

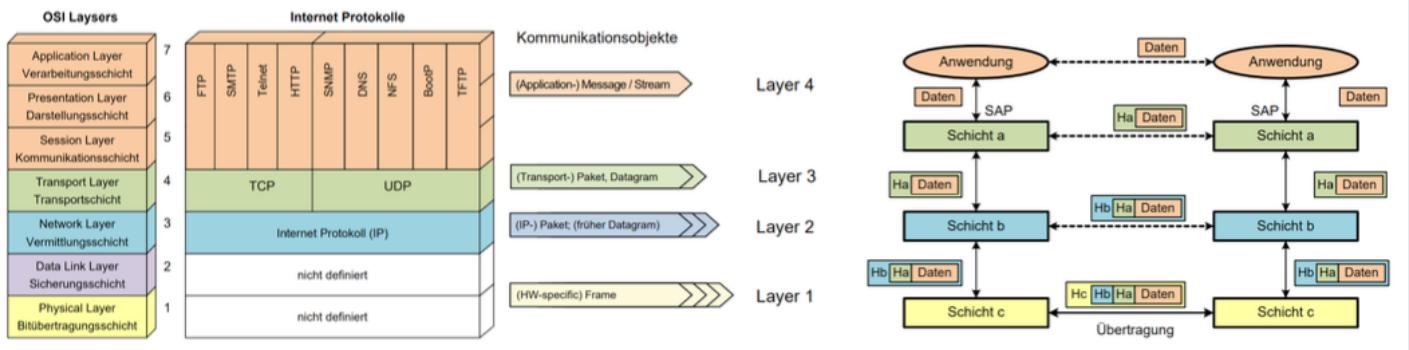
1 OSI-Modell

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



(I) Physical Layer

Übertragung eines Bit-Stromes zwischen zwei Knoten über physikalisches Medium.

- Elektrische & optische Eigenschaften (Frequenz, Timing)
- Codierung (Manchester etc.)
- Mechanische Eigenschaften (Pinbelegung)

(II) Data Link Layer

Stellt der höheren Schicht gesicherte Übertragungsstrecke zur Verfügung.

Für zwei Teilnehmer (Peer to Peer):

- Massnahmen zur Fehlererkennung & Korrektur
- Verpacken der Datenblöcke vom Network Layer in Datenrahmen und Auspacken der Datenblöcke aus empfangenen Datenrahmen
- Flow Control: Massnahmen, dass Sender nicht zu schnell sendet

Mehrere Teilnehmer (gilt zusätzlich):

- Adressierung der Teilnehmer durch eindeutige Adresse
- Medium Access Control: Steuerung des Zugriffs

(III) Network Layer

Daten austauschen zwischen Knoten vereinheitlichen. Dazu netzweite Layer 3 Adressierung erforderlich sowie Routing-Verfahren.

Verbindungsorientierter Dienst:

- Datenpakete werden für Weiterleitung entschlüsselt, mit lokalem Identifier versehen
- Vor der Übertragung wird Pfad durch das Netzwerk festgelegt
- Nach Übertragung werden Ressourcen wieder abgebaut
- Wichtiges Verfahren: Multi Protocol Label Switching (MPLS)

Verbindungsloser Dienst:

- Paketinhalt erhält vollständige Adresse des Empfängers
- Jeder einzelne Knoten entscheidet selbst, welcher Weg genutzt wird
→ Dazu werden Informationen über Verbrauch in Routing-Tabellen abgelegt (Beispiel: IP-Protokoll)

Verbindungsorientiert vs Verbindungslos

- | | |
|--|---|
| ◦ Charakteristik (Delay, Verlust) durch vorgegebenen Pfad sichergestellt | ◦ Keine Routberechnung = kein Aufwand |
| ◦ Gezielte Lenkung des Verkehrsstroms | ◦ Beim Unterbruch wird andere Route verwendet |
| ◦ Reihenfolge der Daten bleibt | |

(IV) Transport Layer

Stellt End-to-End Übertragungsqualität sicher. Wird abhängig von Layer 1-3 entsprechend Zuverlässigkeit gestaltet.

- User Data Protocol (UDP): Verbindungslos, unsicher
- Transmission control Protocol (TCP): Verbindungsorientiert, sicher

(V) Session Layer

Legt Ablauf der Kommunikation fest. (Aufbau und Abbau von Sessions)

Beim Ablösen einer Session für Wiederaufbau verantwortlich.

(VI) Presentation Layer

Für Darstellung der zu übertragenden Daten zur Verfügung.

Typisches Beispiel: Kodierung der Daten auf standardisierte Art:
◦ ASCII, ISO, Unicode

(VII) Application Layer

Bindeglied zur eigentlichen Anwendung.

- Typische Protokolle:
 - File Transfer Protocol (FTP)
 - Simple Mail Transfer Protocol (SMTP)
 - Hypertext Transfer Protocol (HTTP)
 - Domain Name System (DNS)

2 Übertragungsmedien

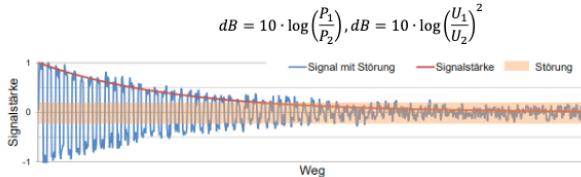
Ausbreitungsgeschwindigkeit

Funk- oder Licht-Signale sind elektromagnetische Wellen, die sich im Vakuum mit Lichtgeschwindigkeit $c_0 = 299'792'458 \frac{m}{s}$ ausbreiten. Die Vakuumgeschwindigkeit kann nicht überschritten werden.

$$c_{\text{Medium}} = 200'000 \frac{km}{s} \approx \frac{2}{3} c_0$$

Signaldämpfung

Die Signaldämpfung bezeichnet die Leistungsabnahme eines Signals auf einer Übertragungsstrecke. Sie ist ein wesentlicher Faktor, der die erreichbare Distanz beschränkt. Die Angabe der Signaldämpfung erfolgt in dB als logarithmische Verhältniszahl von Eingangsleistung P_1 zur Aufgangsleistung P_2 .



