1 - OSI-Modell

Ein **Dienst** sendet und empfängt bestätigte und unbestätigte Daten.

Klassifizierung von Diensten

- Verbindungsorientiert oder verbindungslos
- Zuverlässig oder unzuverlässig

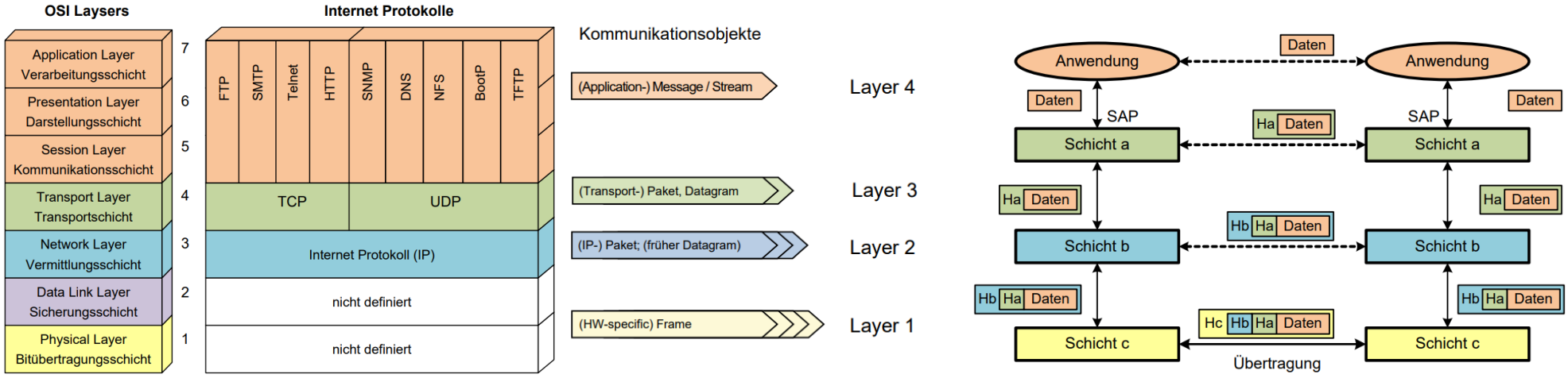
Verbindungsorientiert	**Verbindungslos**
Verbindungs-Aufbau nötig	Jederzeit Nachrichten schicken
Ziel muss bereit sein	Ziel muss nicht «bereit» sein

Zuverlässig	**Unzuverlässig**
Kein Datenverlust	Möglicher Datenverlust
Sicherung durch Fehler-Erkennung -/ Korrektur	Keine Sicherung
Text-Nachrichten	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.



Pascal Isliker

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.

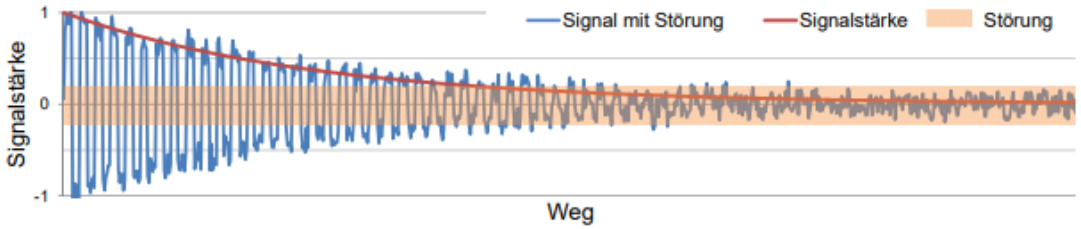
$$C_{Medium} = 200'000\frac{km}{s} \approx \frac{2}{3}c_0$$

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.

$$dB = 10 \cdot \log\left(\frac{P_1}{P_2}\right), dB = 10 \cdot \log\left(\frac{U_1}{U_2}\right)^2$$

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

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

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

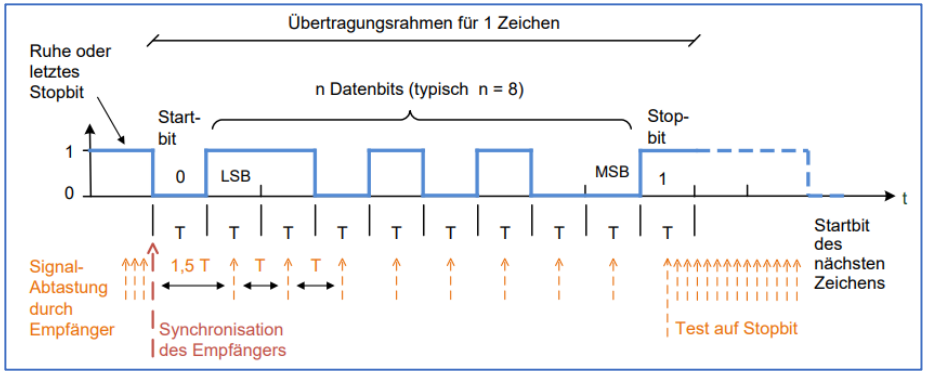
Pascal Isliker

3 - Physical Layer (Bitübertragungsschicht)

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



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.

