Verbindungsorientierter Dienst

- Absprache über den bevorstehenden Datenaustausch
- Verbindungsauf- und abbau
- End- und Zwischenknoten speichern Zustandsinformationen der Verbindung
- Reihenfolge der gesendeten Daten wird eingehalten

Beispiele: Telefonverbindung, TCP

Verbindungsloser Dienst

- Kein Verbindungsauf- und abbau
- Daten tragen die Adresse des Empfängers und werden unabhängig voneinander Transportiert
- Keine Zustandsinformationen
- Reihenfolge der gesendeten Daten ist nicht gesichert.

Beispiele: Internet Protocol (IP), Briefpost

Zuverlässiger Dienst

- Es gehen grundsätzlich keine Daten verloren
- Gesichert: Fehlererkennung, Fehlerkorrektur, Quittierung

Beispiel: Filetransfer

Unzuverlässiger Dienst

- Daten können verloren gehen

Beispiel: Sprach- und Videoübertragung

7 Schichten OSI-Modell

	Layer Name	Schichtnamen	Beispiel	
7	Application Layer	Verarbeitungsschicht	HTTP	Anwendungsschichten
6	Presentation Layer	Darstellungsschicht		
5	Session Layer	Kommunikationschicht		
4	Transport Layer	Transportschicht	TCP	Transportschichten
3	Network Layer	Vermittlungsschicht	IP	
2	Data Link Layer	Sicherungsschicht		
1	Physical Layer	Bitübertragungsschicht		

Physical Layer

Sorgt für ungesicherte Übertragung und definiert:

- Elektrische Eigenschaften (Signalform, Amplituden, Frequenzen etc.)
- Codierung (Abbildung auf Signale)
- Mechanische Eigenschaften (Stecker, Pinbelegung etc.)

Glasfaser Vorteile

- Unempfindlich gegen elektromagnetische Störungen
- Kleine Signaldämpfung (grosse Übertragungsdistanzen)
- Grosse Bandbreiten (grosse Übertragungsraten)

Mögliche Probleme

- Modendispersion = Überlappung des Signals. Passiert wenn eine Lichtwelle die andere aufgrund eines kürzeren Weges (Spiegelung) die andere “einholt”.
- Chromatische Dispersion = Teilung einer Lichtwelle in mehrere Lichtwellen (Farben).

Übertragungsverfahren

Legt fest wie die Daten vom Sender zum Empfänger übertragen werden.

- Synchron (Sender Taktet)
- Asynchron (jeder Taktet für sich)

Signaldämpfung

- Wichtiges Kriterium für Übertragungsstrecke
- Teilweise in Abhängigkeit der Frequenz (Multimode und Monomode Lichtleiter)
- Angabe in dB/km (3dB = halbierung der Leistung)

Berechnung

Dämpfung von P in dB (A_{dB}) $= 10 \cdot \log_{10} \cdot \frac{P}{P_0}$
P_0 =Bezugsleistung (z.B. Leistung beim Sender oder Kabelanfang)

Beispiel

$P_0 = 100mW$, $P = 50mW$
$A_{dB} = 10 \cdot \log_{10}(\frac{50mW}{100mW}) = 10 \cdot \log_{10}(\frac{1}{2}) \backsimeq -3dB$

Data Link Layer

Setzt auf dem Physical Layer auf, bietet eine gesicherte (fehlerfreie Datenübertragung) und hat folgende Aufgaben:

- Framing (Rahmenbildung/-erkennung)
- Flow Controll (Flusssteuerung: anpassen der Sendegeschwindigkeit)
- Adressierung
- Media Access (Medium Zugriff: Koordination des Zugriffs auf gemeinsames Medium)

Network Layer

Muss Wege durch ein Netz mit mehreren Knoten finden und die Daten entlang dieses Weges übertragen.

- Routing
- Verbindet einzelne Systeme oder Teilnetze zu einem grossen Netz

Transport Layer

Hat die Aufgabe, unabhängig vom Netz, eine bestimmte Qualität für die Ende-zu-Ende Übertragung zu definieren und diese einzuhalten.

