KT Summary (10 page max)

22. Februar, 2023; rev. 11. Juni 2023

Linda Riesen (rieselin)

1 Das OSI Referenzmodell :01 (Vorlesung)

1.1 Kommunikationsschicht / Protokoll / Dienst / Interface

Eine Kommunikationsschicht N:

- bietet der höheren Schicht N+1 über ein Interface Dienste an. (ausschliesslich N+1)
- verwendet zur Erfüllung der Aufgaben Dienste der Schicht N+1 (ausschliesslich N+1)
- kommuniziert logisch mit korrespondierender Schicht N (von Gegenseite) über ein Protokoll

Protokoll: Sammlung von Nachrichten / Nachtrichtenformaten / Regeln zu deren Austausch Bsp: Telefongespräch: Hallo, hier ist .. etc. **Dienst** Bsp: Sende unbestätigte/ bestätigte Daten, empfange Daten **Interface** Bsp: send_uc(message, address), send_cond(message, address, quality), ...

1.2 OSI Modells aufzählen

OSI Modell Idee:

- Erstellung eines Modells dass nur so viele Schichten wie nötig hat, sodass Beschreibung und Implementierung nur so schwierig wie nötig ist.
- Ähnliche Funktionen in gleiche Schicht, Grenzen mit nur direkt benachbarter Schicht
- Jeweils einen Grenzpunkt wo die Interaktionen stattfinden.

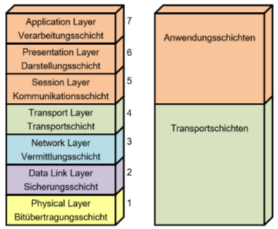
1.2.1 OSI (Open System Interconnection) Modell im Detail

Bei jeder Schicht wird jeweils ein neuer Header + Footer angehängt (die Daten werden verpackt)

- Dient als Referenzmodell mit 7 Schichten
- Schichten haben steigenden Applikationsgrad
- Schichten 5-7 (Applikationsschichten) lösen allgemeine Aufgaben
- Schichten 1-4 (Transportschichten) Treiber/ Betriebssystem, Schnittstelle zur Applikation

Decimal	Binary	Hex
0	0000	0x0
1	0001	0x1
2	0010	0x2
3	0011	0x3
4	0100	0x4
5	0101	0x5
6	0110	0x6
7	0111	0x7
8	1000	0x8
9	1001	0x9
10	1010	0xA or 0xa
11	1011	0xB or 0xb
12	1100	0xC or 0xc
13	1101	0xD or 0xd
14	1110	0xE or 0xe
15	1111	0xF or 0xf

(a) Bit Hex Dez



(b) OSI Modell

1.2.2 Kritikpunkte OSI Modell

- Protokolle konnten sich nicht durchsetzen da zu komplex, ineffizient, teuer
- Durch Weiterentwicklung fehlen heute wichtige Themen

1.2.3 Physical Layer (Bitübertragungsschicht)

Ungesichterte Übertragung eines Bit-Stroms

- Elektrische Eigenschaften (Signalform, Amplituden, Frequenz)
- Codierung (Abbildung der Daten auf elektrische Signale)
- Mechanishce Eigenschaften (Stecker, Pinbelegung etc.)

Übertragungsmedium (zb Kabel)

- Liegt unterhalb, formal nicht teil von OSI Modell, nur durch Spezifikation beschrieben

1.2.4 Data Link Layer (Sicherungs-/Verbindungsschicht)

Gesicherte Übertragungsstrecke zwischen direkt verbundenen Knoten
Aufgaben:

- Framing (Rahmenbildung/-erkennung) (= Verpacken von Datenblöcken in Datenrahmen, für Übertragung, Auspacken der Datenblöcke aus den empfangenen Frames)
- Fehlererkennung und Korrektur
- Fluss-Steuerung (Flow Control) (schneller Sender soll langsamen Empfänger nicht überfordern)

Bei mehreren Teilnehmern Zusätzlich:

- Addressierung der Teilnehmer (eindeutige Addresse pro Kommunikationsknoten)
- Medium Zugriff (Media acces) (=Koordinaten des Zugriffs auf das gemeinsame Medium)

1.2.5 Network Layer (Vermittlungsschicht)

Leitungsvermittlung und Packetvermittlung
Leitungsvermittlung: Datentransfer mit Verbindungsnummer, Datentransfer mit fixem Pfad
Paketvermittlung: Datentransfer von a nach d, Datentransfer mit fixer Adresse

1.3 Zuverlässige unzuverlässige Dienste / verbindungsorientierte verbindungslose Dienste

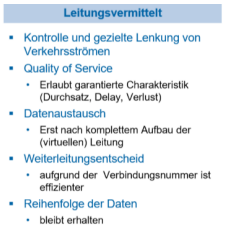
1.3.1 Zuverlässig vs Unzuverlässiger Dienst

Zuverlässig:

- Es gehen grundsätzlich keine Daten verloren
- Wird gesichert durch Fehlererkennung, Fehlerkorrektur, Quittierung von erhaltenen Daten
- Bsp: Online Backup

Unzuverlässig

- Es können Daten verloren gehen
- Bsp: Telefonie



(c) Vergleich der Diensttypen

(d) Vergleich der Transporttypen

1.3.2 Transport-Layer (Transportschicht)

User Data Protocol (UDP) (= verbindnungsloser **unzuverlässiger** Dienst im Internet)
Transmission Control Protocol (TCP): (= verbindungsorientierter **zuverlässiger** Dienst im Internet)
TCP schafft die Illusion einer fehlerfreien, virtuellen Verbindung (tatsächliche Verbindung findet eigentlich auf Unterer Ebene statt und ist nicht fehlerfrei)