Dämpfung von 6dB

Leistungsabnahme: Faktor 4
Spannungsabnahme: Faktor

Dämpfungsbelag

Für Übertragungsmedien ist die Dämpfung pro Distanz massgebend. Typischerweise in dB pro 100 m angegeben.

Kabel-Typen

- Koaxialkabel Geeignet für hochfrequente Signale
- Twinaxial-Kabel Hoher Schutz
- Twisted Pair (TP) Häufig im Einsatz (Shielded / Unshielded)
- Glasfaser Hohe Bandbreite, Geringe Dämpfung, Resistent

Schirmeigenschaften

- Drahtgeflecht -> niederfrequente Einstreuungen
- Metallisch beschichtete Folien -> hochfrequente Störungen

xx/y worin TP für Twisted Pair steht:

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

(2.2) Koaxialkabel

Gut geeignet für Übertragung von hochfrequenten Signale.

- Kleiner Dämpfungsbelag
- Unempfindlich gegenüber elektromagnetischen Störungen
- Für grosse Distanzen geeignet
- Dürfen nicht geknickt / verquält werden

⇒ Heute: Für Peer to Peer in Hochgeschwindigkeitsnetzen

Funktionsprinzip

Störungen können kapazitiv, induktiv oder galvanisch auftreten.

Durch das Senden eines komplementären Signals und das Addieren beider Signale beim Empfänger durch einen Differenzverstärker, haben sich die Signale vollständig auf und das Störignal bleibt übrig. Bei den direkten Leitungen ändern sich lediglich die Art / Umwandlung der Aufteilung des Signals. Das Prinzip bleibt dasselbe.

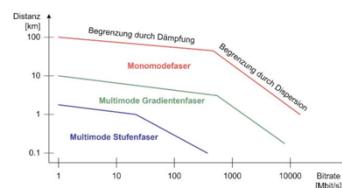
(2.4) Lichtwellenleiter

Bestehen aus Glas und haben folgende Vorteile:

- Vollständige Unempfindlichkeit gegen elektromagnetische Störungen
- Kleine Signaldämpfung => Große Distanzen
- Große Bandbreite und große Übertragungsgeschwindigkeiten

Dispersion: Verzerrung des Signals => Nicht mehr erkennbar

Arten von Glasfasern:



3 Physical Layer

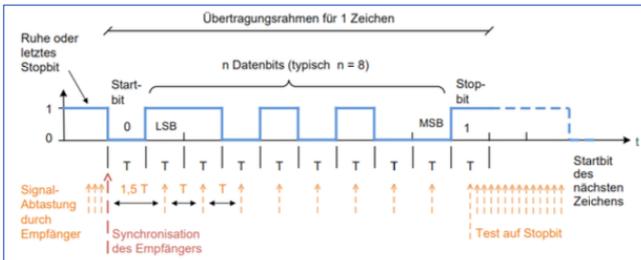
⇒ Ungesicherte Übertragung eines Bitstroms zwischen 2 Teilnehmern über das physikalische Medium

Serielle asynchron Übertragung (ohne Synchronisations-Takt)

Zwischen Sender und Empfänger werden folgende Abmachungen benötigt

- Bitrate
- Anzahl Datenbits Typischerweise 1 Byte
- Anzahl Stopbits Typischerweise 1 Bit

Nachteil: bei einem Bitfehler => Datenblock wertlos



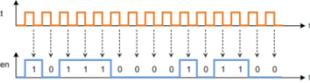
Die **Taktrückgewinnung** ist möglich, solange regelmässig Zustandsänderungen auftreten.

Serielle synchron Übertragung

Bei der synchronen Übertragung arbeitet der Empfänger mit dem gleichen Takt wie der Sender.

- Es werden keine Start- und Stopbits benötigt
- Der Takt muss zusätzlich übertragen werden

Die Übertragung des Takts erfolgt über ein Codierungsverfahren oder eine zusätzliche Leitung.



Effizientere Bandbreitennutzung -> keine Start + Stopbits

Arten der Kommunikation (Verkehrsbeziehung)

- **Simplex** Ein Kanal, in eine Richtung
- **Halbduplex** Ein Kanal, abwechselndweise in zwei Richtungen
- **Voll duplex** Ein Kanal pro Richtung

Arten der Verbindungen (Kopplung)

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

Datenübertragungsrate

- **Baudrate** Symbole pro Sekunde
- **Zeichenrate** Zeichen pro Sekunde

Die maximale Symbolrate f_s (Baud) ist gleich der doppelten Bandbreite B (Hz) des Übertragungskanals. $f_s = 2B$

Bandbreite

Die Bandbreite hängt von der Übertragungsstrecke und der Stärke des Signals im Vergleich zu den vorhandenen Störungen, ab.

- Eigenschaft des Übertragungskanals und durch das Medium begrenzt
- Maßeinheit Hertz (Hz)

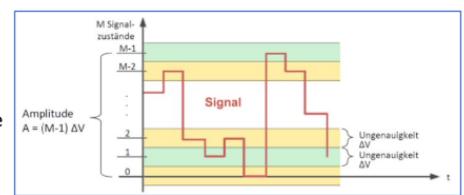
Maximal erreichbare Bitrate

Maximal Bitrate R [bit/s]

$$\bullet R \leq 2B \cdot \log_2(M)$$

Unterscheidbare Signalzustände

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



Leitungscodes

- Separate Leitung zur Übertragung des Takts

Anforderungen: Taktrückgewinnung & Gleichspannungsfreiheit

Gleichspannungsfreiheit

- Mittlerer Spannungswert eines Signals = 0
- 0 und 1 Bits wechseln sich regelmäßig ab

Taktrückgewinnung

- Lokaler Takt darf nie verloren gehen
- Zu viele 0 sorgen für Taktverlust

4 Data Link Layer (Sicherungsschicht)

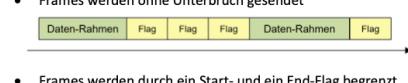
Framing (Asynchron)

- Keine Daten → Nichts wird gesendet
- Zu Beginn eines Frames wird ein Start-Bit gesendet



Framing (Synchron)

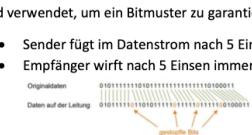
- Frames werden ohne Unterbruch gesendet



Framing: Bitstopfen

Wird verwendet, um ein Bitmuster zu garantieren.