- Ist nur in Endsystemen vorhanden (nicht in Switches/Router)
- Bietet den oberliegenden Schichten einen zuverlässigen Dienst über einen unzuverlässigen Network Layer (TCP über IP).

Session Layer

- Auf- und Abbau einer Session
- Verbindungsunterbruch: er kann eine neue Verbindung aufbauen ohne das höhere Schichten etwas merken

Presentation Layer

- Umwandlung der Darstellung von Daten
- Konvertierung von ASCII, ISO und Unicode
- Konvertierung zwischen verschiedenen Arten der Zahlendarstellung

Application Layer

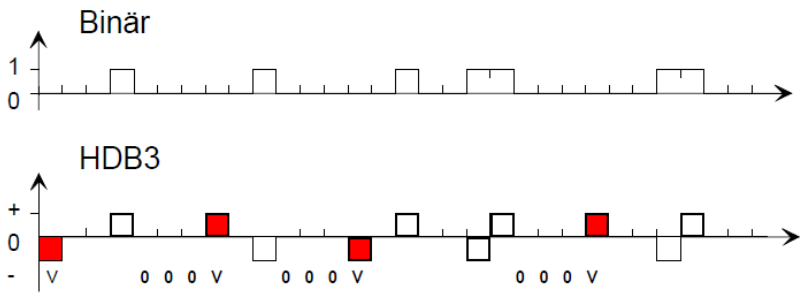
- Bindeglied zu eigentlichen Anwendung, bestimmt die Protokolle der verschiedenen Anwendungen

z.B: Terminal Emulation, File Transfer, E-Mail etc.

HDB3

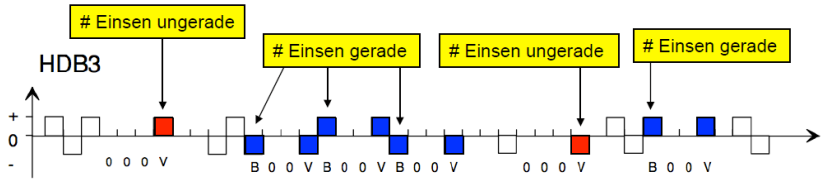
Taktrückgewinnung:

- Tritt vier mal nacheinander eine 0 auf, so wird anstelle der vierten 0 eine 1 gesendet.
- Damit es erkennt wird hat es die gleiche Polarität wie die letzt gesendete 1

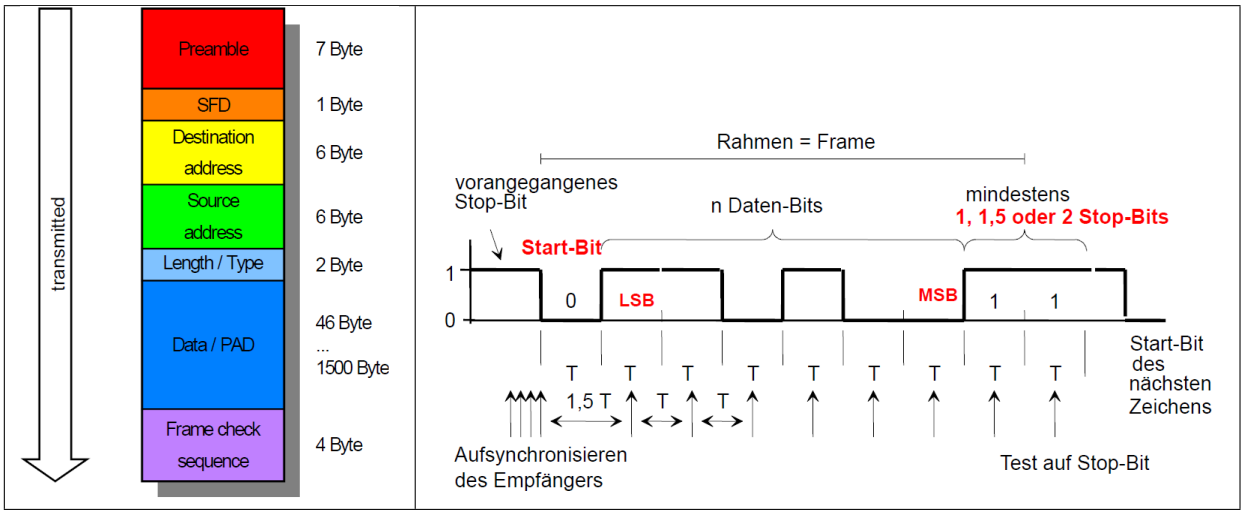


Gleichspannungsfreiheit:

- 4 Nullen werden nicht immer mit 000V ersetzt.
- Ist die Anzahl Einsen (nur richtige Datenbits werden gezählt) seit dem letzen eingefügten 000V/000B ungerade dann wird 000V verwendet, ansonsten 000B (Polarität wechselt).



Frame Format



Payload

$$Payload = \frac{??? \, Bit/s}{8*(38+Nutzdaten)} = ???Frames/s \Rightarrow Frames * Payload = ???Bit/s$$

38 Bit = Präambel (8) + SFD (1) + Destination Address (6) + Source Address (6) + Length/Type (2) + Frame Check Seq. (4) + Interframe Gap (12) = 38

IP und Netzwerkkonzepte

Router

Verbinden Netzwerke und Übertragungstechnologien miteinander, Paketweiterleitung bis zum Ziel

Vorteile und Nachteile von Routern über Bridges:

VORTEILE	NACHTEILE
optimaler Pfad	Teuer
Netze können logisch getrennt werden	konfigurationsintensiv
Abgrenzung von Schicht 2 (Broadcast-Shit-Storm)	teilweise lassen sich Protokolle nicht routen (Netbios)

Kriterium
Loop-Unterdrücku
Sicherheit
Pfade
Broadcast
Multi MTU
Multi Medium
S3-unabhängig

Routingalgorithmen:

- RIP: Routing Information Protocol
- BGP: Border Gateway Protocol

Brouter

- Router mit Bridging-Funktionen, Bridges die routen

Gateway

- Spannen über alle OSI Layer
- Verbinden komplette Systeme

Internet Protocol

Das IP Protokoll ist aus dem ARPANET (US DOD) entstanden. Idee: keine zentrale Steuerung Der Internetlayer ist ein verbindungsloser Networklayer, er ermöglicht Datengramme über jedes Netz zu senden. Der Transport-Layer befindet sich oberhalb des Internet-Layers. Er beinhaltet die Kommunikation zwischen der Quelle und dem Ziel.

- TCP Transmission Control Protocol
  - Verbindungsorientiert, zuverlässig, Flowcontrol, fehlerfreie Übertragung
- UDP User Datagram Protocol
  - TCP ohne Flowcontrol, unzuverlässig, time-reliable

Der höhere Layer (Application Layer) beinhaltet Protokolle wie SSH, HTTP etc.

Adressierung

Adresse	Dezimal	Binär	Berechnung
Host-Adresse	160.85.17.161	1010 0000 / 0101 0101 / 0001 0001 / 1010 0001	
Netz-Adresse	160.85.17.160	1010 0000 / 0101 0101 / 0001 0001 / 1010 0000	host AND netmask
Netzmaske	255.255.255.240	1111 1111 / 1111 1111 / 1111 1111 / 1111 0000	
Broadcast-Adresse	160.85.17.175	1010 0000 / 0101 0101 / 0001 0001 / 1010 1111	host OR inv(netmask)

SubNetBin	SubNe
0000.0000	0
1000.0000	128
1100.0000	192
1110.0000	224
1111.0000	240
1111.1000	248
1111.1100	252
1111.1110	254
1111.1111	255

Eine IP Adresse besteht somit aus 4Byte. Ebenfalls ist die IP 127.0.0.1 (/8) eine LoopBack Adresse (Bereich)