1.3.3 Anwendungsschichten 5-7

- 7 Application Layer (Anwendungs / Verarbeitungsschicht)
  - Verbindung zur eig. Anwendung, bestimmt die Protokolle der versch. Anwendungen
  - Bsp. File Transfer, E-Mail, WWW, Namensauflösung (DNS), ...
- 6 Presentation Layer (Darstellungsschicht)
  - Umwandlung der Darstllung v. Daten
  - Konvertierung von ASCII etc. Codes, Konvertierung zw. versch. Arten der Zahlendarstellung
- 5 Session Layer (Sitzungsschicht)
  - Auf/Abbau einer Session
  - Wird die Transportverbindung unterbrochen so kann Session Layer eine neue Verbindung aufsetzen ohne das die höheren Schichten etwas merken

2 Übertragungsmedien :01 (Praktikum)

Die Ausbreitungsgeschwindigkeit in drahtgebundenen und optischen Leitern (Glas u Kupfer) beträgt ca. 2/3 von c (Lichtgeschw.) = 200'000'000 m/s = 200'000 km/s = 20 cm/ns

2.1 Maximale Leitungslänge

2.1.1 Signaldämpfung

(= Leistungsabnahme eines Signals): (je grösser Signalrate desto höhere Datenrate, je kl. Dämpfung desto grösser Distanz oder grössere Bitrate)
Dämpfung $A = 10 * log(P_1/P_2)$ und $A = 10 * log((U_1/U_2)^2) = 20 * log(U_1/U_2)$

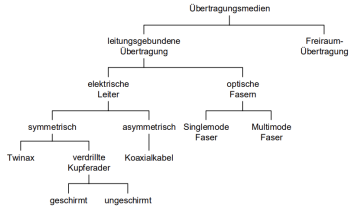


Abbildung 1: Übersicht Übertragungsmedien

2.1.2 Max Leitungslänge:

Wird gesetzt durch: **Dämpfungsbelag** und **Signal to Noise Ratio (SNR)**
$SNR = 10 * log(P_{Signal}/P_{Strung})$

- Koaxial Kabel: viel besser (hochfrequente u. elektromagnetische Signale), aber schwieriger zu verlegen (heikel gegen knicken/quetschen) und teurer als TP Kabel
- Paarsymmetrische Kabel (Twisted Pair):
  - Häufig, breitbandig Nutzbar, gibt es shielded und unshielded (geschirmt mit besserer Störsicherheit) (da sonst die Nachbarkabelpaare gestört werden durch Magnetfeld (kapazitiv/induktiv)
  - Komplementäre Signale und Schirmung als Massnahme gegen **kapazitive Störungen**, Verdrillung (= Verdrehung der Kabel) gegen **induktive Störungen**
  - Taxonomie der TP Kabel: xx/yTP (TP = Twisted Pair, (xx = Platzhalter f. Gesamtschirmung: U = ungeschirmt, F = Folienschirm, S = Geflechtschirm, SF = Geschirm aus Geflecht u Folie) (y = Platzhalter f. Aderpaarschirmung (einz. Drahtpaare): U = ungeschirmt, F = Folienschirm, S = Geflechtschirm)
- Optische Leiter haben viel geringere Dämpfungsbeläge als elektrische Leiter, **Dispersion** (= Verzerrung des Signals durch Polarisation, Wellenlänge, mechanische Ungenauigkeiten, Nichtlinearitäten, etc) zusätzlich einschränkend bei Glasfaser
- Glasfaserkabel (steigend nach Kosten u Qualität)
  - Multi Mode **Stufenfasern** (dickster Kern, mehrere Wege möglich grösste Dispersion)
  - Multi Mode **Gradientenfasern** (Bremsung der Moden im Zentrum = Gleichmässiger)
  - **Single Mode Fasern** (sehr dünner Kern, nur Grundmode, keine Dispersion)

Grundprinzip d. optischen Fasern: **Totalreflektion** (am Mantelglas und Lichtstrahlführung dadurch) und Ausbreitung des Lichtes in bestimmten Moden (Multi/Single)

2.2 LSB (Least Significant Bit)

Beim Empfangen der Daten muss der Empfänger die Bits in umgekehrter Reihenfolge lesen, um den ursprünglichen Wert des Bytes wiederherzustellen. Das bedeutet, dass der Empfänger zuerst das LSB liest, dann das zweitniedrigste Bit und so weiter, bis zum MSB. (Da das LSB als erstes gesendet wird)

3 Physical Layer :02

Die Physikalische Schicht befasst sich mit der **Umwandlung physikalischer Signale** (elektrisch/optisch) in einen **Bitstrom** und umgekehrt. Dabei sind bestimmende Eigenschaften:

Verkehrsbeziehung (Simplex/Halb-Duplex/Voll-Duplex)

- Simplex: 1 Sender, 1 Empfänger, Datenfluss in 1 Richtung
- Halb-Duplex: 1 Sender, 1 Empfänger aber Datenfluss kann nacheinander in beide Richtungen stattfinden
- Voll-Duplex: 2 Sender/Empfänger, Datenfluss kann gleichzeitig in beide Richtungen stattfinden

Kopplung (Punkt-Punkt / Shared Medium): Nur 2 Endstücke der Leitung/ Mehrere Empfänger, bei Voll-Duplex Mehrere Sender/Empfänger möglich

Übertragungsmedium (Koaxialkabel/Twisted Pair/Lichtwellenleiter/Radiowellen)

Übertragungsverfahren (synchron/asynchron) zudem: Basisband/Trägerfrequenz

- Synchron: Vorteil: Nur 1 Leitung Benötigt, Nachteil: Zusätzlich 2x Leitungseinrichtung (teuer)
- Asynchron: Vorteil: Billiger, Nachteil: Genauigkeit gefordert

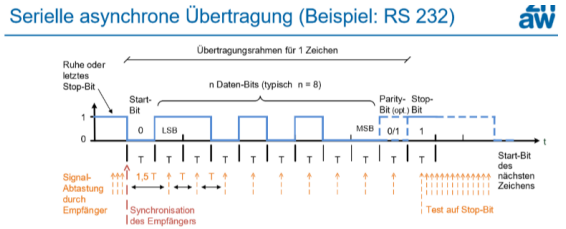


Abbildung 2: Mit Letzer Abtastung zwingend im Zeitfenster (Stop Bit bei Stop Bit) damit nä. Zeichen richtig erfasst wird.