- Sender fügt im Datenstrom nach 5 Einsen immer eine 0 ein.
- Empfänger wirft nach 5 Einsen immer ein Bit weg.



Fehlererkennung / Fehlerkorrektur

- **FER** (Frame Error Ratio)
- **RER** (Residual Error Ratio)
- **BER** (Bit Error Ratio)

Wahl der Framelänge

- Lange Frames Höhere Nutzdatenrate, Fehleranfälligkeit
- Kurze Frames Tiefer Nutzdatenrate, Zuverlässigkeit

Datenraten

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

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

Zugriffsmechanismen (Media Access Control = MAC)

(4.6) Medium Access Control

Header: Slave, Verzögern

Header: Zögert zeitlich Schritte ab und kontrolliert Zugriff.

Vorteil: Keine Korrasie

Nachteil: Master = Single Point of Failure (SPoF)

Master: Dezentralisiert, Master: Anfordung (Startup, Token Verlust)

Slave: Zentralisierte Zuordnung, Daten wird an alle Stationen gleichzeitig gesendet.

Vorteil: Optimierung möglich (Auslastung, Distanz)

Nachteil: Planung schwierig, jeder Knoten muss den Daten herunterholen

Carrier Sense Multiple Access CSMA

Jede Station darf nach Kontrolle des Bus (frei oder nicht) direkt beginnen.

Vorteil: Kein Verlust, Realisierung geschwierig

Nachteil: Vollkommen können ausfallen

CSMA/CD = Collision Detection: Überlappungszeit, später Empfang

CSMA/CA = Collision Avoidance: Ressource-freies Wiederaufsenden

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

Einfluss der Frame Länge auf den Durchsatz

Frame Erfolgswahrscheinlichkeit: $(1 - p_e)^N$

Frame Fehlerwahrscheinlichkeit: $1 - (1 - p_e)^N$

Optimale Frame-Länge:

$$\sqrt{\frac{H}{p_e}} \quad (H = \text{Header-Länge}; p = \text{BER})$$

Fehlerkorrektur

Erkennbare Fehler = Hamming-Distanz - 1

(4.5) Fehlerkorrektur

Backward Error Correction:

Nach jedem Paket muss Bestätigung folgen. Bei hoher BER wird das sehr ineffizient.

Forward Error Correction (FEC)

Nach erkannten Fehlern wird die am wahrscheinlichsten gesendete Nachricht geschickt.

Korrigierbare Fehler = $\frac{\text{Hamming-Distanz} - 1}{2}$

Parity

- eine der einfachsten Methoden für die Fehlererkennung

• 1-Bit Fehler erkennbar

Jedem Datenelement wird ein zusätzliches Parity-Bit hinzugefügt, so dass die Anzahl der Einsen inklusive Parity-Bit entweder gerade (Even Parity) oder ungerade (Odd Parity) ist.

5 Local Area Network

Im LAN-Bereich gibt es drei Übertragungsarten

- Unicast an einzelne Stationen
- Broadcast an alle Stationen
- Multicast an eine Gruppe von Stationen

Als Leitungscode wird ein *Manchester-Code* eingesetzt.

- 1 positive Flanke, 0 negative Flanke
- Erlaubt die Taktrückgewinnung auf einfache Weise
- Bandbreite von 10 MHz benötigt (also das doppelte des theoretischen Minimums)



Kollisionen können durch Überlagerung von Signalen entstehen. Kollisionen müssen erkannt werden.

Bedingung für Kollisionserkennung

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

Maximale Ausdehnung eines Segments

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

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

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

Bustopologie:

- Stationen passiv angeschlossen
- Werden nur beim Senden aktiv
- Empfänger erkennt, falls Paket für ihn relevant



Ringtopologie:

- Besitzt Verfahren zur Vermeidung von Loops.



Starstopologie:

- Jeder Knoten an Switch



Linentopologie:

- Peer to Peer Anordnung
- Jeder Knoten muss Daten empfangen und weiterleiten
- Ausfall eines Knoten = Spaltung LAN



Dopperringtopologie:

- Erhöhung Redundanz: Ausfall eines Rings => Anderer übernimmt

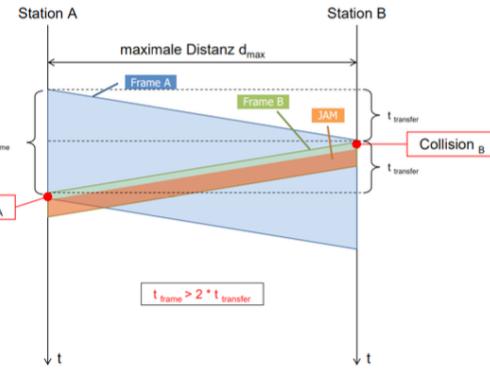


Baumtopologie:

- Hierarchische Erweiterung Starstopologie



Bedingung für Kollisionserkennung



Ethernet Format

Length/Type (2 Bytes)

- Fall 1: Länge von DATA ohne PAD (≤ 1500)
- Fall 2: Typ von Data = Protokoll der nächsten Schicht (≥ 1536)

Data / Padding (46 – 1500 Bytes)

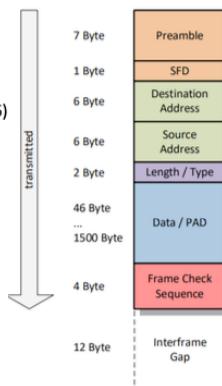
- Enthält die eigentlichen Datenbytes
- Bei weniger als 46 Bytes wird mit PAD Bytes abgefüllt

Frame Check Sequence, FCS (4 Bytes)

- IEEE CRC-32 Algorithmus

Interframe Gap, IFG (12 Bytes)

- «Zwangspause» zwischen aufeinanderfolgenden Frames
- Ist NICHT Teil des Ethernet Frames



Repeater and Collision Domain

Eine **Collision Domain** ist ein Teilbereich eines LANs, in dem die Frames der Stationen miteinander kollidieren können.

