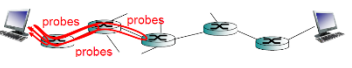


racroute

Misst Weg vom Startshot zum Zielhost
Für alle i:
- Sende Pakete die nur i laufen können richtung Ziel (TTL Feld)
- i.ter Router sendet Pakete zurück -> Sender lernt alle Router kennen - vgl. Breitensuche
Basiert auf ICMP



Home Router Aufgaben
DHCP Server, WLAN Access Point, IP Router, DSL Modem / Kabelmodem, DNS Resolver

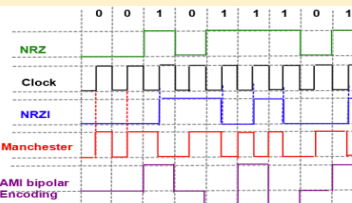
Schichtenmodell (ISO/OSI)

Zusätzlich:
Presentation: Semantik der übertragenen Kommunikation (Kompression, Verschlüsselung, BE, LE)
Session: Sitzungsauf- und abbau Synchronisierung zwischen beteiligten Prozessen

7 application
6 presentation
5 session
4 transport
3 network
2 link
1 physical

Nachteile: Leichter Overhead, teilweise gleiche Aufgaben in mehreren Schichten implementiert (historische Gründe), Höhere Schicht benötigt Infos aus niedrigerer Schicht (z.B. WLAN Routing Protokolle (Schicht3) benötigen Infos aus Schicht2)
Änderungen an Service API Schicht k hat Auswirkungen auf k+1

Baseband Transmission (Leitungscodes)
Manchester: XOR Clock mit Bits
Bipolar: abwechselnd + u. - für jede 1



NRZ
Clock
NRZI
Manchester
AMI bipolar Encoding

Multiplexing (mehrere User 1 Übertragungsmedium)

Frequency Division Multiple Access (FDMA):
- Jeder Benutzer hat eigenen Frequenzbereich
- Bei **Vollduplex** zwingend notwendig!

Time Division Multiple Access (TDMA):
- Frequenzbereich wird über Zeit geteilt
- Round-robin
- Benutzer wechseln sich zeitlich ab

Auch **Kombination** aus beiden Möglich.

Cyclic Redundancy Check (CRC): Ethernet und WLAN
Zu übertragende **Datenbits D**
Generator G, den Sender u. Empfänger kennen (+1Bits)
Sender bestimmt **r zusätzliche Bits** und hängt diese an d an.
d+r wird dann übertragen. **d+r muss durch G teilbar** sein.

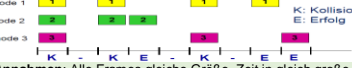
Beispiel:
 $D = 101110, d_{\text{re}} = 0$
 $G = 1001, r = 3$

Sender: R berechnen:
 $R = \text{Rest}(D/2^r / G)$
R gfgs mit führenden Nullen zu r Stellen ergänzen.

Empfänger prüft, ob durch G teilbar
 $D \cdot 2^r \text{ XOR } R = n \cdot G$?
Falls rest übrig bleibt -> Fehler

Funktioniert schlecht, wenn Bitfehler direkt hintereinander

Slotted ALOHA



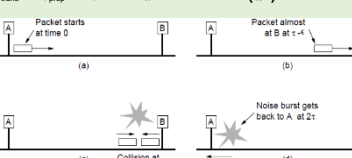
Annahmen: Alle Frames gleiche Größe. Zeit in gleich große Zeitslots unterteilt. Intervall reicht zum Senden des kompletten Pakets. Hosts müssen bzgl Zeit synchronisiert sein.

Sobald neuer Frame vorhanden. Versuche im nächsten Slot zu senden.

- Keine Kollision: fertig.
- Kollision: Versuche beim nächsten Slot mit Wahrscheinlichkeit p erneut. (p-persistent)

Vorteile: nur 1 Host: volle Rate, Dezentral, Einfach
Nachteile: Kollisionen verschwenden Zeitslots. Sync der Uhren notwendig. Hosts erkennen evtl. Kollision bevor Übertragung beendet ist und brechen das Senden ab.