Die Leitungscodierung legt fest wie genau diese Umsetzung erfolgt.
Dabei ist wichtig:

Gleichspannungsfreiheit Aus dem Zusammengepressten (codierten) Code muss wieder Takt und Datensignal hergestellt werden können (auch bei zbsp längeren Folgen von Nullen.)

Taktrückgewinnung: Durch Phasenvergleich wird der Takt angepasst/korrigiert (schneller/langsamer) wodurch der ganze Datenstrang korrigiert wird.

Beispiele: RS-232 (Asynchron Seriell), PAM3 (Gleichspannungsfrei)
Wichtige Kenngrössen im Zusammenhang mit der (maximalen) Übertragungsrate sind:

Bandbreite (B): Eigenschaft des Übertragungskanals durch das Medium begrenzt, Masseinheit Hertz (Hz)

Symbolrate (Nyquist): Anzahl der Symbole pro Zeit limitiert durch die Bandbreite ($\leq$ 2B), Masseinheit Baud (Bd): $f_S \leq 2B$ (für ideales Übertragungsmedium ohne Störungen)

Symbol (!= INCO): Zu gewissem Zeitpunkt übertragenes Signal das mit Symbolrate seien Wert (Amplitude, Frequenz, Phasenlage, etc) verändert)

Baudrate: Schrittgeschwindigkeit = Leitungssymbole pro Sekunde

Zeichenrate: anz. (zbsp ASCII) Zeichen pro Sekunde

Bitrate (Hartley): Prodkt von Symbolrate u. mittlerem Informationsgehalt der Symbole, Masseinheit bits/s (bps)

Anz. Zustände pro Symbol: Bitrate / Symbolrate

- Unterscheidbare Signalzustände pro Symbole: $M = 1 + \frac{A}{\Delta V}$
- Informationsgehalt von 1 Symbol: $I_s = log_2(M)$ ($log_2 = ld$)
- Max. Bit-Rate einer Übertragungsstrecke: $R \leq 2B \cdot log_2(M)$ (kann nicht beliebig gross gemacht werden da Rauschen!)

Kanalkapazität (Shannon): Berücksichtigt zusätzlich das Rauschen, Masseinheit bits/s (bps): $C_s = B \cdot \log_2(1 + \frac{S}{N})$

4 Datalink Layer :03

4.1 Framing, Erkennen von Framegrenzen

Schicht 2 ist bei Senden für Framing, bei Empfangen für erkennen von Framegrenzen aus Bitrstrom der Physical Layer liefert zuständig.
-> Framing wird sichergestellt mithilfe von Bitstuffing (Bitstopfen = Sender fügt wenn Flag fast erreicht wurde das jeweils andere Endbit ein so dass Flag nicht gesendet wird. (Bsp. Flag = 0110, Nachricht: 11.. Zwingend wird jetzt 1 eingefügt.))
Datenübertragung findet statt.
asynchron (Pause zw. Frames) /**synchron** (kontinuierlicher Bitstrom) -> Maskierung von Sonderzeichen (Flags) nötig.

4.2 Fehlererkennung

Hinzufügung von Redundanz (zusätzlich übertragene Information) -> Erhöhung der Hamming Distanz (min. Anz. untersch. Bits zw. gültigen Codewörtern)
Hammingdistanz d erlaubt Erkennung von (d-1) Fehlern, Korrektur von (d-1)/2 (abrunden).
Bsp: Blockcodes (Ein- und Zweidimensionale Parity, Checksummen, CRC)

4.3 (optimale) Framegrösse

Optimale Framegrösse stetiger Kompromiss zwischen Overhead und einer geringen Frame/Restfehlerwahrscheinlichkeit.
Beeinflusst von: Bitfehlerwahrscheinlichkeit, Datenrate, Verzögerungen im System
Optimale Frame Grösse (Näherung) = $\sqrt{\frac{H}{p_e}}$ [H= Header Länge, $p_e \ll 1$]

4.3.1 Fehlerwahrscheinlichkeit

- Um N Bit Fehlerfrei zu empfangen muss jedes einzelne Bit fehlerfrei empfangen werden
- Erfolgswahrscheinlichkeit für 1 Bit: $P_{Erfolg} = (1 - p_e)$
- Erfolgswahrscheinlichkeit für den ganzen Frame (N Bit): $P_{Erfolg,Frame} = (1 - p_e)^N$
- Fehlerwahrscheinlichkeit für ganzen Frame: $P_{Fehler,Frame} = 1 - (1 - p_e)^N$
- für $p_e \ll 1$ gilt Näherung: $P_{Fehler,Frame} = p_e \cdot N$ = FER
- Framerate: $\frac{BitrateB}{(Payload+Overhead)*8Bits}$
- Nutz Bitrate von Payload: $Framezisze * SizeofFramePayload$
- Delay (t) Store/ Forward Switch bei Framelänge l: $\frac{framesize}{bitrate}$

Begriffe: BER (Bit Error Ratio (=Fehlerfate Bits / Gesamtzahl Bits)), FER (Frame Error Ratio = Fehlerhaft empfangene Frames (= Datenrahmen)), RER (Residual Error Ratio = Unentdeckte fehlerhaft empfangene Frames)

Fehlerkorrektur Fehlerkorrektur: gibt es Rückwärts (erneutes übertragen der Daten) und vorwärts (Rekonstruktion von verfälschten Bits bei Empfänger.

