korrekt und vollständig  
Gibt an wo Daten beginnen / enden  
Explicit Congestion Notification  
URG, ACK, PSH, RST, SYN, FIN  
Verfügbare Puffergrösse  
URG = 1 → Position der wichtigen Daten  
Häufigste Verwendung: MSS

⇒ Verbindungsorientiert und zuverlässig.  
⇒ Min. 20 Bytes, Max. 60 Bytes

## TCP Verbindungsphasen

> Verbindungsauftbau:

Client Zustände: CLOSED, SYN-SENT, ESTABLISHED  
Server Zustände: LISTEN, SYN-RECEIVED, ESTABLISHED

Legende: Auf Anforderung warten, Anforderung geschickt, Anforderung erhalten, Verbindung besteht

Wenn Fin-Flag dann Verbindungsabbau

> Datenaustausch:

Hin & Her

⇒ 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.

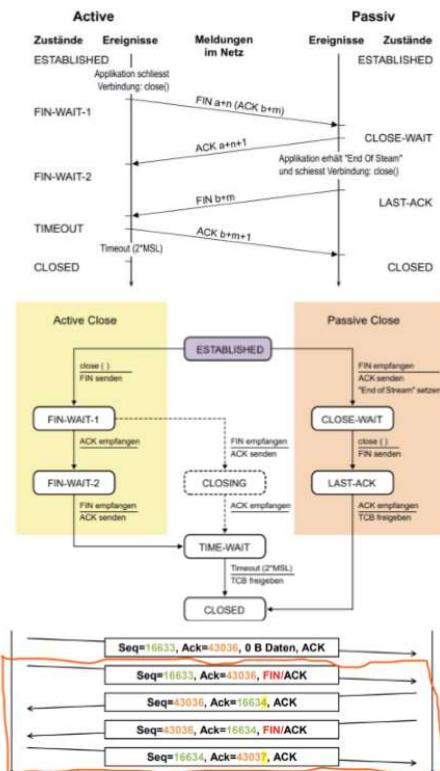
Im TIME-WAIT Zustand wartet der «Closing-Host» eine gewisse Zeit, um auch im Fall eines Übertragungsfehlers die Verbindung regulär schliessen zu können.

Abbauanforderung gesickt  
Auf Lokale Verbindung warten  
Verbindungsabbau bestätigt

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

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

#### > Verbindungsabbau:



#### 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*

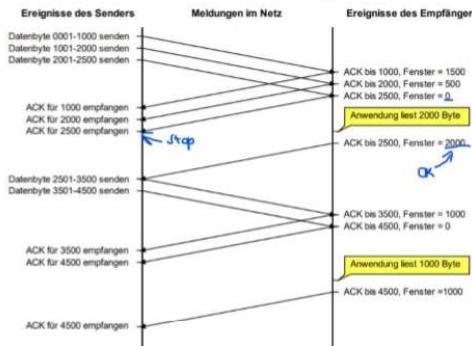
$$\alpha = 0.125: SRTT_n = (1 - \alpha) \cdot SRTT_{n-1} + \alpha \cdot RTT_n$$

$$\beta = 0.25: RTTVar_n = (1 - \beta) \cdot RTTVar_{n-1} + \beta \cdot |SRTT_n - RTT_n|$$

$$RTO_n = SRTT_n + 4 \cdot RTTVar_n$$

#### TCP: Fluss-Steuerung (Sliding Window)

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



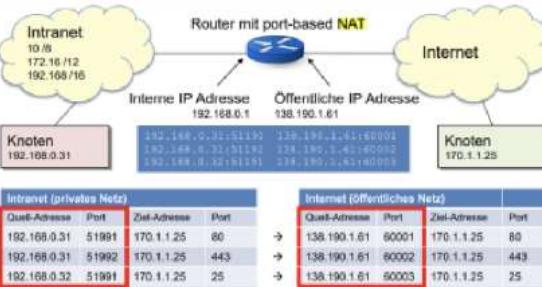
Fenstergröße im Window Feld des TCP Headers.

#### TCP: Überlast Steuerung (Congestion Control)

- ⇒ Fluss-Steuerung schützt 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)

### NAT (Network Address Translation)



- 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).