Arten der Kommunikation (*Verkehrsbeziehung*)

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

Arten der Verbindungen (*Kopplung*)

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

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)

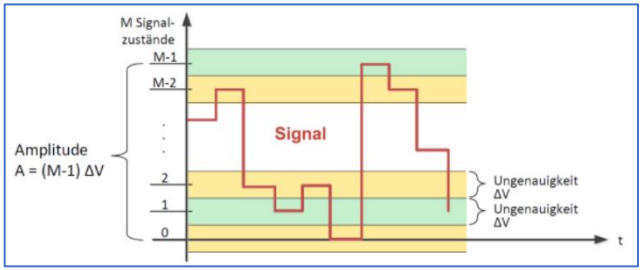
Maximal erreichbare Bitrate

Maximal Bitrate $R\ [bit/s]$

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

Unterscheidbare Signalzustände

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

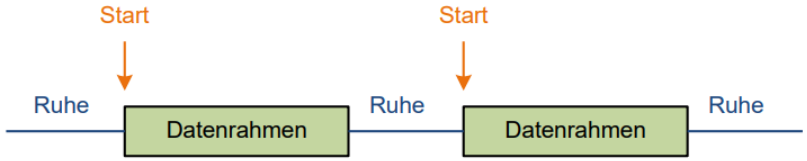


Pascal Isliker

4 - Data Link Layer (Sicherungsschicht)

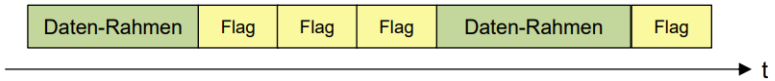
Framing (Asynchron)

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

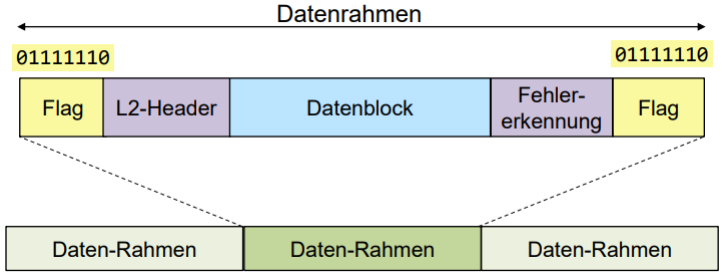


Framing (Synchron)

- Frames werden ohne Unterbruch gesendet



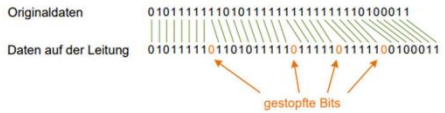
- Frames werden durch ein Start- und ein End-Flag begrenzt



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** (**F**rame **E**rror **R**atio)
- **RER** (**R**esidual **E**rror **R**atio)
- **BER** (**B**it **E**rror **R**atio)

Wahl der Framelänge

- Lange Frames — Höhere Nutzdatenrate, Fehleranfällig
- Kurze Frames — Tiefere Nutzdatenrate, Zuverlässig

Datenraten

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

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

Zugriffsmechanismen (Media Access Control = MAC)

- Master-Slave Verfahren
- Token-Verfahren
- Zeitsteuerung
- Carrier Sense Multiple Access / CD (Collision Detection), CR (Collision Resolution)

Kollisionsbehandlung

Pascal Isliker

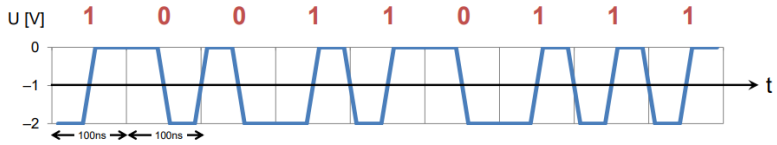
5 – Local Area Networks

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)