4.4 Shared Medium: Addressierung & Steuerung der Sendeberechtigung

Wird auf Datalink Layer gelöst bei mehr als 2 Kommunikationsteilnehmern.

- Master/Slave (Master koordiniert Zugriffe, keine Konflikte, hat aber Single P. of Failure)
- Tokengesteuert ((mit Token oder Frame), Knoten Senden/fügen Daten an nur wenn Token bei ihnen, deterministisch, aufwändig)
- Zeitgesteuert (analog Taktfahrplan (Bahnnetz), Optimierung möglich, Planung erforderlich, Konflikte mit unplanbarem Verkehr)
- Kollisionserkennung und auflösung (Gleichberechtigung von allen Stationen, Übertragungsmedium wird vor Senden abgehört ob frei, kommt zu Kollision wenn 2 gleichzeitig Senden: > Abbrechen und nochmals versuchen / Arbitrierung (= Auflösung))
  $t_{frame} > 2 * t_{transfer}$

4.5 Flusskontrolle (= Flow Control)

Siehe Schicht 4, ist aber auch Aufgabe von Schicht 2 falls implementiert.
Empfänger kann Sender temp. stoppe, Stop/Start Meldungen erfolgen über Datenrückkanal (geht automatisch mit Backward Error Correction da Sender dort sowieso auf Quittierung wartet)

5 Ethernet 1 (LAN, Grundlagen) :04

Ethernet: Verbindungslos (basiert auf Verbindungsorientiert LAN), Zuverlässig)

5.1 LANs (Local Area Network)

Ethernet ist die Variante die sich durchgesetzt hat. **historisch:** räumlich kleine Netze, die verschiedene Geräte verbinden und in welchen Daten mit hoher Geschwindigkeit übertragen werden
LAN-Topologien: Bus (kann sich ins Wort fallen), Linie, Ring, Stern (kann sich nicht mehr ins Wort fallen), Baum und vermaschte Strukturen

- Bus: alle Stationen passiv, horchen Leitung permanent ab, werden aktiv wenn sie senden wollen, keine festgelegte Ausbreitbungsrichtung, (anhand der Adresse erkennen Empfänger ob Daten relevant)
- Linie: Punkt zu Punkt verbindungen zwischen benachbarten Konten, Alle Stationen müssen Daten empfangen, Daten regenerierne, falls nötig weiterleiten, Falls eine Station ausfällt, Segmentiert das LAN in 2 Teile
- Stern: jede Station an zentralen Verteiler (Switch/Bridge) angeschlossen, Verteiler entkoppelt Knoten, weniger störungsanfällig, Verteiler leitet Daten von Station an andere Knoten weiter
- Baum: Hierarchische Erweiterung der Sterntopologie, Itelligente Switches ermöglichen einen grossteil der Kommunikation lokal, Verringerung der Last für die einzelnen Switches
- Ring: Benötigt Verfahren zur Verhinderung von endlosem Kreisverkehr, hat gewisse Redundanz bei Ausfall von 1 Station kann kann immer noch jede Station erreicht werden
- Vermascht (teilweise/komplett): Weitere Erhöhung der Redundanz, Ausfall v. einer oder evt. auch mehrerer Stationen oder Verbindungen kann toleriert werden, Zusätzliche Kosten Aufwand um mehrfache Lieferung der Daten zu verhindern

untere Ebene des LANs: unicast (nur an 1 Adresse), multicast (an mehrere mit Gruppen Adresse), broadcast (an alle in einem LAN) **Standards (IEEE):** Norm **802**: eine Reihe von Standards für LAN und MAN aufgestellt

5.2 Ethernet Varianten

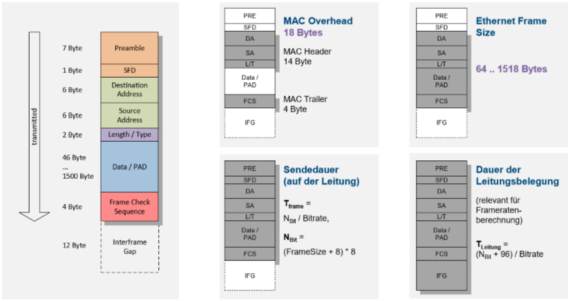


Abbildung 3: Aufbau Ethernet Frame Format

- Hat mindestlänge für Kollisionserkennung (46-1500 Bytes)
- Definieren die **physikalische und Teile der Sicherungsschicht**
- verwenden das gleiche **Frame-Format**, das auch allen später entwickelten Ethernet/802.3-Varianten verwendet wird
- MAC-Adressen der Länge 6 Bytes identifizieren Ethernet Geräte: (Bsp: 04-0a-E0-13-14-26, 3 Byte für Hersteller Identifikation, 3 Byte für Laufnr durch Hersteller, dann 1. gesentetes Bit = Individual (0)/ Group Adress (1) , 2. gesendetes Bit = Universal (0)/ Local Administrated Adress (1))

5.3 10BASE-T

- sehr alt kann einfach beobachtet werden,
- Manchester Codierung, Unterstützung von Repeatern/Hubs
- Betrachtung nicht der Takte sondern der Flanken (steigend, sinkend) => es wird immer etwas gelesen auch wenn zbsp lange Serie von Nullen. Um den Clock herauszulesen wird Preamble (101010 von 7 Bytes + Strart Frame Delimiter 11 (1 Byte) gesendet) damit sich der Clock einpendeln kann. => Dann können (theoretisch beliebig viele) Daten gesendet werden ohne dass Clock wieder angepasst werden muss

5.4 Switches (Bridges)

- Broadcast Domain: schickt an alle, umspannt das ganze LAN
- Ansonsten schickt an Adresse die bekannt oder falls unbekannt auch an alle.
- arbeiten transparent (unsichtbar) auf dem Data Link Layer

- schliessen mehrere Segmente zu einem LAN zusammen
- Das resultierende LAN ist eine einzige Broadcast Domain
- Bridges leiten (Address Learning) Frames nur dorthin weiter, wo sie empfangen werden müssen => Lastreduzierung und Erhöhung der effektive nutzbaren Kapazität
- Switches ab 2-Port (Bridge) werden auch als Multi-Port (Ethernet-Bridge) bezeichnet

5.5 Verbindungslos / Verbindungsorientiert

Verbindungslos: Datenpakete werden unabhängig voneinander übertragen, ohne vorherige Verbindungseinrichtung, was Flexibilität bietet, aber keine Garantie für Reihenfolge, Zustellung oder Fehlerfreiheit der Pakete.