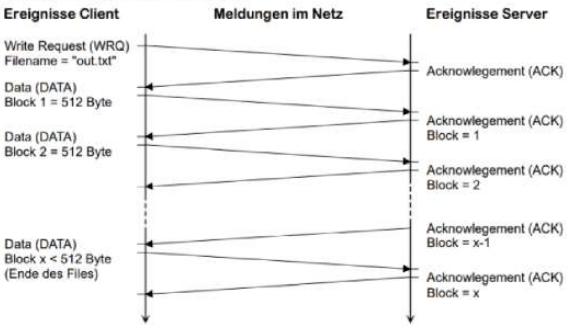
NAT Database		Global Port
Type Local Address : Port		
Dyn. 10.1.1.22	: 36789	34201
Dyn. 10.1.1.44	: 49919	34202
Stat. 10.1.1.94	: 69	69

Primär für die Übersetzung von IPv4 zu IPv6

## 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).

## Glossar:

RTO	Retransmission Time Out	Zeit, nach der ein gesendetes Paket als verloren gilt und erneut gesendet wird (ACK wurde nicht erhalten).
	Sliding Window	Mechanismus in der Flusssteuerung, reguliert Datenübertragung, sodass Sender nicht mehr Daten sendet als Empfänger verarbeiten kann. Empfänger sendet mit ACK auch die Fenstergröße = Wieviel Daten er bereit ist zu empfangen.
	Congestion Control	Staukontrolle, steuert und vermeidet Überlastungen verursacht durch Datenstau.
	Slow Start	Mechanismus der Congestion Control. Hierbei wird die Übertragungsrate langsam gesteigert und bei einem erreichten Schwellenwert angepasst.
	Top-Level-Domain	Höchste Ebene der Namensauflösung. (z.B. ".com", ".net" usw.)
	Second-Level-Domains	"Standard" Subdomain (z.B. <a href="http://www.zhaw.ch">www.zhaw.ch</a> -> "zhaw" ist Second-Level-Domain.)
	Filtering Database	Beinhaltet jede bekannte MAC-Adresse und über welchen Port diese erreicht wird.
	Frame Flooding	Ausgabe des frames an allen ports
ACK	Acknowledgment Number	Nummer des Empfänger von Datenpaketen, um dessen Empfang zu bestätigen. Ist die Sequenz Number des nächsten erwarteten Bytes.
RTT	Round-Trip-Time	Zeitmessung Datenpakete um von einem Ausgangspunkt zu einem Ziel zu gelangen.