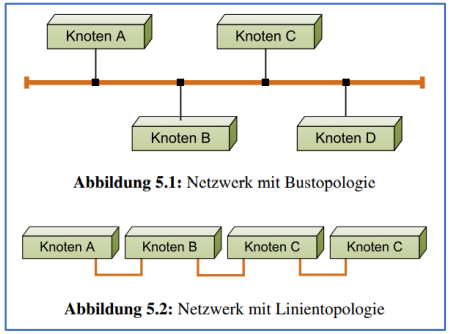


Abbildung 5.1: Netzwerk mit Bustopologie

Abbildung 5.2: Netzwerk mit Linientopologie

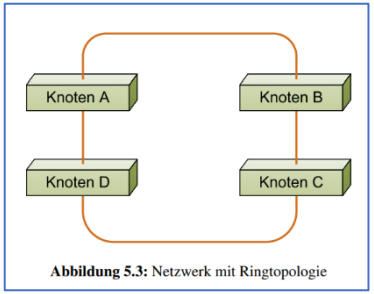


Abbildung 5.3: Netzwerk mit Ringtopologie

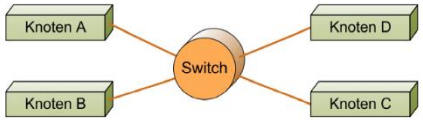


Abbildung 5.5: Netzwerk mit Sterntopologie

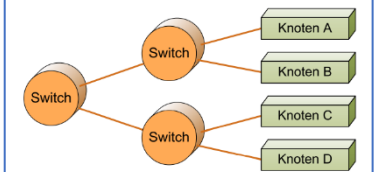


Abbildung 5.6: Netzwerk mit Baumtopologie

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

Bedingung für Kollisionserkennung

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

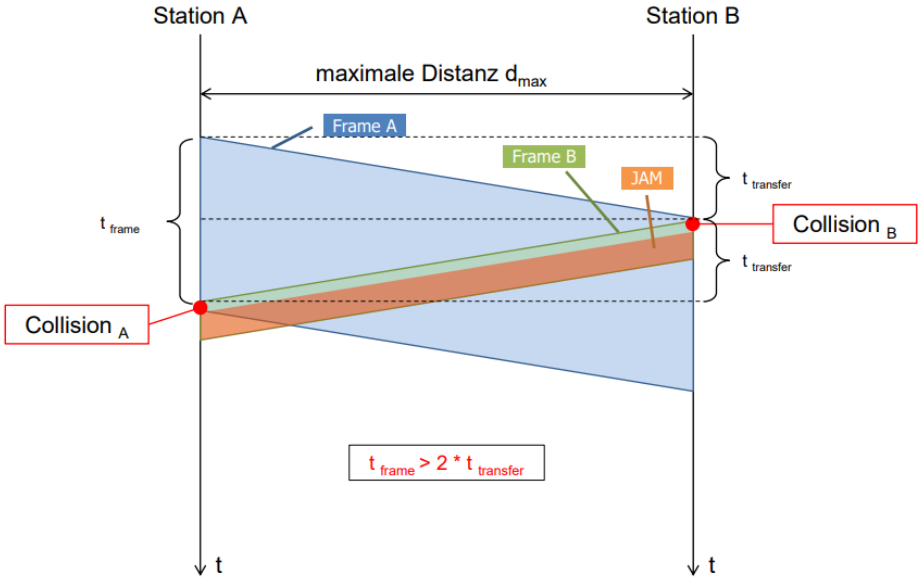
Maximale Ausdehnung eines Segments

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

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

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

Bedingung für Kollisionserkennung



Pascal Isliker

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)

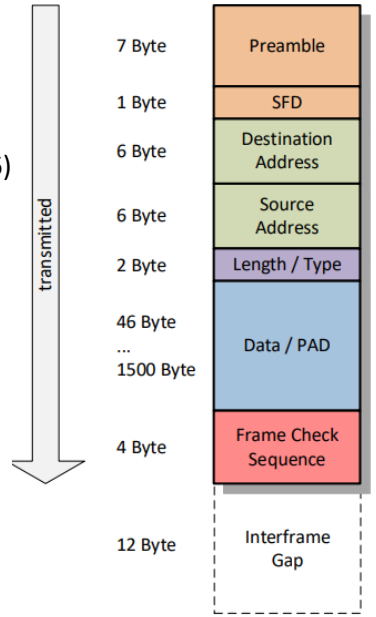
- Enthält die eigentlichen Datenbytes
- Bei weniger als 46 Bytes wird mit PAD Bytes abgefüllt

Frame **C**heck **S**equence, FCS (4 Bytes)

- IEEE CRC-32 Algorithmus

Inter**f**rame **G**ap, IFG (12 Bytes)

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



IEEE MAC Adressen

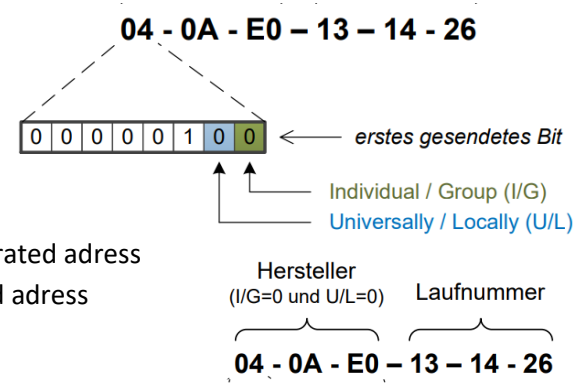
Die ersten beiden Bits des ersten Adress-Bytes haben eine spezielle Bedeutung:

Individual / Group Bit

- 0 = individual address
- 1 = group address

Universally / Locally Bit

- 0 = universally administrated adress
- 1 = locally administrated adress



Repeater and Collision Domain

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

Erkennen von Kollisionen

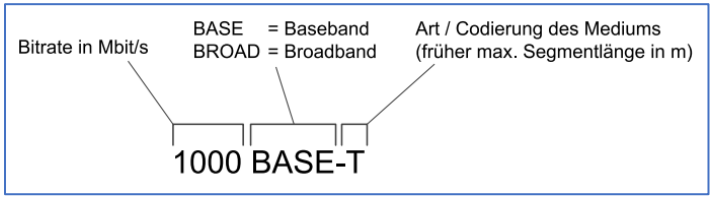
- Halbduplex Collision Detection Unit
- Vollduplex Keine Kollisionen

Shared Medium Ethernet

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

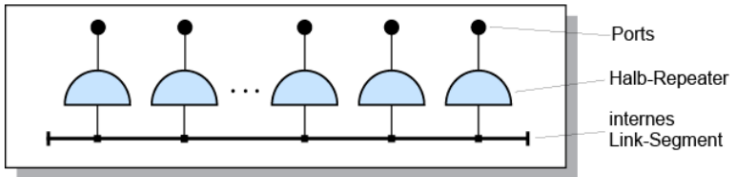
Normen für CSMA/CD

- 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.



Pascal Isliker

6 – Switched LAN and Ethernet-Technologien

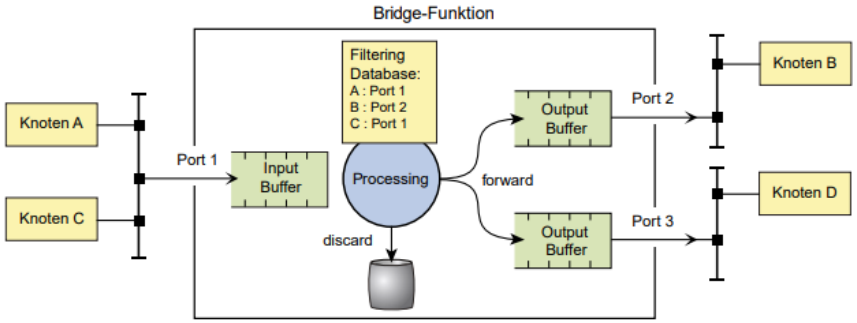
Bridges

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

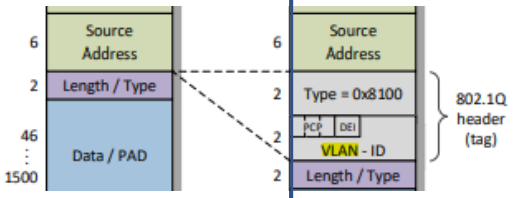
Eine **Collision Domain** *(CD)* besteht aus mit Repeatern zusammengeschlossenen Segmenten.