Verbindungsorientiert: Vor der Datenübertragung wird eine Verbindung zwischen Sender und Empfänger hergestellt, um Zuverlässigkeit, Fehlererkennung und die Reihenfolge der übertragenen Daten zu gewährleisten.

6 ETH 2 :05

6.1 VLAN

Mit gemanagten Switches/Bridges kann ein physikalisches LAN in mehrere **virtuelle LANs (VLAN)** mit separaten Broadcast Domains aufgeteilt und **Prioritäten** unterstützt werden
Einsatz: (Firma mit separatem Gästezugang / Bürogebäude mit mehrern Firmen / Entwicklungsabteilung mit Versuchsnetz) **Zuordnung der Frames**

- Zuordnung durch getrennte (phyisch getrennte Netze) (Access Ports) oder durch
- Adressierung (Tagging: Unsichtbar für Endgeräte, Konfiguration nur im Netz) (Trunk Ports) Beim Header kommt erst die Adresse, dann der Tag damit auch für nicht Vlan Switches lesbar.
- Quality of Service (QoS), Frames können im Switch überholen, durch Priorisierungs Strategien (Bsp Strict Priority)

6.2 Port Mirroring

Port Mirroring ist ein mögliches Verfahren zur Verkehrsbeobachtung und Fehlersuche in Switched Ethernet

6.3 Redundanz

Redundanz wird ermöglicht:

- durch die „künstliche“ Reduktion der Topologie auf eine Baumstruktur durch **Spanning Tree Algorithmen**: Alle Segmente in einer loop-freien Topologie verbinden:
  Root Bridge wird ausgewählt (willkürlich aber eindeutig), Ausgehend von Root wird ein Baum aufgebaut, redundante Pfade werden gesperrt

6.4 Kompatibilität

Kompatibilität 10/100/1000BASE-T (letzes Zeichen für Kabel Art, hier T = Twisted Pair) wird erreicht durch **Beibehaltung** von Frame Format und Schnittstelle zwischen PHY und MAC **Autonegotiation** mittels FLP bursts / NLP Zur Zeit dominieren

- Geswitchte 100BASE-TX oder 1000BASE-T Systeme, die oft gemeinsam in einem LAN betrieben werden
- **Geswitchter Vollduplex Betrieb** (mikrosegmentiertes LAN)

Methoden zur Verkehrsbeobachtungn von geswitchtem. Eth Lan anwenden: Praktikum: Einschaltung von eigenem Switch, Ersetzung einens Switches und Reduzierung der anliegenden Frames auf lesbare Framerate.

6.5 Phy Codierung

PHY Codierung ist unterschiedlich (Manchester, scrambled NRZ/MLT-3 mit 4B5B Codierung, etc.)

- Höhere Datenrate => höhere Ansprüche an die Signalverarbeitung und Algorithmen im PHY
- Massnahmen zur Reduktion von Maximaler Signalfrequenz und EMV Pegeln werden mit steigender Datenrate immer wichtiger

6.6 100 Base T, 1000 Base (= 1 Gbs) T, 10 Gbs

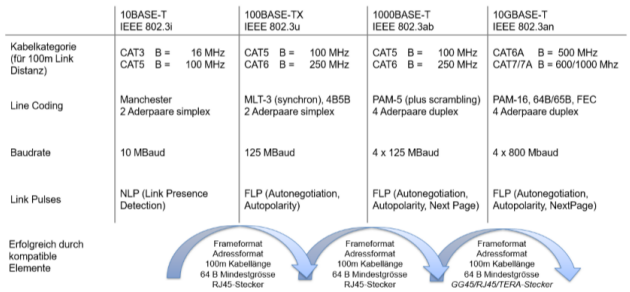


Abbildung 4: Ethernet Vergleiche Evolution

Meist unterstützt ein Ethernet Anschluss mehrere Bitraten = Autonegation

6.6.1 Autonegation

Beruht auf Fast Link Pulses (FLP), dies gleicht die Normal Link Pulses und Fast Link Pulses ab und bei der Decodierung werden diese ineinander gereiht (Frame hat im Header Bedeutung für Identifizierung der verscheidenen Pulses)

7 IP (Teil 1) :06

Die Netzwerkschicht verbindet einzelne, auf Schicht zwei verbundenen Netze, zu einem grossen **virtuellen Netzwerk** (einem Internet)

- Interna der einzelnen Netzwerke bleiben für die Endknoten verborgen
- Die einzelnen Netzwerke können ganz unterschiedliche Technologien verwenden

7.1 Hauptaufgaben der Netzwerkschicht

Die Netzwerkschicht erfüllt hierbei zwei Hauptaufgaben

Routing (Bestimmung der Wege durch das Netz, Aufbau von Routingtabellen)

Forwarding (Weiterleitung von Packets gemäss der Routingtabellen)

7.2 Adress-Schema

Um global Kommunikationsteilnehmer identifizieren (adressieren) zu können, wird ein **hierarchisches** Adress-Schema verwendet; Routing und Forwarding erfolgt aufgrund der **Netzzugehörigkeit von Knoten**, nicht aufgrund der Knotenadressen selbst

- Flacher vs Hierarchischer Adressierraum IP Adressen sind 2 Stufig hierarchisch, IP Adresse eines Hosts = Netz Adresse + Interface Adresse
  Router suchen jeweils die momentan schnellste und noch stabile (nicht kaputte) Route, Reihenfolge der Pakete kann ändern, Verlust kann passieren (ist Aufgabe der oberen Layer)
- Router Funktonsweise Verbindet 2 Netze, kann Technologie ändern, muss aber nicht (ETH-XX oder ETH-ETH), Router betrachtet Adress, schaut in Tabelle ob Adresse vorhanden, falls nein leitet an nächsten Router weiter. Router fasst generell Network Layer nicht an.
  Firewall schränkt das Routing eines Routers ein.
  Adresstabelle enthählt jeweils Port/Switch und zugehörige MAC Adresse, wird alle Ageing Zeit (Standard 30s) gelöscht.