Erkennen von Kollisionen

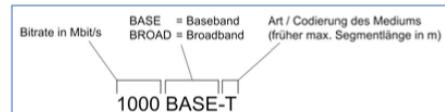
- Halbduplex Collision Detection Unit
- Voll duplex Keine Kollisionen

Shared Medium Ethernet

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

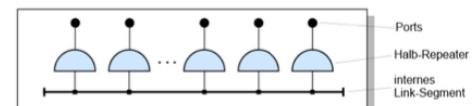
Normen für CSMA/CD

- Verbilligung (Thick Ethernet → Thin Ethernet)
- Vereinfachung (Koaxial → Twisted Pair)
- Leistungssteigerung (10 → 100 ... 100'000 Mbit/s)



Repeater / HUB

Ankommendes Signal wird an alle anderen Ports weitergeleitet, regeneriert und ausgesendet.



CSMA/CD = Carrier Sense Multiple Access with collision detection

(I) Senden ohne Kollision:

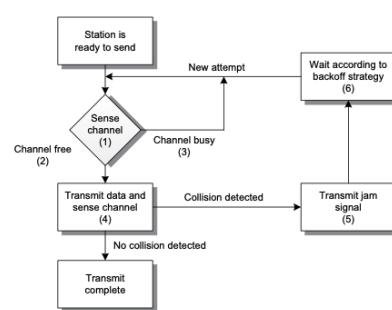
- Warten bis Kanal frei
- Physical Layer sendet Preamble und SFD, damit Empfänger sich synchronisieren kann
- Physical Layer überwacht während Sendezzeit Signalepegel
⇒ Bei Kollision (Signaleinstieg) wird Collision Detected Signal an Data Link Layer gesendet

(II) Empfangen ohne Kollision:

- Alle Knoten erkennen Senderseiten und medien ihrem Data Link Layer keine Jendiversität zu unternehmen
- Alle Knoten im LAN werden zu Empfangsknoten

(III) Senden mit Kollision:

- Falls mehrere Knoten gleichzeitig Kanal als frei sehen
- JAM - Signal wird an alle versendet
- Data Link Layer des Empfängers erkennt durch Prüfsumme Fehler



6 Switched LAN und Ethernet-Technologien

Wird die Adresse nicht gefunden, wird das Frame an alle gesendet!

Bridges = L2-Switch mit mehreren Ports

Bridges verfügen über einen Mechanismus zum *Erlernen von Adressen*. Eine Bridge hört den Verkehr von allen Ports ab und merkt sich die Sender-Adressen aus den empfangenen Frames in der sogenannten «*Filtering Database*». Diese beinhaltet für jede bekannte Mac-Adresse das Bridge-Port, über welches der zugehörige Knoten erreichbar ist. Unbenutzte Einträge in der Filtering Database werden nach einer gewissen Zeit automatisch gelöscht.

Diese Verarbeitung benötigt etwas Zeit, ist aber dennoch vorteilhaft, da das Paket nur an die richtige *Collision Domain* geschickt wird.

Multi-Port-Bridges verbinden mehr als zwei Segmente.

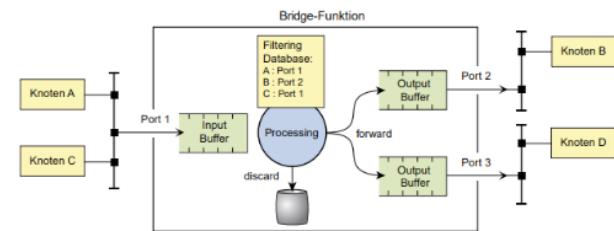
- Daten werden ausschliesslich an den richtigen Port weitergeleitet.
- Standard-Komponente zur Kopplung von Segmenten
- Werden als Ethernet-Switch bezeichnet

Broadcast and Collision Domain

Eine **Collision Domain (CD)** besteht aus mit Repeatern zusammengeschlossenen Segmenten.

- Max. halb so lange wie die Ausdehnung des kürzesten Frames

Ein virtuelle LAN bildet eine **Broadcast Domain**. Das heisst die Grenzen für die Verteilung der Broadcast-Frames.



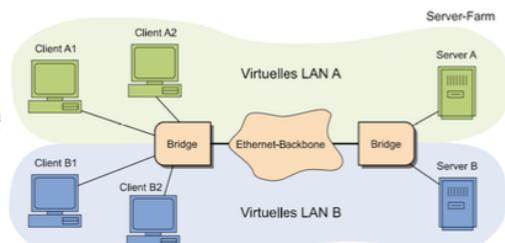
VLANs

Mithilfe von virtuellen LAN kann ein grosses Netz in unabhängige logische Netze aufgeteilt werden. Jedes Switch-Port kann einem beliebigen VLAN zugeordnet werden.

VLAN-Tag

- VLAN-ID im VLAN-Tag wird zur Zuordnung verwendet
- Priority Code Point ermöglicht die Priorisierung gewisser Applikationen
- Discard Eligibility Indicator 0 → Frame wird bei Engpässen zuerst verworfen

Trunk = Tagged, Access = Untagged



Spanning Tree (Redundanz-Protokoll)

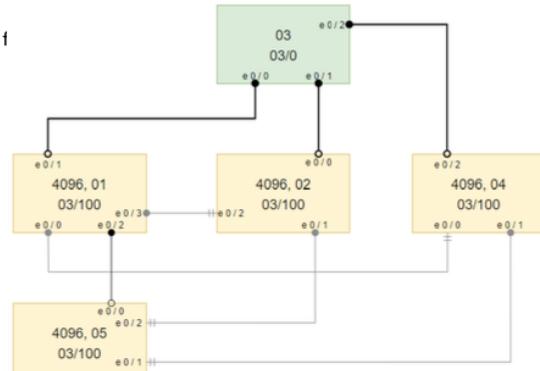
Beim Spanning-Tree werden von redundanten Pfaden alle außer einer gesperrt. Im Fehlerfall wird f

Der Algorithmus bestimmt eine Root-Bridge, von welcher aus dem Baum aufgespannt wird.