- 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

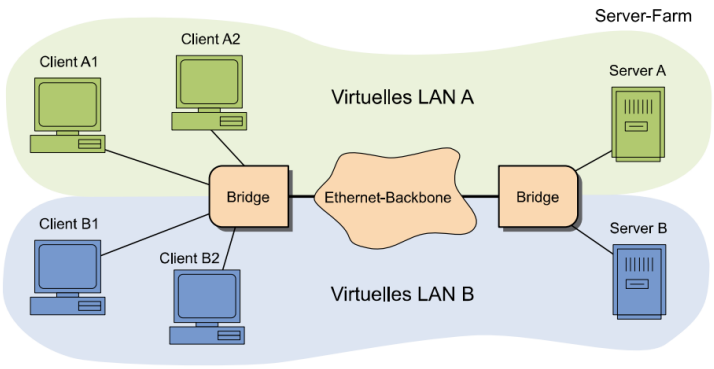
Mithilfe von virtuellen LAN kann ein grosses Netz in unabhängige logische Netze aufgeteilt werden. Jedes Switch-Port kann einem beliebigen VLAN zugeordnet werden.



VLAN-Tag

- VLAN-ID im VLAN-Tag wird zur Zuordnung verwendet
- **P**riority **C**ode **P**oint ermöglicht die Priorisierung gewisser Applikationen
- **D**iscard **E**ligibility **I**ndicator 0 → Frame wird bei Engpässen zuerst verworfen

Trunk = Tagged, Access = Untagged



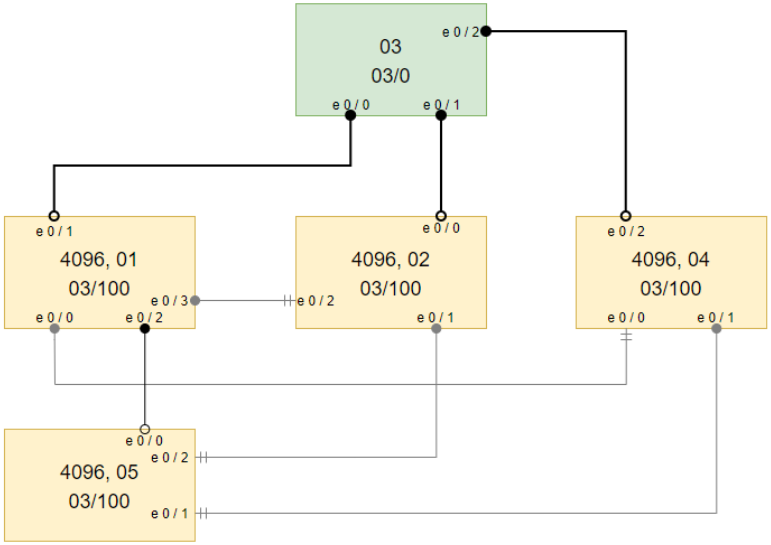
Pascal Isliker

Spanning Tree (Redundanz-Protokoll)

Beim Spanning-Tree werden von redundanten Pfaden alle ausser einer gesperrt. Im Fehlerfall wird falls möglich ein ausgefallener Port ersetzt.

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-Identfier* (Priorität, MAC-Adresse)
2. Direkt angeschlossene Bridges bestätigen (verbinden)
3. Weitere Verbindungen abhängig von *Kosten* und *Bridge-Identifier* 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	10GBBASE-T
Kabelkategorie	CAT3 - 16 MHz CAT5 - 100 MHz	CAT5 - 100 MHz CAT6 - 250 MHz	CAT5 - 100 MHz CAT6 - 250 MHz	CAT6A - 500 MHz CAT7 - 600 MHz CAT7A – 1000 MHz
Line Coding	Manchester 2 Aderpaare simplex	MLT-3, 4B5B 2 Aderpaare simplex	PAM-5, 8B/10B 4 Aderpaare duplex	PAM-16, 64B/65B, FEC 4 Aderpaare duplex
Baudrate	10 MBaud	125 MBaud	4 x 125 MBaud	4 x 800 MBaud
Link Pulses	NLP	FLP	FLP	FLP

Merkmale von Bridges

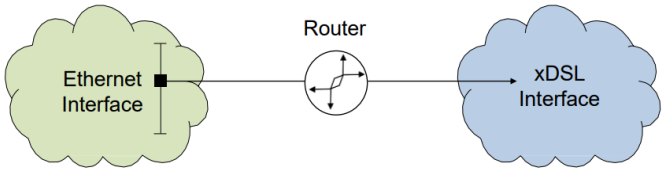
Anzahl Ports	Steckergrösse ist im Extremfall die Limitierung
Adresstabelle	Wie viele Stationen können im LAN existieren
Filterrate	Maximale Frames / s / Port (Empfangsrichtung)
Transferrate	Maximale Frames / s / Port (Senderichtung)
Backplane / Fabric Kapazität	Maximaler Gesamtdurchsatz zwischen allen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

Pascal Isliker

7 – Internet / Network Layer

Router sind Komponenten, die es erlauben Subnetze miteinander zu verbinden. Router haben eine ähnliche Funktion wie Bridges, allerdings arbeiten sie auf dem Network Layer.