7.3 Art des Dienstes

Gemäss den Designkriterien bei der Entwicklung der TCP/IP Protokollsuite bietet IP einen **verbindungslosen, unzuverlässigen** Dienst
Aufbau von Ip-Adressen:

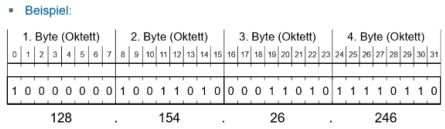


Abbildung 5: IP-Adresse Beispiel Aufbau

- Erlaubt dafür relativ einfache Implementierung von Routern und bietet ein robustes Verhalten bei Fehlern im Netz (Link- / Komponentenausfall)

7.4 Aufbau IP Netz

IPv4 Adressen bestehen aus 32 Bit; diese sind in eine **Netz- und einen Host-Teil** unterteilt wichtigste dienstprotokolle ip4: .....siehe Link (https://www.youtube.com/watch?v=OjBJvXcuE-I&ab_channel=FlorianDalwigk)

- Bitweises AND von Netzmaske und IP Adresse ergibt die **Netzadresse**
- Sind alle Bits des Host- dressteils gleich „ “, so erhält man die **Broadcastadresse** im jeweiligen Netz
- Es gibt da 1 immer links, 0 immer rechts stehen müssen nur 9 mögliche Subnetzmasken
- Knoten mit **übereinstimmender Netzadresse** gehören zum gleichen Netz und können direkt (über Layer 2) miteinander kommunizieren, die Kommunikation zu **allen anderen Knoten** muss **über Router** verlaufen

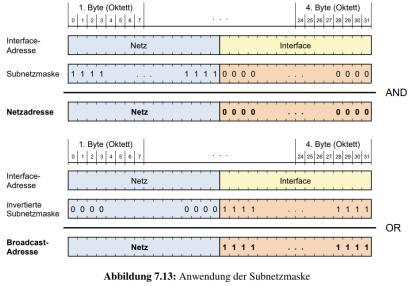


Abbildung 7.13: Anwendung der Subnetzmaske

Abbildung 6: Anwendung Netzmaske

7.5 Routingtabellen

Routingtabellen definieren, über welche Netzwerk-Interfaces welche Netze erreichbar sind.

- Sie in den Hosts werden nach der Grösse der Netzmaske abgearbeitet

- Bei flachem Routing umfasst die Routingtabelle alle bekannten (im Internetwork vorhandenen) Netze
- Hierarchisches Routing arbeitet mit Default-Einträgen

Der **Default-Eintrag** in der Routingtabelle definiert, wohin IP-Pakete geroutet werden sollen, für die keine Eintrag in der Routing Tabelle passt

8 IP (Teil 2) :07

8.1 IP-Header

Der IP-Header besteht aus 20 Bytes

- Version (IPv4 oder 6) können durch Versionsnr parallel in Stack betrieben werden
- Internet Header Length (4 Bit) (Länge Header incl Optionen in Vielfachen von 4 Byte Zeilen, Feldgrösse 4 Bit, 15* 4 = 60 Bytes)
- TOS (Type of Service (8 Bit) -> Prioriesierung, Einteilung in versch. Verkehrsklassen
- Total Length 16 Bit (Länge IP Paket incl. Header und Nutzdaten)
- Time to Live (TTL) 8 Bit, Verbleibende Lebenszeit (dekrementiert von Routern beim Weiterleiten, verhindert endlose Zirkulation)
- Protocol (8 Bit) der Nutzdaten
- Header Checksum (16 Bit)
- Source Adress (32 Bits) IP ursprünglicher Absender
- Destination Adress (32 Bits) IP schlussendlicher Ziel Empfänger
- Padding/Options (variabel)
- Identification Nr/ Flags / Fragment Offset (folgt im direkten Anschluss)

8.2 Fragmentierung und Reassembly

Um über Netze mit verschiedenen Maximum Transfer Units (MTU) arbeiten zu können, unterstützt IP Fragmentierung und Reassembly: Aufteilung (falls nötig) in kleinere IP Pakete mit eigenständigem IP-Header und ert beim Zielhost wieder zum Ursprünglichen Paket zusammengesetzt.

- Jedes IP Fragment beinhaltet alle notwendigen Daten um den Endknoten zu erreichen (IP Header) und ein Vielfaches von 8 Bytes an Transportlayer-Daten (Ausnahme: letztes Fragment)
- Fragmentierung erfolgt direkt beim Sender oder im Router beim Eintritt in das MTU limitierte Netz, Reassembly im Endknoten

8.3 ARP-Request (Address Resolution Protocol)

IP-Pakete werden in Ethernet Frames gekapselt und von jedem Router wieder ausgepackt und erneut gekapselt. Dazu muss der Router die Layer-2 Adresse (MAC-Adresse) des nächsten Routers/Hosts kennen (ARP-Cache) oder erfragen (ARP-Request)
Bei einem **Gracious ARP Request** wird die Adresse gleich gebroadcasted.