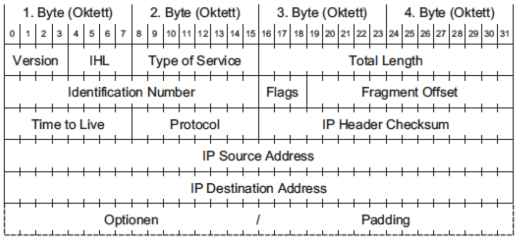
Classful-Routing

Es wird keine SUbnetzmaske benötigt. A(2^24, 1byte Netz (128), 3byte host (16'777'214)), B(2^16, 16'384, 65'534),C(2^8, 2'097'152, 254), D(Multicast,224.0.0.0 – 239.255.255.255), E(Zukunft, 240.0.0.0 – 247.255.255.255)

Routing

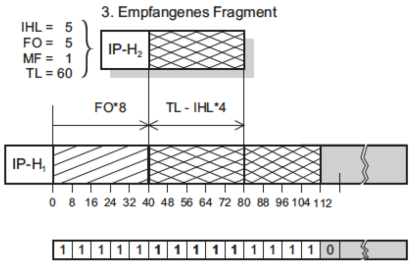
Routen können mit “route -n” oder “netstat -rn” angezeigt werden. (route add -net 160.85.19.0 netmask 255.255.255.0 dev eth2) Falls kein Eintrag der Routingtabelle matcht, dann wird das Paket einfach an den “default” Host weitergeleitet.

IP Protokoll



- Die Internet Header Length (IHL) gibt die Länge des IP-Headers(min5/max15) inklusive dem optionalen Teil(max40byte) in Double Words (32 Bit) an. Die Länge bezeichnet also die Stelle wo im Datagramm die Nutzdaten beginnen.
- Quality of Service, gibt die Eigenschaft an. Dringend, hi reliablility, throughput etc.
- Total Length bezeichnet die gesamte LÍange des Datagramms in Byte (inklusive Header und Nutzdaten)
- alle Fragmente des Datagramms den gleichen Identifikationswert
- Flags: reserved null, fragment allowed, last more fragments
- innerhalb des Datagramms ein Fragment: Der Fragment-Offset wird in 8-Byte-Einheiten (64 bits) angegeben, wobei das erste Fragment einen Offset von Null hat (in maximal 213 = 8192 Fragmente zerlegt)
- TTL: verbleibende Zeit in Sekunden an, die das Datagramm noch im Internet-System verbleiben darf
- Protocol: 1 ICMP / 6 TCP / 17 UDP

Fragmenting



Adressauflösung

Address Resolution Protokoll (ARP) von 4-Byte-langen IP-Adressen auf 6-Byte-lange Ethernet-Adressen

- ARP-Request: “who-has x.x.x.x” als Broadcast ins Netz, wird durch Bridges nicht gefiltert, dadurch kann hoher Traffic entstehen
- ARP-Response”is-at y:y:y:y:y:y direkt an den anfragenden Knoten, man beachte, dass die gesuchte Antwort im Feld Sender-MAC-Address zu finden ist

Im ARP-Cache werden die Adressen zwischengespeichert, sodass man nicht immer für jedes Paket eine neue ARP Anfrage machen muss.

- Gratuitous ARP: ARP Requests/Replies die nich (nach Standart) notwendig sind. Sie werden verwendet um IP-Adresskonflikte zu erkennen. Auch beim ändern der IP-Adresse verschickt, aber mit dem Zweck, die ARP-Cache der anderen Knoten zu berichtigen.

Mit dem Befehl “arping -C 1 -U x.x.x.x” kann ein Request gesendet werden.

Reverse Address Resolution Protocol (RARP) von Ethernet-Adresse auf IP-Adresse

- Verwendung von RARP ist besser als das Ablegen einer IP-Adresse in einem Disk-Image, weil dadurch die gleiche Konfiguration auf allen Maschinen benutzt werden kann
- Nachteil, dass es MAC-Layer-Broadcast benutzt, um den RARP-Server -> von Routern nicht weitergegeben
- Alternative: BOOTP und DHCP

Internet Control Message Protocol (ICMP)

- Zur Übertragung von Fehlermeldungen oder Informationsautausch auf Internet Layer
  - Time to live hat den Wert 0 erreicht
  - Host möchte testen ob ein anderer "up" ist
- Meldungen werden in IP Paketen gekapselt (wird zum Network Layer gezählt)
- Gebräuchliche Meldungstypen:

ICMP-Typ	Bedeutung (Fehler)	ICMP-Typ
3	Destination Unreachable	IP Paket kann vom Router nicht zugestellt werden..
4	Source Quench	Pufferspeicher des Routers voll, Pakete werden verworden, senderate soll gedrosselt wer
5	Redirect	Hinweis das ein Paket direkt an den Zielhost gesendet werden kann.
11	Time Exceeded	Time to Live abgelaufen oder fragment. Paket kann nicht innerhalb nützlicher Zeit reassemblie
12	Parameter Problem	IP-Header enthält ungültige Parameter
	Bedeutung (Info)	
0	Echo Reply	Anwort auf Echo (Echo Reply), gleiche Daten wie Echo
8	Echo	Echo Request
13	Timestamp	Wie ein Echo, aber mit zusätzlicher Zeit. (32-Bit Wert, Millisekunden seit Mitternacht G
14	Timestand Reply	Timestamp Reply

- Destination Unreachable Codes:
  - 0 = net unreachable
  - 1 = host unreachable
  - 2 = protocol unreachable
  - 3 = port unreachable
  - 4 = fragmentation needed an DF set
  - 5 = source route failed

Trace Route Programm

Erlaubt den Weg zu einem Zielhost (oder fehlerhafter Router auf dem weg) zu finden.

- Man sendet UDP Datagramme an den Zielhost; wobei eine hohe Portnummer zufällig gewählt wird (default: 33434)
- Das erste Datagramm wird mit TLL=1 gesendet, der erste Router setzt TTL auf 0, verwirft das IP Paket und sendet eine Time Exceeded ICMP Message zurück, erster Router ist bekannt.
- Das gleiche mit TTL=2 und so weiter.

Um die Entfernung zu bestimmen, wird zugleich die Round-Trip Zeit gemessen.

IPv6

- 32-Bit Adressen zu kurz (IPv4)
- IPv6: 64-Bit Network- und 64-Bit Host-Nummer
- Header Format: ziemlich verändert, von 20 auf 40 Bytes gewachsen
- Mehrere Header: ein Header kann auf den nächsten zeigen (sog. extensions)
- Video-/Audiounterstützung: Flow-Label im Header

Transport Layer

- Stellt den Applikationen eine geeignete Ende-zu-Ende Qualität für Datenübertragung zu Verfügung.
  - UDP: gibt die Eigenschaften von IP fast unverändert weiter: Verbindungslos, Unzuverlässig
  - TCP: zusätzliche Funktionen: Verbindungsorientiert, zuverlässig.
- Bildet Schnittstelle zwischen Betriebssystem (Kernel Space) und Anwendungen (User Space).

- Der Zugriff auf die Funktionen des Transport Layers erfolgt via einer klar definierten Schnittstelle:
  - TCP/UDP Sockets (Unix/Linux/BSD)
  - WinSock (Windows)
- Kapselung:
  - Applikationsdaten erhalten einen TCP/UDP Header
  - Das Paket wird als User Datagram (UDP) oder Segment/TCP-Nachricht (TCP) bezeichnet
  - Ein Transport Layer Paket wird in ein IP Paket eingefügt

Multiplexing und Demultiplexing

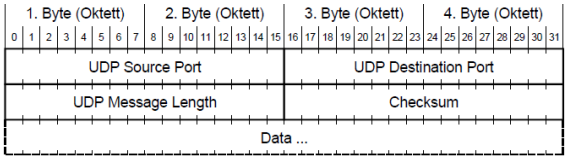
Identifikation eines Hosts über IP Adresse, Identifikation einer Applikation auf einem Host über Port Nummer.

- Multiplexen: Mehrere Kommunikationsbeziehungen zwischen Applikation werden mittels Port Nummern eindeutig bezeichnet.
- Demultiplexen: Verteilen der eingehenden Daten mittels der Port Nummern auf die Applikationen (Es wird zuerst das Type-Feld (ARP/IP/RARP) ausgewertet. Ists IP Type, so wird zwischen ICMP, IGMP, TCP und UDP unterschieden. Aufgrund der Portnummer im TCP- oder UDP Header können die Daten einer Applikation zugeordnet werden.