- Alle Knoten werden genau einmal verbunden
- Verbindungen, die zu Schleifen führen werden gesperrt
- Die Auswahl der Root-Bridge ist vom *Bridge-Identifier* abhängig
- Der *Bridge-Identifier* besteht aus einer wählbaren Priorität und der MAC-Adresse

Vorgehen

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



Ethernet-Systeme

- *Autonegotiation* Ermittlung der besten Betriebsart durch Austausch der Leistungsmerkmale zweier Netzwerkkomponenten.
- *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	MLT-3, 4B5B 2 Aderpaare simplex	PAM-5, 8B/10B 4 Aderpaare duplex	PAM-16, 64B/65B, FEC 4 Aderpaare duplex
Baudrate	10 MBaud	125 MBaud	4 x 125 MBaud	4 x 800 MBaud
Link Pulses	NLP	FLP	FLP	FLP

Merkmale von Bridges

Anzahl Ports	Steckergroesse ist im Extremfall die Limitierung
Adressabelle	Wie viele Stationen können im LAN existieren
Filtrate	Maximale Frames / s / Port (Empfangsrichtung)
Transferrate	Maximale Frames / s / Port (Senderichtung)
Backplane / Fabric Kapazität	Maximaler Gesamtdurchsatz zwischen allen Ports
Architektur	Store-and-Forward: Frame wird komplett empfangen und dann weitergeleitet Cut-Through: Frame wird schon nach Decodierung der Zieladresse weitergeleitet Leitet auch korrupte Frames weiter, in der Regel aber kein Problem Adaptive Cut-Through: Schaltet bei hohen Fehlerraten 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

Herausforderungen bei Vervielfachen der Datenrate:

- (1) CSMA/CD: Maximale Segmentgrösse umgekehrt proportional zur Datenrate.
- (2) Baudrate: Höhere Datenrate = Höhere Baudrate / Bandbreite
Dämpfung nimmt zu
- (3) Heterogene Datenraten: Möglichst keine Konfiguration systemrelevanter Parameter beibehalten

Lösung : 100BASE-TX

100BASE-TX:

CSMA/CD

- CSMA/CD ist unterstützt
- Vollduplex
 - Optisch (100BASE-FX)

Segmentlänge 200 m (einschließlich 2 Hubs)
100 m Kabellänge
MM Faser 2000 m, SM bis 40 km

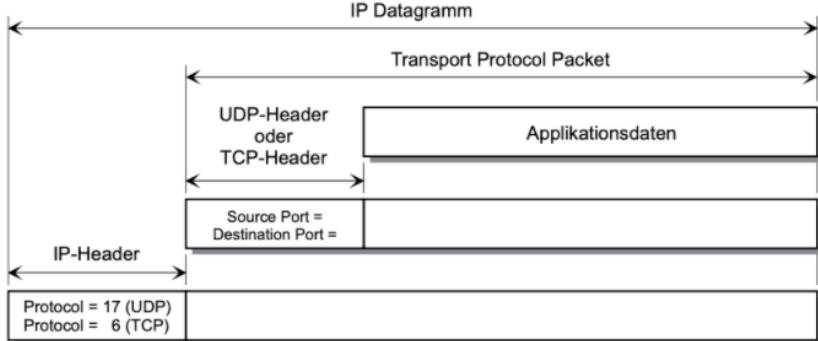
Baudrate / Bandbreite

- CAT3 Kabel nicht mehr unterstützt (16 MHz Bandbreite ungünstig für 125 MBaud)
- MLT-3 und 4B5B Codierung reduziert höherfrequente Anteile und erlaubt Verwendung von CAT5

Kompatibilität und Unterstützung von Systemen mit heterogenen Datenraten

- Einführung Autonegotiation mithilfe von Fast Link Pulsen
- Definition geschwindigkeitsunabhängiger Schnittstellen (MII - Media Independent Interface)
- Sonst alles gleich