8.4 ICMP Internet Control Message Protocol

ICMP wird verwendet, um Fehler innerhalb der Netzwerkschicht zu behandeln (keine Retransmissions)
Bsp: Dont Fragment aber zu kleine MTU -> ICMP Meldung & Datagramm wird verworfen

- ICMP Nachrichten werden in IP-Pakete gekapselt, werden aber dennoch der Netzwerk-Schicht zugeordnet

traceroute traceroute erlaubt den Weg zu einem beliebigen Host (oder fehlerhaft konfigurierten Router auf diesem Weg) zu finden + misst Round Trip Zeit
ping echo-echo reply ping
Wird verwendet um Verbindung zu Host/Router zu prüfen und Round Trip Zeit zu messen

9 TCP (Transportschicht) :09

Transport Layer: Schnittstelle zw. Betriebssystem (Kernelspace) und den Anwendungen (User Space): darauf zugreifen kann man via klar definierte Schnittstelle (TCP/UDP Sockets, Winsock)
Applikationsdaten werden von Protokollen des Transportslayers in IP-Paket gekapselt. (IP-Header + UDP/TCP-Header (ICMP 0001/ TCP 0006/ UDP 0017) + Applikationsdaten)
Port Nr. / Kommunikation Applikationen via Transportlayer: (mehrere Verbindungen pro IP)

- Server Applikationen warten (=listen) an bekannten (well-known) Ports
- Der Vorgang, lokal Daten an verschiedene Instanzen höherer Protokollschichten zu verteilen, wird als Multiplexing / Demultiplexing bezeichnet und findet auf allen Schichten statt („Type“ bei Ethernet, „Protocol“ bei IP, „Port“ bei TCP/UDP)

9.1 UDP (kommt wahrsch. nicht an Prüfung)

- Dient Multiplexen und Demultiplexen der Datagramme zu den Applikationen
- Verbindungslos (AppData wird ins UDP Datagramm eingefügt und gesendet)
- Unzuverlässig (keine Massnahmen gegen Verlust oder Vertauschen von Datagrammen, gleich wie IP-Pakete)

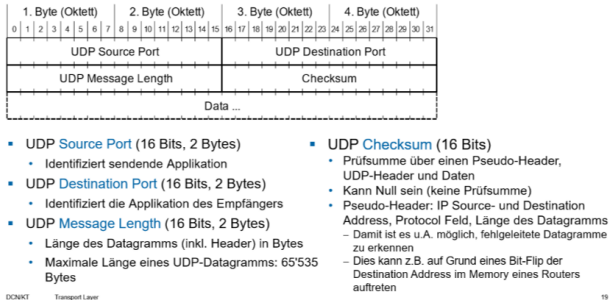


Abbildung 7: UDP Header

9.2 TCP

Ein UDP Datagramm / TCP Segment wird in genau ein IP Paket eingefügt TCP verwendet folgende Massnahmen, um die sichere Kommunikation zu gewährleisten:

- **32-Bit Sequenznummern** – jedes Byte im Datenstrom ist eindeutig identifiziert: Hilft für Reihenfolge und erkennen von verlorengegangenen Daten zsm mit Acknoledge Numbers (Gegenrichtung)
- **3-Wege Handshake** beim Verbindungsaufbau mit **zufälliger Initialisierung** der Sequenznummern

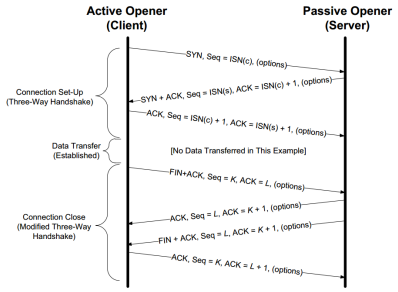


Abbildung 8: TCP Connection Setup / Teardown

- **Kontrollierter Verbindungsabbau** mit der Möglichkeit, ausstehende Daten zu senden
- **Adaptive Timeouts** basierend auf Wert und Varianz der gemessenen Round-Trip Zeiten (Retransmission Time-Out, RTO= SRTT +4*RTTVAR)
(SRTT = Smoothed Round Trip Time = $(1-\alpha)*SRTT+\alpha*RTT$ mit $\alpha=0.125$)
Streuung (gewichteter Mittelwert der Abweichungen) RTTVAR = $(1-\beta)*RTTVAR+\beta*|SRTT-RTT|$ mit $\beta=0.25$
- **Schutz des Empfängers** vor Überlast durch dynamische Anpassung der Fenstergrösse beim **Sliding Window Protokoll** (Advertised Window, wird dem Sender **vom Empfänger** mitgeteilt, bei keinem Platz mehr wird ZeroWindow übergeben und sobald wieder Platz im Buffer ist unaufgefordert ein neues Sliding Window überliefert)
- **Schutz des Netzwerks** vor Überlast durch **Congestion Control (im Sender)** mit dem **Slow Start Algorithmus** => Empfänger setzt die Fensterlänge
- TCP Broadcast gibts nicht immer **Punkt zu Punkt Verbindung.**

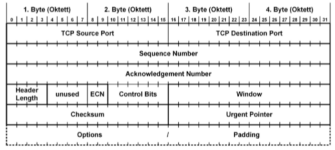


Abbildung 9: TCP Header

9.2.1 TCP Ablauf

- Verbindungsaufbau: Client ist Initiator, Server wartet auf Kontakt, Aushandeln von Optionen, Aushandeln von Sequenznr. Initialisierung von Ressourcen
- Nachrichtenaustausch: Übertragung von Nutzdaten, Sequenznr. sichenr korrekte Reihenfolge, Explizite bestätigung empfangener Daten, Wiederholte Übertragung verlorener Daten
- Verbindungsabbau: Sicherstellen des geordeneten Austausches bis zum Ende, Freigabe der allozierten Ressourcen