Mindestlänge von Ethernet Frames
Worst-Case: Kollision wird erst nach $2 \cdot d_{\text{prop}}$ erkannt.
Ziel ist es, dass Sender **Kollision noch erkennt, bevor er alle Bits seines Frames losgesendet hat.** (Transmission delay)
=> Minimale Paketgröße nötig
 $d_{\text{trans}} > 2d_{\text{prop}} \Rightarrow L/R > 2 \cdot s/v \Rightarrow L > 2 \cdot R \cdot (s/v)$



(a) Packet starts at time 0
(b) Packet almost at B at t=t+L
(c) Collision at time t
(d) Noise burst gets back to A at 2t

Ethernet Switch
Arbeite auf **Link Layer**.

- Empfang, Zwischenspeicherung und Weiterleitung von Ethernet Frames
- Untersucht MAC Adresse der ankommenden Frames und leitet Frame selektiv nur an richtigen Port weiter.

Klassischer Switch hat **keine IP-Adresse**.

Transparenz:
- Ethernet Hosts merken nichts von der Anwesenheit eines Switches

Plug-and-Play:
- Selbstlernend
- Muss nicht konfiguriert werden.

Leitungsvermittlung (Circuit Switching)
Benötigte Ressourcen müssen vorab reserviert werden
Verbindung wird nur zugelassen, falls ausreichend Netzkapazität vorhanden. Sonst abgelehnt.
Dann Senden eines kontinuierlichen Datenstroms.
Übertragungsrate garantiert.

Paketvermittlung (Packet Switching)
Host teilt Nachricht in kleine Pakete auf und schickt sie unabhängig voneinander los.
Gleichzeitige Pakete müssen sich einen Link teilen und zeitlich hintereinander gesendet werden.
Router: **Store-and-Forward**.
Jeder Router muss gesamtes Paket empfangen, bevor er es auf den ausgehenden Link weiterleitet

Signalübertragung
Dämpfung: Längere Leitung -> mehr Dämpfung
Leistung/Amplituden verringert
Verzerrung: Frequenzen werden von Übertragungsmedien verschieden stark gedämpft.
Meist nur Frequenzen bis zu einem max Wert gut übertragbar
Bandbreite: E-Technik: Frequenzbereich der gut übertragen werden kann

Duplex vs Simplex
Vollduplex: Beide Richtungen gleichzeitig möglich
z.B. meist bei Kabelübertragung
Halbduplex: Beide Richtungen, aber nicht gleichzeitig
z.B. WLAN
Simplex: Nur eine Richtung möglich

Taktrückgewinnung durch Leitungscodes
Häufige Symbolwechsel nötig, damit Empfänger den **Takt rückgewinnen** kann. 100000 schwierig wie viele 0en.
Lösungen:
- Synchronre Uhren
- Manchester Code (Taktfreq = 2 * Bitfreq)
- Codierung: z.B. 4B/5B bildet 4 Bits auf 5 Bits ab mit vielen Wechseln (so bestehen Codewörter niemals nur aus 1en oder 0en)

Data	Code	Data	Code	Data	Code	Data	Code
0000	11110	0100	01010	1000	00010	1100	11010
0001	01001	0101	01011	1001	00011	1101	11011
0010	10100	0110	01110	1010	00101	1110	11100
0011	10101	0111	01111	1011	00111	1111	11101

Weitere Vorteile: Effizientes Ausnutzen der Bandbreite. Gleichspannung unterdrücken (AMI)

Link Layer
Host: Endpunkt eines Ende-zu-Ende Pfades
Node: Jedes Gerät, das am Netzwerk teilnimmt (Host, Router, Switch, Access Point,...)
Frame: Nachricht auf Schicht 2.
Wird in allen Nodes implementiert (**Netzwerkarte/HW**). Nicht in Hubs!