8 Transport Layer



UDP dient dem <i>Multi- und Demultiplexen</i> der Datagramme zu den Applikationen.		TCP-Header																															
<ul style="list-style-type: none"> • Verbindungslos • Unzuverlässig 		<table border="1"> <tr> <td>1. Byte</td><td>2. Byte</td><td>3. Byte</td><td>4. Byte</td></tr> <tr> <td>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</td><td>UDP Source Port</td><td>UDP Destination Port</td><td></td></tr> <tr> <td>UDP Message Length</td><td>Checksum</td><td></td><td></td></tr> <tr> <td colspan="4">Data</td></tr> </table>		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	UDP Source Port	UDP Destination Port		UDP Message Length	Checksum			Data																	
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	UDP Source Port	UDP Destination Port																															
UDP Message Length	Checksum																																
Data																																	
Message-Length (in Byte) Header + Daten = min. 8 B		Min length = 20 Byte / Max Length = 60 Byte																															
System Ports (Well-Known) User Ports (Registered) Dynamic / Private Ports		<ul style="list-style-type: none"> • Sequence-Nr. Nummer zur Ordnung der Segmente • Acknowledgement-Nr. $n+1 \rightarrow$ Daten korrekt und vollständig • Data Offset Gibt an wo Daten beginnen / enden • ECN-Flags Explicit Congestion Notification • Control Bits URG, ACK, PSH, RST, SYN, FIN • Window Verfügbare Puffergrösse • Urgent Pointer URG = 1 \rightarrow Position der wichtigen Daten • Options Häufigste Verwendung: MSS 																															
Frei verfügbare Ports <table border="1"> <tr> <td>System Ports</td><td>User Ports</td><td>Dynamic Ports</td></tr> <tr> <td>0 - 1023</td><td>1024 - 49'151</td><td>49'152 - 65'535</td></tr> </table>		System Ports	User Ports	Dynamic Ports	0 - 1023	1024 - 49'151	49'152 - 65'535	<table border="1"> <tr> <td>1. Byte</td><td>2. Byte</td><td>3. Byte</td><td>4. Byte</td></tr> <tr> <td>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</td><td>TCP Source Port</td><td>TCP Destination Port</td><td></td></tr> <tr> <td>Sequence Number</td><td>Acknowledgement Number</td><td></td><td></td></tr> <tr> <td>Header Length</td><td>unused</td><td>ECN</td><td>Control Bits</td></tr> <tr> <td>Checksum</td><td>Urgent Pointer</td><td></td><td></td></tr> <tr> <td colspan="4">Options / Padding</td></tr> </table>		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	TCP Source Port	TCP Destination Port		Sequence Number	Acknowledgement Number			Header Length	unused	ECN	Control Bits	Checksum	Urgent Pointer			Options / Padding			
System Ports	User Ports	Dynamic Ports																															
0 - 1023	1024 - 49'151	49'152 - 65'535																															
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	TCP Source Port	TCP Destination Port																															
Sequence Number	Acknowledgement Number																																
Header Length	unused	ECN	Control Bits																														
Checksum	Urgent Pointer																																
Options / Padding																																	
Verbindungsaufbau		Datenaustausch																															
Verbindungsabbau		Sicherstellung der Zuverlässigkeit <ul style="list-style-type: none"> (1) Retransmission: Empfänger schickt Acknowledgement an Sender, falls erfolg. Falls Sender nach Ablauf des Timers kein Ack hat, sendet er nochmals. (2) Adaptive Waitzeit: Wartezeit vor dem Neusenden wird mit Roundtrip Time berechnet (RTT). Wartezeit bis Neuübertragung \rightarrow Retransmission Time out (RTO). 																															

8.1 TCP

Zuverlässig & verbindungsorientiert \rightarrow sichert Reihenfolge & Schutz vor Datenverlust

Wichtige Merkmale:

- Verbindungsorientierte Übertragung: Verbindung muss aufgebaut werden
- Hohe Zuverlässigkeit: Schutz vor Datenverlust, Reihenfolge bleibt
- Vollduplex Übertragung: Gleichzeitige Übertragung in beide Richtungen
- Stream Schnittstelle: Anwendung sender/empfängt unstrukturierte Bytefolge
- Eleganter Verbindungsabbau: Gewährt Zustellung aller Daten auch beim Verbindungsabbau.

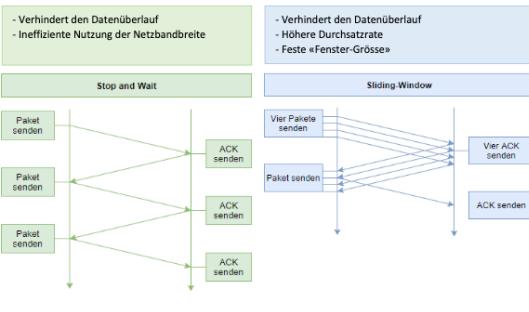
Sicherstellung der Zuverlässigkeit

(1) Retransmission: Empfänger schickt Acknowledgement an Sender, falls erfolg. Falls Sender nach Ablauf des Timers kein Ack hat, sendet er nochmals.

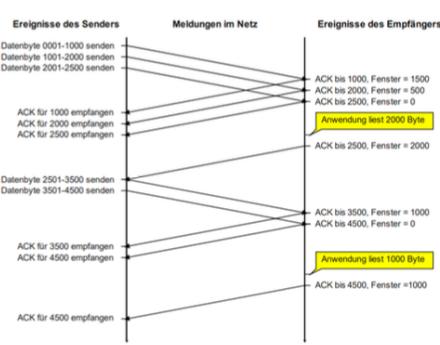
(2) Adaptive Waitzeit: Wartezeit vor dem Neusenden wird mit Roundtrip Time berechnet (RTT). Wartezeit bis Neuübertragung \rightarrow Retransmission Time out (RTO).

Überlast des Empfängers: Fluss-Steuerung

TCP verwendet den *Sliding-Window Mechanismus*. Beide Seiten einen Buffer (Window).



Fluss-Steuerung bei TCP



bei Ankunft eines Segments gibt

der Empfänger in der Bestätigung

das restliche Window an

→ Window Advertisement

Überlast des Netzes: Congestion Control

TCP benutzt den Paketverlust als Masseneinheit für Überlastung und reagiert durch Absenken der Übertragungsrate (*Slow Start*). Dadurch kann die Überlastung überwacht und verhindert werden.

Hierfür pflegt jeder Sender zwei Fenster (vom Sender gewährtes Fenster, Überlastungsfenster). Das Minimum der Fenster stellt die Anzahl Bytes dar, die gesendet werden können.

Erkennung von verlorengegangenen Telegrammen (Round Trip Time)

Um Fehler Paketverluste und andere Fehler zu verhindern, werden Pakete nach einer bestimmten Zeit erneut übertragen, wenn keine Bestätigung gesendet wurde. Um diese Zeit zu optimieren, misst TCP bei jeder aktiven Verbindung die *Round-Trip Time (RTT)*.

Gewichteter Mittelwert *SRTT* (*Smoothed Round-Trip Time*)

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

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

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

9 Application Layer

Domain Name Space (DNS)

- Leserliche Darstellung von IP-Adressen
- Hauptdomäne = Root

Beispiel

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

```

graph TD
    Root[.] --- eng[eng]
    Root --- mkt[mkt]
    Root --- sales[sales]
    Root --- hr[hr]
    eng --- hw[hw]
    eng --- sw[sw]
    sw --- bob[bob]
    sw --- carol[carol]
    sw --- ted[ted]
  
```

Name-Server

```

graph TD
    Anwendung[Anwendung] --> Resolver[Resolver]
    Resolver -- Anfrage --> NameServer[Name-Server]
    NameServer -- Antwort --> Anwendung
    NameServer -- "Anfrage nach 'eng.'" --> RootServer[Root-Server]
    RootServer -- "DNS-Server von 'eng.' ist ..." --> engServer[DNS-Server der Domain "eng."]
    engServer -- "Anfrage nach 'sw.eng.'" --> engSubServer[DNS-Server der Domain "sw.eng."]
    engSubServer -- "IP-Adresse von 'bob.sw.eng.' ist ..." --> bobServer[DNS-Server der Domain "sw.eng."]
  