UDP	User Data Programm	verbindungsloser unzuverlässiger Dienst im Internet
TCP	Transmission Control Protocol	verbindungsorientierter zuverlässiger Dienst im Internet
RFC	Request for Comments	Document that contains specifications and organizational notes about topics related to the internet and computer networking.
ppm	Parts per million	Parts per million wird für die Genauigkeit bei der Datenübertragung beschrieben. Ex. Ethernet standard = 5ppm
AMI-Code	Alternate Mark Inversion	Eine Art um Binär Daten zu schicken. Keine Gleichspannung wird hier geschickt.
	Baudrate	Schrittgeschwindigkeit = Leistungs-Symbole pro Sekunde
B	Bandbreite B (Hz)	Eigenschaft des Übertragungskanals und durch das Medium begrenzt
	Symbolrate f s (Bd)	Anzahl der Symbole pro Zeit. Limitiert durch die Bandbreite ( $\leq 2B$ ) (Nyquist)
R	Bitrate R (bps)	Produkt von Symbolrate und mittlerem Informationsgehalt der Symbole (Hartley)
	Kanalkapazität C (bps)	Berücksichtigt eines realen Kanal Signal-zu-Rausch Leistungverhältnis S/N (Shannon)
	Frame = Datenrahmen	Ein Frame besteht meist aus einem Header mit der Anzahl Elemente im Datenblock, dem Datenblock und dem Code für die Fehlererkennung (z.B. Checksumme)
	Flag	Frames werden ohne Unterbruch gesendet. Stehen keine Daten an, werden Flags gesendet. Frames werden durch ein Start- und ein End-Flag begrenzt.
FER	Frame Error Ratio	Fehlerhaft empfangene Datenrahmen (Frames)
RER	Residual Error Ratio	Unentdeckte, fehlerhaft empfangene Frames (Fehlererkennungsalgorithmus erkennt diese Fehler nicht)
	Hamming-Distanz	"Wie viele Bits muss ich flippen um wieder ein gültiges Code-Wort zu erhalten? je grösser Hamming-Distanz, desto besser Fehlererkennung."
BEC	Backward Error Correction	Bei erkanntem Fehler entsorgt Empfänger die Nachricht. Bei TCP: Es gibt keine Rückmeldung und Sender schickt Nachricht nochmals.
FEC	Forward Error Correction	Man prüft Redundanten um zu schätzen, was wohl gesickt hätte werden sollen.
	Token Verfahren	Gesteuerter Medium Zugriff. Anstelle eines Tokens wird ein Frame geschickt....
RMA	Random Medium Zugriff	Zufällige Zeit für das senden auf einer Leitung um Kollisionen zu verhindern
LAN	Local Area Network	Reichweite: 10 bis wenige km, Folie S.9
	Unicast (Übertragungsart)	Ein Empfänger
	Multicast (Übertragungsart)	Gruppierte Empfänger (Funktionelle Adressierung)
	Broadcast (Übertragungsart)	An alle Geräte gerichtet
	IEEE MAC Adressen	Erste drei Byte sind Hersteller-eindeutig, letzte 3 Bytes sind Laufnummern (global eindeutig). Das erste Bit bestimmt individualität, und das zweite Bit bestimmt ob die Adresse registriert oder nicht ist.
MAC	Media Access Control	
	unregistrierte MAC Adresse	Wenn das zweite Bit einer MAC Adresse eine 1 ist, bedeutet die Adresse kann nicht als Quelle verwendet werden, nur als Empfänger.
	Ethernet 802.3	Wurde in 1975 entwickelt. Fullduplex, Bustopologie
	Ethernet 802.3 Frame Format	Frame-Länge 64 - 1518 Bytes, Overhead 18 Bytes, Payload 46 - 1500 Bytes Wenn weniger wie 46 Bytes, wird mit 0 aufgefüllt
Pre / SFD	Physical Layer Teil eines Frame	7 Byte Preamble, 1 Byte SFD
	Frame Overhead	6 Byte Destination Adress, 6 Byte Source Adress, 2 Byte Length / Type, Payload, 4 Byte Frame Check Sequence
IFG	Interframe Gap	mindest Pause bis zum nächsten Frame: 12 Byte
	Netto-Datenrate in %	Verhältnis der Payload zur gesamten Främelänge + IFG
	VLAN TAG	VLAN TAG wird von den Bridges eingefügt und vor dem Endgerät wieder entfernt.
	VLAN ID	Identifier der einzelnen VLAN, Bridges ordnen Frames aufgrund der VLAN ID den unterschiedlichen VLAN zu.
	PCP (Priority Code Point)	8stufige Priorisierung, erlaubt Priorisierung von gewissen Frames.
	DEI (Discard Eligibility Indicator)	bei hohem Verkehr werden Frames bei welchen das DEI Bit "1" ist zuerst discarded.
	Access Port	Port welcher eindeutig einem VLAN zugeordnet werden kann. Untagged Daten
	Trunk Port	Port welcher mit anderen Bridges verbunden ist und Frames von verschiedenen VLAN transportiert. Tagged Daten
	Address Learning	Bridges müssen nicht vorkonfiguriert werden, sondern lernen die Verbindungen indem sie den Verkehr an ihren Ports abhören.