Übertragung von Frames zwischen benachbarten Nodes
Rahmenbildung: Positionsrichtige Erkennung von Zeichen, Erkennung von Blockgrenzen. Frame = Header+Payload.
Payload = IP Paket
Vielfachzugriff: Wer darf Medium wann nutzen?
Fehlererkennung/-korrektur: Umgang mit Bitfehlern auf physical layer. Hinzufügen von Redundanz
Zuverlässige Datenübertragung: Korrektur von Paketverlusten, korrekte Reihenfolge, Vermeidung von Duplikaten. Bei WLAN teilweise, bei Ethernet gar nicht.

MAC-Adressen (Adresse der Link Layer)
Nur lokal gültig. Zur Identifikation von Nachbarn.
Jedes Interface eines Hosts hat eigene MAC-Adresse.
Switch hat keine MAC Adresse, weil kein Host! Bei Ethernet u. WLAN 48 Bit.

Broadcast-Adresse FF-FF-FF-FF-FF-FF

Jede Netzwerkkarte muss eindeutige MAC-Adresse haben innerhalb eines lokalen Netzwerkes.
Teilweise MAC Adresse fest mit Netzwerkkarte verknüpft.


Carrier Sense Multiple Access (CSMA)
Carrier Sensing: Mitlauschen am Kanal.
Kanal frei: Beginne Übertragung.
Kanal belegt: Verschiebe Übertragung.

- **1-persistent:** Sende sobald Kanal wieder frei
- **p-persistent:** Sende im nächsten Slot, mit W'keit p falls Kanal frei ist.
- **Non-persistent:** Warte Zufällige Zeit und prüfe erneut, ob Kanal frei. => **Ethernet**

Wegen d_{prop} erkennen Sender erst verspätet, ob es zu Kollisionen kommt.
 d_{prop} hat Einfluss auf Kollisionswahrscheinlichkeit.

Problem: Bei spät erkannter Kollision ist losgesendetes Paket wertlos.

Vielfachzugriff bei WLAN 802.11
CS: Wie Ethernet wird vor Senden Medium abgehört
Collision Detection nicht möglich, weil:
- WLAN ist **halbduplex**: empf. Signal sehr schwach
- WLAN Stationen können sich nicht gegenseitig hören
=> **Hidden Station Problem**



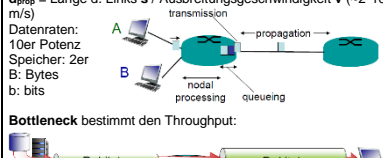
Kollisionen müssen beim Empfänger erkannt werden!

Switch Forwarding
Forwardingtafel enthält Info, an welchen Port ein Frame weitergeleitet werden muss:

- Ziel MAC-Adr | Ziel Ausgangs-port | TTL


Ablauf:
- Selbstlernend: Bei **ankommendem** Frame werden Infos des Absenders gespeichert.- **Nachschlagen**, ob Eintrag mit Ziel MAC schon in Tabelle.
- **Verhanden:** Weiterleiten an Zielport. Falls Zielport == Quellport. Frame verwerfen.
- **Sonst:** Fluten. Weiterleiten an alle Hosts mit Ausnahme des Senders. Auch die, die er schon weiß, was dranhängt.

Paketverzögerungen/-verlust
Verlust: Pakete verworfen, wenn Puffer nicht frei
Verzögerung: durch Pufferung
 $d_{\text{node}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$
 $d_{\text{trans}} = \text{Paketlänge (Bits) } L / \text{Bandbreite } B \text{ (Links (bps) } R$
 $d_{\text{prop}} = \text{Länge } s / \text{Ausbreitungsgeschwindigkeit } v \text{ (~} 2 \cdot 10^8 \text{ m/s)}$



Datenraten:
10er Potenz
Speicher: 2er
B: Bytes
b: bits

Bottleneck bestimmt den Throughput:




Nyquist (Datenrate D bei unverraushtem Kanal)
Bandbreite **B**; Anz. verw. Signalstufen **V**
D = 2 * B * Id (V) [bit/s]

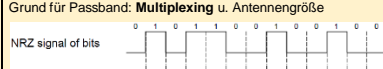
Shannon (Datenrate D bei verrauschten Kanal)
Gilt zusätzlich zu Nyquist!
Nutzsignalleistung S; Rauschleistung N
D = B * Id (1 + S/N) [bit/s]; S/N in dB: $10 \cdot \log_{10}(S/N)$
Wenn in dB geg., dann erst umrechnen

Bit vs Baud
Bitrate:
20 bit/s

Baudrate (Anz. Signalschritte pro Sekunde):
10 Baud



Passband Transmission
Nutzsignal ändert Trägersignal
Bei Frequency Vereinbarung welche Freq 0 und 1
Grund für Passband: **Multiplexing** u. Antennengröße



NRZ signal of bits


Amplitude shift keying

Frequency shift keying

Phase shift keying

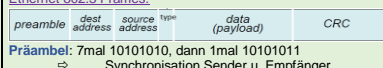
Rahmenbildung (Zerlegung des Bitstroms in endliche Seq)
Erkennung, wann Frame beginnt und endet.

Byte Count: Zu Beginn jedes Frames Feld, das Anz. enthaltener Bytes angibt (Anz. inkl. diesem Feld)
Nachteil: Nach Fehler erneute Synchronisation schwer
Byte Stuffing: FLAG markiert anfang und Ende. Falls FLAG in Nutzdaten, ESC aber auch escapen. Overhead, aber einfaches Synchronisieren nach Fehler.



Bit Stuffing: Frame beginnt mit speziellen reserviertem Bitmuster. Beim senden wird nach 5 zusammenhängenden 1-er Bits immer ein 0 Bit eingefügt und beim Empfang nach 5 zusammenhäng. 1er Bits immer ein 0 Bit gelöscht.
Vorteil: Framelänge muss kein vielf. von 8Bit sein.

Ethernet 802.3 Frames:



Präambel: 7mal 10101010, dann 1mal 10101011
=> Synchronisation Sender u. Empfänger

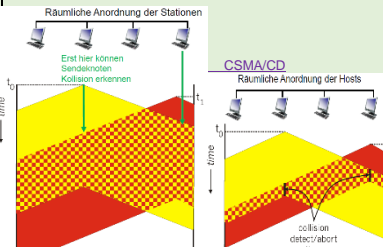
Adressen: je 6 Byte Sender u. Empfänger MAC. Normalerweise, NW Karte leitet Frame nur an BS weiter, wenn des adresse passt. Ausnahmen: Broadcast oder Promiscuous Mode

Type: 2Byte Art des Netzwerkprotokolls IPv4/IPv6...

CRC: 4Byte

Eigenschaften:
Verbindungslos: Kein Verb. Aufbau vor Datenaustausch
keine zuverlässige Verbindung: Frameverlust mögl.
Vielfachzugriff: Nur bei Punkt-zu-Punkt: Unsl CSMA/CD

CSMA



Räumliche Anordnung der Stationen

CSMA/CD

Räumliche Anordnung der Hosts

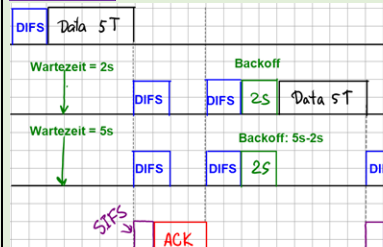
CSMA/CA (Collision Avoidance) bei WLAN
Sender: Kanal min. für **DIFS** frei -> sende kompletten Frame ohne CS

Kanal belegt:
- hier schon exponential Backoff
=> Unterschied zu CSMA/CD
- Höre Kanal ständig ab und dekrementiere Timer nur während Zeiten, wo Kanal frei ist.
- Erneute Übertragung, wenn Timer ausläuft

Falls kein ACK eintrifft -> Wieder zu belegt Fall. Gfgs backoff Intervall erhöhen.