```

Trivial File Transfer Protocol (TFTP)

- Basiert auf UDP

TFTP	Datensec
UDP-Header	Datasec
Port = 69	UDP-Datasec
IP-Datasec	
Protocol = 17	IP-Datasec

Hypertext Transfer Protocol (HTTP)

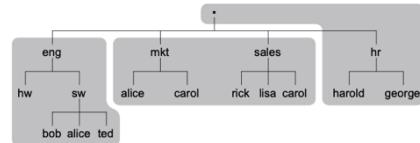
- WWW basiert auf HTTP

Funktionsweise von HTTP

- Basiert auf TCP, Port 80
- ASCII-Basiert, MIME-Typen, Codierungen
- Transaktionsbasiert: HTTP Request → HTTP Response

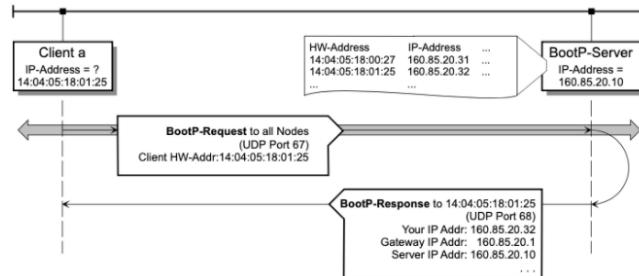
9.1 Name-Server

- verantwortlich für meistens 1 Zone
- Mehrere Name-Server pro Zone = Redundanz
- ➔ Jede Zone muss von einem Master-Name-Server bedient werden



9.2 BootP

- ➔ Wie erhält ein Knoten seine IP-Adresse?



baut auf UDP auf:

-> UDP Port 67: Kommunikation mit BootP-Server

-> UDP Port 68: Kommunikation mit dem Client

-> Server kann auch in anderem IP-Subnetz sein (UDP)

BOOTP			
<ul style="list-style-type: none"> • Manuelle Verwaltung • Heimanwender sind überfordert • Statische Adresszuordnung 			
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	IP-Address ...
Operation	Hardware Type	Hardware Length	Hop Count
Transaction Identification			
Seconds			
Unused			
Client IP Address			
Your (Client) IP Address			

Simple Mail Transfer Protocol (SMTP)

Standard-Protokoll zum Versenden oder Weiterleiten von E-Mails. Es können nur ASCII-Zeichen versendet werden. Für weitere Zeichen wird MIME verwendet.

MIME-Standard (Multipurpose Internet Mail Extension)

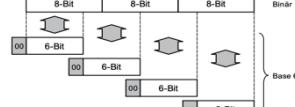
Ermöglicht eine Codierung zu wählen, um auch nicht-ASCII-Zeichen zu versenden.

- Maximale Zeilenlänge = 76 Zeichen
- «B»-Encoding (Base64)
- Beispiel: Züri → WvxyaQ==
- echo «Text» / base64

Base 64 Encoding

resultierende Werte liegen zwischen 0..63

Gruppen von 3 Bytes → 4 Gruppen mit je 6 Bits (RFC 2045)



Dynamic Host Configuration Protocol (DHCP)

- Paketformat identisch zu BOOTP
- Dynamische Zuweisung von IP-Adressen
- Reserviert nur IP's von aktiven Geräten

Ablauf (DHCP)

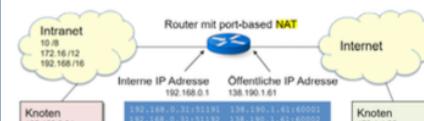
1. Client sucht DHCP Server mittels Broadcast
2. DHCP Server antwortet (DHCP offer)
3. Der Client wählt einen Server und fordert eine Auswahl der angebotenen Parameter (DHCP request)
4. Der Server bestätigt mit einer Message, welche die endgültigen Parameter enthält
5. Vor Ablauf der Lease-Time erneutert der Client die Adresse.

Network Address Translation (NAT)

- NAT (Historisch)
- NAPT (Port Trans.)

Sicherheit durch «Verstecken» von lokalen Adressen
Lokale IP-Adresse → Öffentliche IP-Adresse

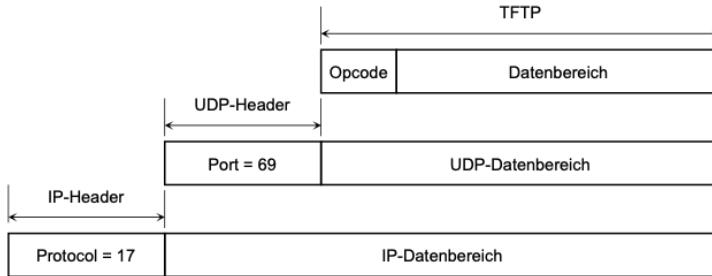
NAT verzerrt das Konzept der OSI-Layer, da eine Network-Funktion auf den Transport-Header zugreift. IP-Adresse und Portnummer werden dabei verändert.