- Router empfangen nur Pakete, die direkt an sie adressiert sind.
- Die Weiterleitung erfolgt anhand der Network Layer Adresse.
- Benutzen immer den optimalen Pfad.



Forwarding (Weiterleiten der Daten)

- Aufgrund von Routingtabellen

Routing (Aufbau der Routingtabellen)

- Statische Konfiguration oder Dynamisch durch Routing-Protokolle

Routing-Tabelle

- Sortiert nach der Länge der Netzmaske
- Von oben nach unten durchsucht
- Verglichen werden die Netzadressen

Flaches Routing

- Router kennt explizite Wege zu jedem Zielnetz
- Redundanz möglich durch Speichern mehrerer Wege ins gleiche Netz
- Grosse Routing-Tabellen

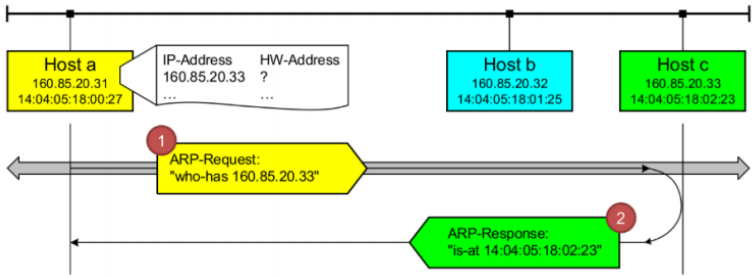
Hierarchisches Routing (Default)

- Router kennt die direkt angeschlossenen Netze
- Einsatz am «Rand» von Netzen
- Kleine Routing-Tabellen (mit Default-Eintrag)

Kapselung und Adressauflösung

ARP (**A**ddress **R**esolution **P**rotocol)

- Ermittelt HW-Adresse (MAC) zu einer IP-Adresse



Internet **C**ontrol **M**essage **P**rotocol (ICMP)

- Übertragungen von Fehlermeldungen oder Informationsaustausch

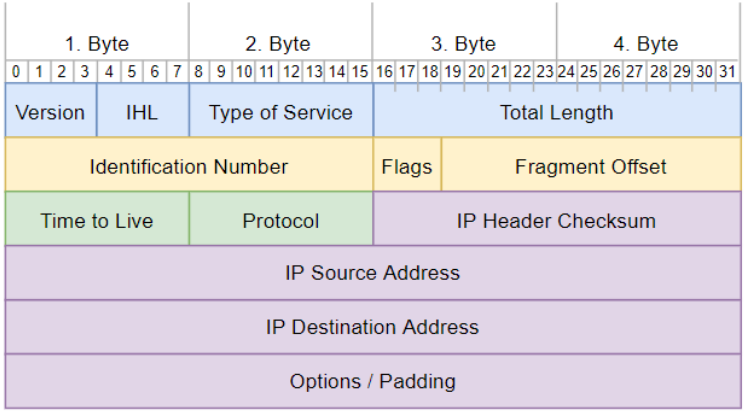
Grundsätze des Internets

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

Internet Protokoll Format (IP-Header)

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

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



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

Das unterliegende Netz limitiert die Grösse eines Pakets (**M**aximum **T**ransfer **U**nit). Der Sender kennt die MTU der Netze nicht.

Fragmentierung

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

Reassembly

1. Zusammensetzen beim Zielhost
2. Letztes Fragment: MF = 0

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

Internet-Adressierung (IPv4)

- Netzadresse — Tiefste Adresse im Subnetz — Interface-Adresse *AND* Subnetzmaske
- Broadcast — Höchste Adresse im Subnetz — Interface-Adresse *OR* Invertierte Subnetzmaske

Beispiel

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

					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	
Subnetzmaske	255	255	240	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
Subnetz	160	85	16	0 / 20	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	AND
Netzadresse	160	85	16	0	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
					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	
Subnetzmaske (invertiert)	255	255	240	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	
Subnetz	160	85	16	0 / 20	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	OR
Broadcast	160	85	31	255	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	

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

Private Adressbereiche (werden im Internet nicht weitergeleitet):

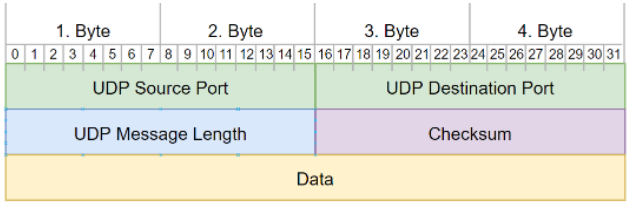
Klasse	Netzadresse(n)	Anzahl Netze	Subnetzmaske
A	10.0.0.0	1	255.0.0.0
B	172.16.0.0 – 172.31.0.0	16	255.255.0.0
C	192.168.0.0 – 192.168.255.0	256	255.255.255.0

Pascal Isliker

8 – Transport Layer

UDP dient dem *Multi-* und *Demultiplexen* der Datagramme zu den Applikationen.