	Hello-Time	Das ist der Zeitintervall zwischen dem Senden der BPDUs
	Aging Time	die längste Zeit in welcher die Filtering Database die Mac-Adressen abspeichert
	On-the-Fly-Switching =Cut-Through Switching	Weiterleitung des ankommenden Frames nach Empfang der 6-Byte-Destination-Adresse. Da nicht das gesamte Frame empfangen werden muss, tritt bei 10 MBit/s nur eine Zeitverzögerung von ca. 40 µs ein
	Autonegotiation	Ein Verfahren, zum selbständig die maximal Übertragungsgeschwindigkeiten und Duplex-Verfahren auszuhandeln und konfigurieren.
	Crossover Kabel	Ein vier- oder achtadriges Twisted-Pair-Kabel, dass beim RJ45 Stecker gewisse Kabelenden vertauscht hat, für Verbindung von gleichen Gerätetypen.
	Fast Link Impulse (FLP)	spezielle elektrische Signale, die verwendet werden, um die Geschwindigkeit und den Duplex-Modus automatisch auszuhandeln.
	Auto-Crossover	Das Auto-Crossover wurde implementiert für die Ersatzung von Crossover-Kabeln.
	Auto-Polarity	Auto-Polarity erlaubt zudem vertauschte Drahte eines Aderpaares zu korrigieren.
	Host	Im TCP/IP Modell werden Sender/Empfänger als Hosts bezeichnet
	Broadcast-Adresse	für die Übertragung von Nachrichten und Datensätzen an Netzwerksysteme
	Local-Host-Adresse	127.0.0.x, Referenziert auf den Server auf dem eigenen Rechner
	Netzmaske	Zeigt an welcher teil der IP-Adresse zur Identifikation des netzes verwendet wird. Schema -> 111...1000 Länge 32 bit. Jedes bit welches ein 1 hat gehört zur netzwerkidentifikation. Die Netzmaske wird notiert durch ein /Anzahl gesetztes Bits. Zum Beispiel 1.2.3.201/16
	Routing-Table	Verzeichnis welches Netzwerk über welches Interface erreichbar ist.
	Flaches routing	Router kennt jedes Netzwerk an welches er angeschlossen ist.
	Hierarchisches Routing	Beim Hierarchischen Routing werden kleinere Netze zusammengefasst unter einer Maske. Durch das müssen andere Router nur einen Eintrag für mehrere Netze haben.
	Subnetz	Ein kleineres Netz welches entsteht wenn ein grösseres aufgeteilt wird
	Supernetting	Beschreibt das Zusammenfügen von kleineren Netzen zu grösseren. Dieser Prozess kann helfen Routentabellen zu verkleinern
	Subnetting	Das Aufteilen eines Netzes in kleinere Netze.
	Routingtabelle	Stehen immer Netze mit der zugehörigen Netzmaske und was man damit tun muss
	localhost	Der localhost, auch als "Loopback-Adresse" bezeichnet, wird verwendet, um eine IP-Verbindung oder einen Anruf zu einem lokalen Computer herzustellen.
TTL	Time to Live	feld im IP Header, beschränkt Datenpakete, wie lange diese im Netzwerk verbleiben können. Bei z.B. 20 Durchgängen kann das Paket durch 19 weitere Router.
	Identification Number	Eindeutige Kennung des ursprünglichen IP-Pakets Erlaubt Identifikation zusammengehöriger Fragmente
	Fragment Offset	Gibt an, wo in einem fragmentierten IP-Paket ein Fragment hingehört (= 8 Byte)
MTU	Maximum Transfer Unit	Grösste Datenpaketgrösse, die ohne Fragmentierung übertragen werden kann.
	Link-Local Adresse	IPv6 Adresse, die nur im lokalen Netz gültig ist (analog zu einer privaten IPv4 Adresse)
NDP	Neighbor Discovery Protocol	ARP-Funktion für IPv6
UDP	User Datagram Protocol	dient zum De- / Multiplexen der Datagramme zu den Applikationen. UDP ist Unzuverlässig und Verbindungslos.
	Well Known Ports (oder Sys-Ports)	1 - 1023 standardisiert durch IANA / IETF
	Registered Ports (oder User Ports)	1024 - 49'151 reserviert durch herstellerspezifische Applikationen
	Dynamic / Private Ports	> 49'152 - 65'536 kann nach belieben verwendet werden
	socketpair plus protocol	Eindeutige bestimmung Kommunikationsbeziehung durch 5 Parameter: (Source und Destination IP Addressen, Source und Destination Port Number, Used Protocol)
	UDP Header	Source Port 2bytes, Destination P 2 Bytes, Message Length 2 Bytes, Checksum 2 Bytes
TCP	Transmission Control Protocol	Full duplex: gleichzeitig senden und empfangen. Stream: Bytes kommen in korrekter Reihenfolge an. TCP ist verbindungsorientiert und zuverlässig.
	TCP-State-Machine	Verschiedene Zustände, die eine TCP-Verbindung durchläuft. Steuerung des Verbindungsauftaus und Datentransfer
SEQ	Sequence Number	Sequenznummer, nummeriert jedes einzelne Byte der über TCP gesendeten Daten. Identifiziert Daten, die Empfänger bereits erhalten und als nächstes erwarten.
SYN	Synchronize Sequence Numbers	Steuerflag, wird in den ersten Schritten des Drei-Wege-Handshakes verwendet um neue TCP-Verbindung zu starten