Intranet (privates Netz)		Internet (öffentliche Netz)	
Quell-Adresse	Port	Ziel-Adresse	Port
192.168.0.31	51991	170.1.1.25	80
192.168.0.31	51992	170.1.1.25	443
192.168.0.32	51991	170.1.1.25	25
		→ 138.190.1.61 60001	170.1.1.25 80
		→ 138.190.1.61 60002	170.1.1.25 443
		→ 138.190.1.61 60003	170.1.1.25 25

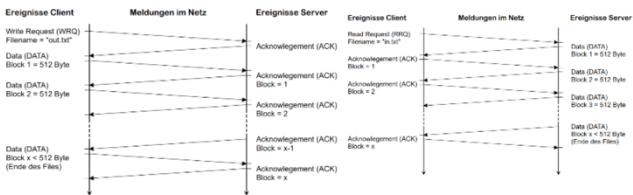
9.3 TFTP

- Protokoll zur Datenübertragung
- Verwendet UDP

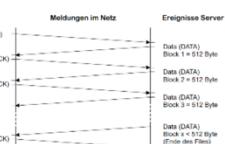


- **Read Request (RRQ):** Anfordern einer Datei vom anderen Host, es wird eine TFTP-„Verbindung“ aufgebaut
- **Write Request (WRQ):** Senden einer Datei zum anderen Host, es wird eine TFTP-„Verbindung“ aufgebaut
- **Acknowledgement (ACK):** Bestätigung eines korrekt empfangenen WRQ oder DATA Pakets
- **Data (DATA):** Übermittlung der eigentlichen Daten, immer in Blöcken von 512 Bytes, ein kürzerer Datenblock beendet die Übertragung, Blöcke sind fortlaufend nummeriert
- **Error (ERROR):** Ein Fehler ist aufgetreten (siehe Error Code), TFTP-Verbindung wird beendet

Empfangen



Senden



9.4 SMTP (TCP)

Aufbau der Verbindung

- gesicherte Verbindung über TCP Port 25
 - Der Sender öffnet eine TCP-Verbindung zum Empfänger.
 - Der Empfänger identifiziert sich gegenüber dem Sender.
 - Der Sender identifiziert sich gegenüber dem Empfänger.
 - Der Empfänger akzeptiert die Identifikation des Senders.

Abbau der Verbindung

Der Verbindungsabau durch den SMTP-Sender erfolgt in zwei Schritten: Nach Übertragung des QUIT-Kommandos wird auf eine Antwort (Reply) des Empfängers gewartet. Anschließend wird ein TCP-CLOSE für die Verbindung initiiert. Unmittelbar nach Empfang des QUIT-Kommandos baut der Empfänger die TCP-Verbindung ab.

Beispiel:

```
Sender: Quit
Empfänger: Bye-Bye
Empfänger: <TCP-Close>
Sender: <TCP-Close>
```

9.5 Mime-Standard

Quoted Printable Encoding

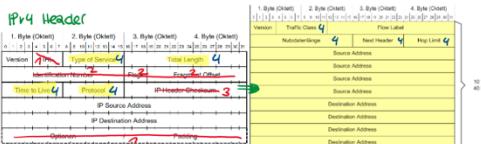
Jeder 8 Bit Wert wird durch 3 ASCII Zeichen ersetzt. (G → =FC)

Da nur 7 Bit ASCII erlaubt, werden Zeichen im Bereich 128-255 umcodiert

BASE64 Encoding

Für rein binäre Daten besser geeignet. 3 Byte werden 4 Blöcke à 6 Bit aufgelebt. Somit werden binäre Werte in ASCII umgewandelt

10 IPv6



(1) Fixe Header Länge:
HHL / Optionen / Padding weglassen und durch Blanks ersetzen

(2) Felder für Fragmentierung entfernt

(3) Header checksum entfernt

(4) Felder umdefinieren/ umbenennen

(5) Neues Feld Flow Label und Adressen von 4 auf 16 Byte

- Version (4 Bits): Das Feld hat den Wert 6 (binär 0110).
- Traffic Class (8 Bits): (RFC 2460) Das Feld dient der Unterscheidung verschiedener Verkehrsklassen oder Prioritäten der IPv6-Pakete. Der Wert kann entweder vom sendenden Endgerät oder von einem Router gesetzt werden. Der 'default value' ist 00000000.
- Flow Label (20 Bits): Damit wird ein Kommunikations-Paar (Sender und Empfänger) identifiziert. Der 'Flow' identifiziert eine Verbindung.
- Nutzdatenlänge (16 Bits): Länge der Nutzdaten ohne Header. Falls keine Optionen definiert sind, beträgt die maximale Länge 65535 Bytes. Anmerkung: Über eine 'Jumbo Payload Option' sind bis zu 4GBYTE lange Datagramme möglich.
- Hop Limit (8 Bits): Entspricht TTL von IPv4, wie es effektiv genutzt wird. Jeder Router, der passiert wird, dekrementiert den Wert. Falls der Wert Null erreicht ist, wird das Paket gelöscht.

Extension Header

Nach dem Header können mehrere Extension Header hinzugefügt werden.

- Vorteile:
 - o Nur da bei Bedarf
 - o Fixe Größe ⇒ einfache Verarbeitung
 - o Im Router weniger Felder zu verarbeiten
 - o Vieles ist im Ziel übersetzt
 - o Forwarding schneller

Quality of Service mit Flow Label

Falls Spezialbehandlung notwendig, ist im Flow Label eine Zahl im Bereich

00000 - FFFFF. Default ist 00000

Es können mehrere Flows existieren.
Fälle eines Flows haben identische Quell- und Zielausadresse

(10.1) Adressierung bei IPv6

Darstellung der 128 Bit langen IPv6 Adresse:

- Folge von Doppel-Bytes als 1- bis 4-stellige Hex-Zahl

• Jeweils 2 Bytes werden durch einen Doppelpunkt getrennt

Verkürzte Notation:

- In Zahlen können links stehenden Nullen weggelassen werden:

2001:0620:0004:0A00:20FF:FE9C:7E4A und

2001:620:0:4:A00:20FF:FE9C:7E4A sind gleichwertig

- Nullfolgen können durch 2 Doppelpunkte dargestellt werden

1023:0000:0000:0000:1736:a673:88a0:a620 und

1023:1736:a673:88a0:a620 sind gleichwertig

↓ Darf nur einmal verwendet werden, weil sonst unklar ist wo die vielen Nullbytes enthalten sind.