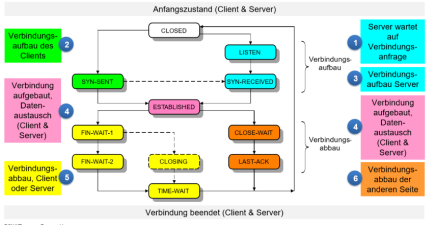


Abbildung 10: TCP Zustandsdiagramm

10 Applikationsprotokolle :10

TCP und UDP: Das Domain Name System (DNS) erlaubt übersetzt Hostnamen in IP Adressen und umgekehrt

- Besteht aus einem hierarchischen DNS (Domain Name Space)
  - Internet Hosts werden meist mit Namen statt IP Adressen bezeichnet (signifikante Vereinfachung f. Benutzer, Internet kennt nur IP Adressen, Namen müssen in IP Adressen aufgelöst werden (= Name Resolution))
  - Früher in host file auf Rechner lokal
  - Hierarchisch Verteilte Verzeichnisstruktur (Baum), Fully Qualified Domain Name (FQDN) muss eindeutig sein (=> Geschwisterknoten dürfen nicht den gleichen Namen haben)
  - die DNS wird verteilt betrieben: Name Server: ist meist für eine Zone (separat adminsistrierter Subtree des DNS, oft eine Domain, ein Name Server kennt: IP Adressen zu Hostnamen seiner Zone, Server seiner Subdomänen (falls nicht in Zone), IP Adressen von Root und TDL Name Server) verantwortlich
  - Meist 2 (master & slave Name Server pro Zone), (für Redundnaz),
- Das DNS wird auf einer grossen Anzahl Name Server verteilt betrieben, ein Name Server ist jeweils für eine Zone verantwortlich (z.B. zhaw.ch)

UDP: DHCP erlaubt einem Rechner, seine IP Konfiguration von einem Server zu beziehen

UDP: TFTP ist ein einfaches, aber zuverlässiges File Transfer Protocol, welches z.B. diskless Systemen dazu dient, das Betriebssystem Image vom Server zu beziehen

TCP: SMTP dient dem Versand von E-Mail Nachrichten, POP und IMAP dem Empfang von EMail Nachrichten aus der eigenen Mailbox

- Mittels MIME und Codierungsverfahren (z.B. Quoted-Printable, Base64) können beliebige Daten als E-Mail Nachrichten versendet werden
- Quoted Printable: (=[A-F][A-F]) Codierung in 8 Bit, 3 ASCII Zeichen, bei Mail wird 128 – 255 (ASCII codiert)
- Base64 Encoding: 3 Bytes werden jeweils als 4 Symbole mit je 6 Bits codiert, 0-63 ASCII Zeichen

TCP: HTTP erlaubt den Zugriff auf verteilte Dokumente, die mittels Uniform Resource Locator (URL) eindeutig adressiert werden

- Basiert auf TCP, Port 80
- Ähnlichkeiten mit SMTP: ASCII-basiert, MIME-Typen, Codierungen
- Dreistellige Statuscodes für die Bestätigungen
- Unterteilung einer Nachricht in Header und nachfolgende Daten
- Transaktionsbasiert: Eine Anfrage vom Client (HTTP Request) resultiert in einer Antwort von Server (HTTP Response)
- HTTP ist zustandslos (stateless): auf dem Application Layer besteht zwischen zwei nachfolgenden Transaktionen kein direkter Bezug

TCP: Network Address Translation (NAT) erlaubt die Wiederverwendung privater IP-Adressen

- Port Based NAT: Alle Host im privaten Netz (192.168.0.0/8) verwenden 192.168.0.1 als Default Gateway
- NAPT-Gateway Funktion: Ersetzt im IP-Header der Ausgehendne Pakete die lokale Source - Adresse durch Globale Gateway Adresse,ersetzt im Transport Layer Header Port durch eine eindeutige / freie Port Nummer, legt Verbindungsinformationen in DB ab, sucht bei eingehenden Paketen die Verbindung in DB und setzt wieder ein.
- Erlaubt zugriff vom Internet auf lokale Hosts/ Dienste

11 Internet Protocol Version 6 IPv6 :13

- IPv4 (2^{32} Adressen) und IPv6 (2^{128} Adressen), Verbesserung Protokollheader, fixe Headerlänge, Felder gelöscht stattessen können mehrere Extension Header folgen, keine Fragmentierung der Pakete an den Routern unterwegs
- keine Fragmentierng nötig durch ermittlung des MTU (Maximum Transmission Unit Path's) -> Fragmentierung wird vor dem Absenden durchgeführt
- IPv6 stellt mit IPsec standardisierte Sicherheitsmechanismen bereit. IPsec ist obligatorischer Bestandteil von IPv6

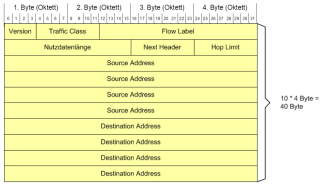


Abbildung 11: Header IPv6

- Extension Header: Bsp Routing Header: Enthält Info zu Next Header, Header Length, und Extension Header Spezifische Daten
- Bei IPv6 können Datenflüsse auf einfache Weise klassifiziert werden; ein Absender kann mit dem Flow Label einen Datenstrom markieren
- Dargestellt werden IPv6 Adressen als Folge von Doppel-Bytes in 1- bis 4-stelligen Hex-Zahlen; je 2 Bytes werden durch einen Doppelpunkt getrennt
- Der IPv6 Adressraum umfasst 3.4 * 1038 Adressen; Adressbereiche werden durch Prefixes gekennzeichnet
- **ICMPv6** ist ein integraler Bestandteil von IPv6 und ist in der IPv6 Implementation eingebaut.
- Das Neighbor Discovery Protocol basiert auf ICMPv6 und ersetzt ARP, DHCP Default Route sowie ICMP Redirect