Empfänger: bestätigt Datenempfang durch ACK nach Zeitspanne SIFS.
SIFS < DIFS Priorisierung von ACK

CSMA/CA Ablauf:



DIFS Data 5T

Wartezeit = 2s Backoff

Wartezeit = 5s Backoff: 5s-2s Backoff rest

SIFS -> ACK

Schichtenmodell (TCP/IP - Internet)

Vorteile: Verringert Gesamtkomplexität. Einfacheres Hinzufügen neuer Features, modulares Entwickeln von für die Datenkommunikation benötigter Hardware, Treiber und Anwendungen. Schichten können geändert werden, ohne Einfluss auf andere Schichten.

Jede Schicht fügt an die Nachricht ihren eigenen Header hinzu

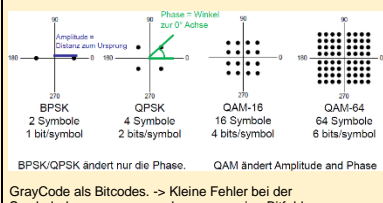
5 Application (HTTP, SMTP, RTP, DNS)
4 Transport (TCP, UDP): Kommunikation zw. Prozessen auf Sender u. Empfängerseite
3 Network (IP, ICMP): Adressierung, Forwarding, Routing
2 Link (DSL, SONET, 802.11, Ethernet): Rahmenbildung, Fehlererkennung/Korrektur, Vielfachzugriff, zuverl. Datübertr
1 Physical: Signalübertragung, Modulation, Übertragungsmedien

Digitale Modulation
Modulation: Umwandlung Bitsequenz in übertragbares Signal.
Demodulation: Rückübersetzung beim Empfänger.

Baseband (bei drahtgebundener Übertragung):
Signal beinhaltet Frequenzen 0 bis fmax und wird direkt in diesem Frequenzbereich übertragen.
Bei Ethernet Kabel z.B. 100BaseT bedeutet: 1Gps, Baseband, Twisted Pair Kupferleitung

Passband (bei drahtloser Übertragung):
Nutzsignal in höheren Frequenzbereich verschieben
Nutzsignal verändert Trägersignal
Rückgewinnung am Empfänger durch **Demodulation**

Passband: Kombination von Modulationsarten
ASK und PSK oft kombiniert -> ergibt mehr Symbole, daher höhere Bitrate bei gleicher Baudrate



BPSK 2 Symbole 1 bit/symbol
QPSK 4 Symbole 2 bits/symbol
QAM-16 16 Symbole 4 bits/symbol
QAM-64 64 Symbole 6 bits/symbol

GrayCode/QPSK ändert nur die Phase. QAM ändert Amplitude und Phase

GrayCode als Bitcodes. -> Kleine Fehler bei der Symbolerkennung verursachen nur wenige Bitfehler.

Fehlererkennung und -korrektur
Keine Fehlerkorrektur (zu viel Redundanz)
Bei Fehlererkennung:
Ethernet: keine Retransmission. Nur durch TCP, falls Timeout eintritt.
WLAN: Aktive Wiederanforderung des fehlerhaften Blocks durch Link Layer

Checksumme (IP und UDP/TCP Header):
- Bits in Gruppen von 16 Bit Wörtern
- Summiere alle 16 Bit Wörter unter Berücksichtigung des Übertrags (Übertrag addieren)
- 1er Komplement des Ergebnisses ist Checksum Empfänger:
- Addiere übertragene Wörter UND Checksum. Übertrag auch wieder addieren!
- Wenn Ergebnis nur 1er: Kein Fehler

Vielfachzugriff
Geteilter Broadcastkanal - **Interferenz** == Kollision falls mehrere Stationen gleichzeitig senden.