- Verbindungslos
- Unzuverlässig



System Ports (*Well-Known*)
User Ports (*Registered*)
Dynamic / Private Ports

Feste Port-Nummern, für bekannte Appl. reserviert
Reservierter Bereich für herstellerspezifische Appl.
Frei verfügbare Ports

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

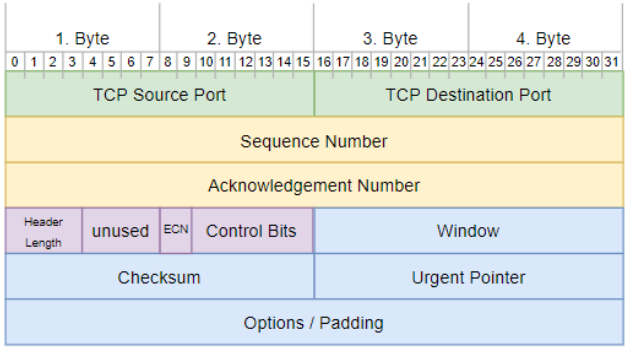
- LISTEN — Auf Anforderung warten
- SYN-SENT — Anforderung geschickt
- SYN-RECEIVED — Anforderung erhalten
- ESTABLISHED — Verbindung besteht

- SYN — Verbindungsaufbau
- ACK — Paket bestätigen
- FIN — Verbindungsabbau

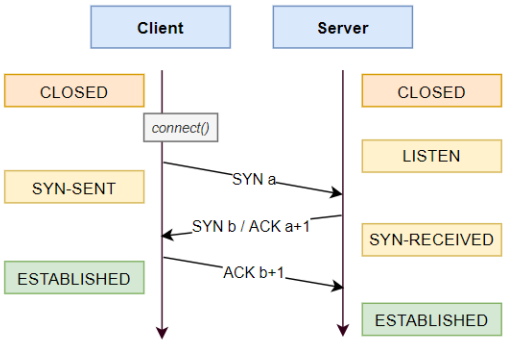
- FIN-WAIT-1 — Abbauanforderung geschickt
- FIN-WAIT-2 — Abbauanforderung bestätigt
- CLOSE-WAIT — Auf Lokale Verbindung warten
- LAST-ACK — Verbindungsabbau bestätigt
- TIME-WAIT — Letzte Bestätigung gesendet

TCP-Header

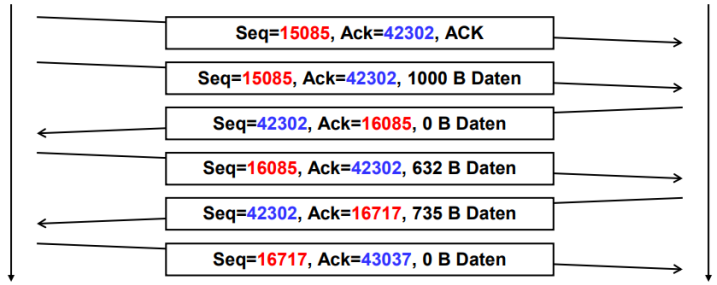
- Sequence-Nr. — Nummer zur Ordnung der Segmente
- Acknowledgement-Nr. — n + 1 → Daten korrekt und vollständig
- Data Offset — Gibt an wo Daten beginnen / enden
- ECN-Flags — Explicit Congestion Notification
- Control Bits — URG, ACK, PSH, RST, SYN, FIN
- Window — Verfügbare Puffergrösse
- Urgent Pointer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