User Datagram Protocol (UDP)

Dient dem Multiplexen und Demultiplexen der Datagramme auf die Applikation. Verbindungslos und unzuverlässig

Header



- Source Port (16 Bits): Identifiziert sendende Appl. (0 wenn nichts zurückkommen soll)
- Destination Port (16 Bits): Identifiziert Appl. des Empfängers
- Message Length (16 Bits): Länge des UDP Datagramms inkl. Header (in Bytes) (Max. 65535 Bytes)
- Checksum: Prüfsumme über Pseudo-Header, UDP Header und Daten.

Transmission Control Protocol (TCP)

Soll unzuverlässiges IP erweitern um zuverlässigen Datentransport zwischen Applikationen. Netze ROuter und Zielhost sollen nicht überlastet werden.

- Verbindungsorientiert (End-zu-End Dienst, Verbindung ist virtuell: wird nur durch Software hergestellt)
- Zuverlässiger Verbindungsaufbau (beide Endpunkte müssen bestätigen)
- Verbindungsaufbau über 3-Way-Handshake
  - Anfrage Client: Seq=100, Ack=0, SYN
  - Bestätigung Server: Seq=200, Ack=101, SYN/ACK
  - Bestätigung Client: Seq=101, Ack=201, ACK
- Hohe Zuverlässigkeit (Richtige Reihenfolge der Daten ohne Datenverlust)
- Vollduplexübertragung
- Stream-Schnittstelle
- Eleganter Verbindungsabbau (Mit 4 Nachrichten; Zustellung aller Daten auch dann, half Close)
- Übertragung gekapselt in IP Paket (Router leiten weiter, IP-Modul des Empfänger liefert es an das TCP-Modul weiter)
- Umlaufverzögerung (Round Trip Delay) wird laufend gemessen und Wartezeit bis Retransmission entsprechend eingestellt.

Sliding Window

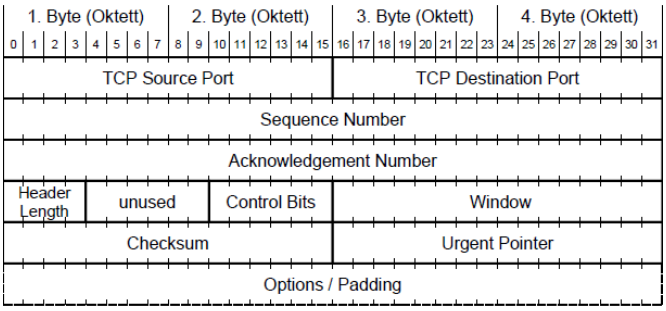
- Sender und Empfänger einigen sich auf fixe Fenstergrösse
- Fenstergrösse = Maximale Paketmenge die ohne bestätigung gesendet werden darf
- Sender speichert jedes Paket bis zur bestätigung
- Die Bestätigung enhält Anzahl offene Bytes im Fenster (Bei 0 gibts später eine erneute bestätigung, das wieder Platz frei ist)

Congestion Control

Überlastungsüberwachung (des Netzwerks), Congestion Window wird vom Sender selbst ermittelt. Das kleinere der beiden Fenster (Congestion oder Sliding) ist ausschlaggebend.

- Slow Start: Algorithmus zum ermitteln der Congestion Window grösse.
- Beginnt mit Maximum Segment Size (MSS=1460 Bytes), bei Bestätigung wirds verdoppelt
- Ab einer bestimmten Schwelle (Threshold, Initial 64 KB) nimmt das Fenster nur noch um 1 MSS zu
- Bei einem Timout wird die Schwelle auf 1/2 des Congestion Window und Congestion Window auf 1 MSS gesetzt.

TCP-Header



- Source/Destination Port (je 16 Bits): Sender- und Empfängerport (bezeichnet Applikation auf Serverseite)
- Sequence Number (32 Bits):