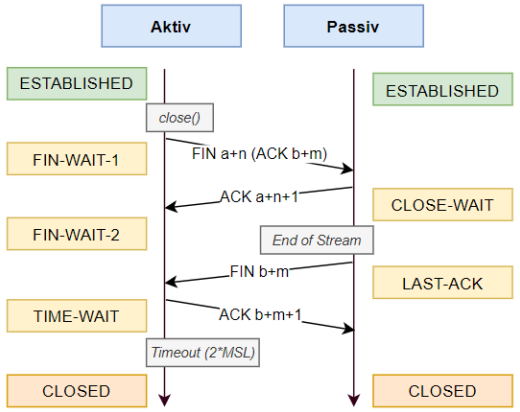
Verbindungsaufbau



Datenaustausch



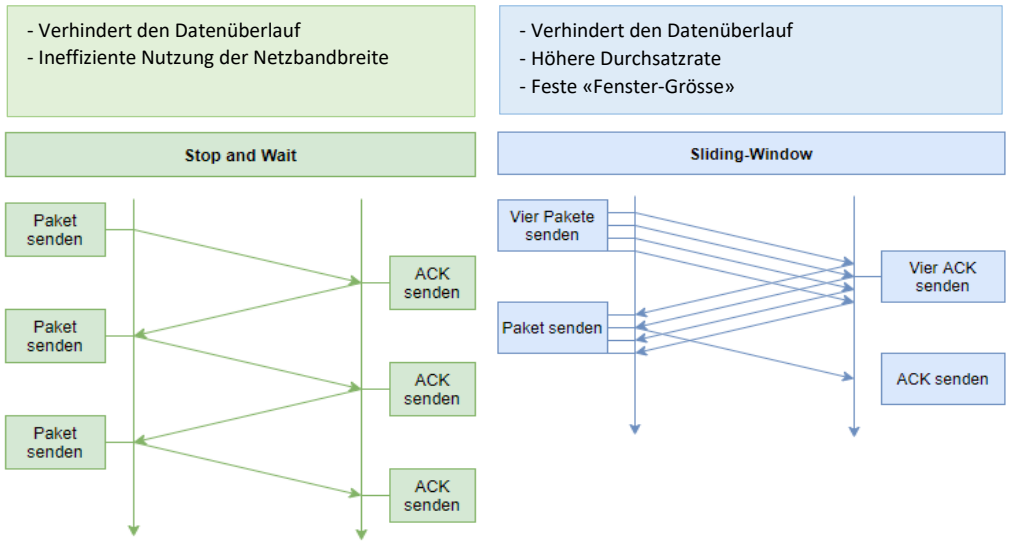
Verbindungsabbau



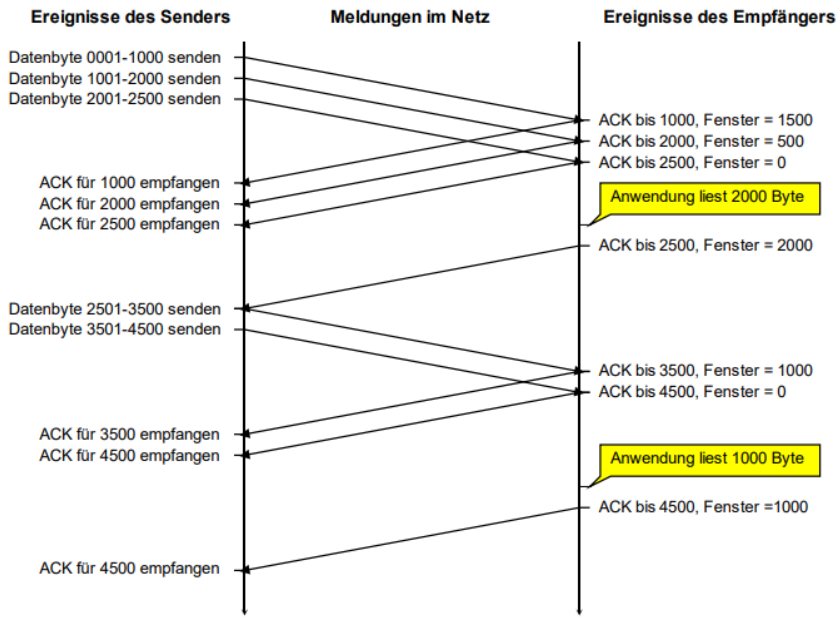
Pascal Isliker

Überlast des Empfängers: Fluss-Steuerung

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



Fluss-Steuerung bei TCP



Überlast des Netzes: Congestion Control

TCP benutzt den Paketverlust als Masseinheit 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)*.

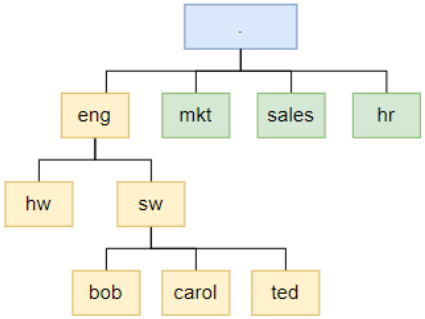
Gewichteter Mittelwert *SRTT (**S**moothed **R**ound-**T**rip **T**ime)*	$\alpha = 0.125$: $SRTT_n = (1-\alpha) \cdot SRTT_{n-1} + \alpha \cdot RTT_n$
Streuung RTTVAR des *SRTT* der Abweichungen	$\beta = 0.25$: $RTTVAR_n = (1-\beta) \cdot RTTVAR_{n-1} + \beta \cdot \lvert SRTT_n - RTT_n \rvert$
Retransmission Time-Out RTO	$RTO_n = SRTT_n + 4 \cdot RTTVAR_n$

Pascal Isliker

9 – Application Layer

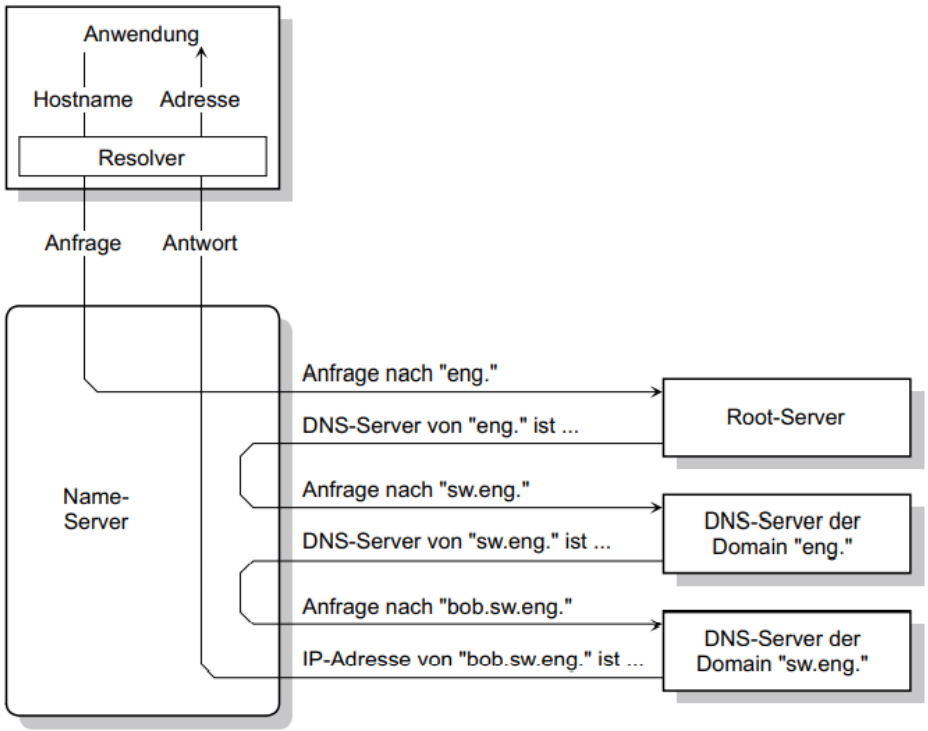
Domain **N**ame **S**pace **(DNS)**

- Leserliche Darstellung von IP-Adressen
- Hauptdomäne = Root



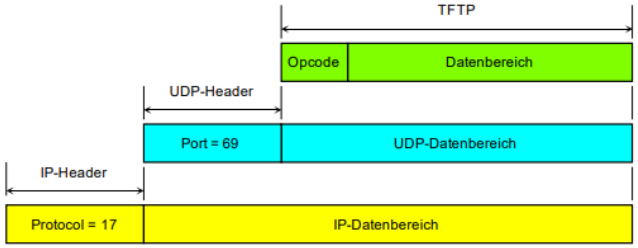
<u>Beispiel</u>

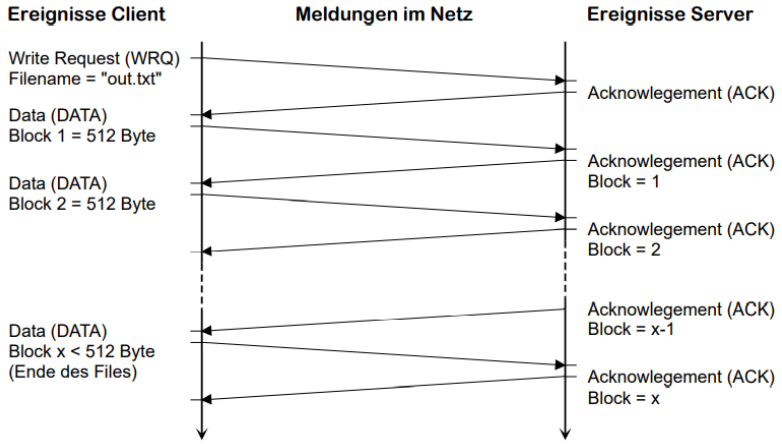
- *bob.sw.eng.* Fully Qualified Domain Name
- *.* Root
- *eng* **T**op **L**evel **D**omain
- *sw* **S**econd **L**evel **D**omain



Trivial **F**ile **T**ransfer **P**rotocol **(TFTP)**

- Basiert auf UDP





Hypertext **T**ransfer **P**rotocol **(HTTP)**

- WWW basiert auf HTTP

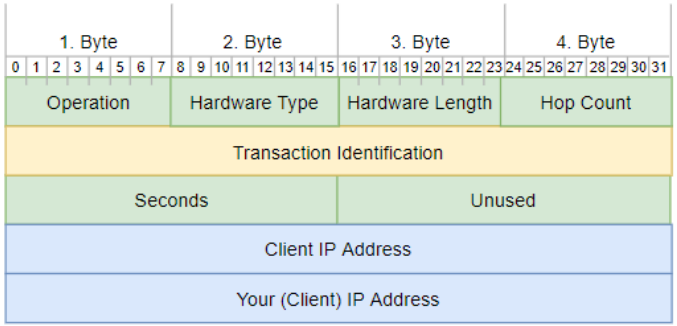
Funktionsweise von HTTP

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

Pascal Isliker

BOOTP

- Manuelle Verwaltung
- Heimanwender sind überfordert
- Statische Adresszuordnung



Dynamic **H**ost **C**onfiguration **P**rotocol **(DHCP)**

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

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 erneuert der Client die Adresse.

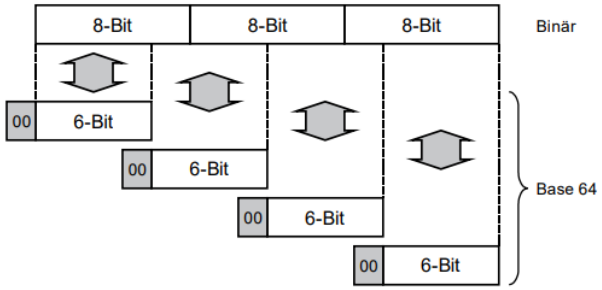
Simple **M**ail **T**ransfer **P**rotocol **(SMTP)**

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 **I**nternet **M**ail **E**xtension**)**

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

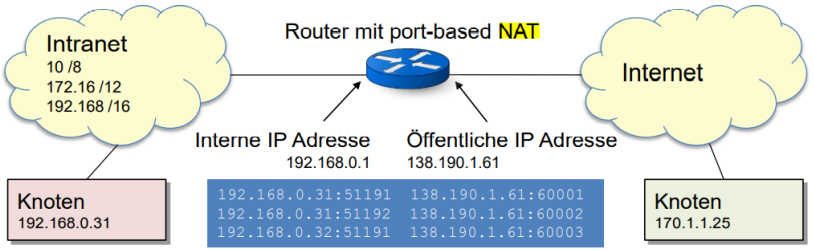
- Maximale Zeilenlänge = 76 Zeichen
- «B»-Encoding (Base64)
- Beispiel: Züri → WvxyaQ==
- *echo «Text» | base64*



Network **A**ddress **T**ranslation **(NAT)**

- NAT (Historisch) Sicherheit durch «Verstecken» von lokalen Adressen
- NAPT (Port Trans.) Lokale IP-Adresse → Öffentliche IP-Adresse

NAT verletzt 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 (öffentliches Netz)			
Quell-Adresse	Port	Ziel-Adresse	Port		Quell-Adresse	Port	Ziel-Adresse	Port
192.168.0.31	51991	170.1.1.25	80	→	138.190.1.61	60001	170.1.1.25	80
192.168.0.31	51992	170.1.1.25	443	→	138.190.1.61	60002	170.1.1.25	443
192.168.0.32	51991	170.1.1.25	25	→	138.190.1.61	60003	170.1.1.25	25

Pascal Isliker