Multiple Access Control: Verteilter Algorithmus, der entscheidet, wann Host senden darf. Entscheidung muss inband sein (kein extra Kanal).
Link hat Kapazität R. Wenn einer, dann Rate R, wenn mehrere Senden Rate R/M

Arten von Multiple Access Control:
Multiplexverfahren: siehe physical Layer.
Random Access Verfahren: Kollisionen (>2 Stationen senden) werden zugelassen. Mechanismen um sich von Kollision zu erholen. z.B. Un-/Slotted ALOHA, CSMA/CD/CA
Token-Verfahren: Kollisionen werden verhindert. Nur wer Token hat darf auf Kanal zugreifen


CSMA/CD (Carrier Sensing + Collision Detection)
CS: Nur senden falls Medium gerade frei ist.
CD: Sender (**Netzwerkarte**) hört während senden Medium weiter ab.

- Sofortiger Abbruch + Jam Signal bei Kollision. Jam Signal zum Sicherstellen, dass andere Nodes Sendetätigkeit einstellen.
- Erneuter Sendeveruch nach zufälliger Wartezeit
- Binary exponential Backoff: mittlere Wartezeit nach jeder erneuten Kollision verdoppelt.

Voraussetzung:
Sender muss zu **listen while talk** fähig sein.
- LAN: Leicht möglich -> **Vollduplex**
- WLAN: Schwierig. Empfangene Signale viel schwächer als gesendete -> **Halbduplex**

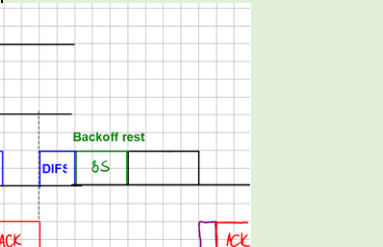
Switched Ethernet
Hub: Alle Leitungen quasi miteinander verbunden. Eine einzige Kollisionsdomäne. CSMA/CD notwendig
Switch: Isoliert jeden Port in eigene Kollisionsdomäne
Bei Vollduplex-Kabeln kein CSMA/CD nötig

- Jeder Host direkt mit Switch-Port verbunden.
- Keine Kollision möglich, falls voll-duplex.
- Kein CSMA/CD notwendig.
- Switches speichern Frames zwischen und leiten Frames weiter
- Gleichzeitige Übertragung von A zu A' und B zu B' möglich.



Kollisionsdomäne

CSMA/CA Ablauf:



DIFS Data 5T

Wartezeit = 2s Backoff

Wartezeit = 5s Backoff: 5s-2s Backoff rest

SIFS -> ACK

TODO: letztes Thema

Abkürzungen

Einführung

DSL: Digital Subscriber Line

ISP: Internet Service Provider

TCP: Transmission Control Protocol (Netzwerkprotokoll, das definiert auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen)

UDP:

IP: Internet Protocol (Protokoll das die Grundlage des Internets darstellt)

HTTP: Hypertext Transfer Protocol (Protokoll zur Übertragung von Daten in der Anwendungsschicht)

RFC: Request for Comments (legt Internet Standards fest)

VoIP: Voice over IP

DSLAM: Digital Subscriber Line Access Multiplexer (übersetzt hochfrequente Töne in digitale Signale, bevor Daten zum Modem im Heimnetz kommen)

CMTS: Cable Modem Termination System (Wie DSLAM aber für Kabelmodem)

DHCP Server: Dynamic Host Configuration Protocol Server (Verteilt automatisch Adressen an Hosts in einem Netzwerk)

DNS Server: Domain Name System Server (Weist im Internet einer URL die richtigen IP-Adresse zu)

SAP: Service Access Point (Im Schichtenmodell stellt jede niedrigere Schicht der jeweils höheren Schicht einen SAP zur Verfügung. Somit kann die Höhere Schicht die Services der niedrigeren benutzen)

ISO: International Organization for Standardization

OSI: Open Systems Interconnection

Network Layer

CIDR: Classless Interdomain Routing (Subnetzteil einer Adresse kann beliebige Länge haben)

Windows/Linux Befehle

Messen der Round Trip Time:

- Windows: ping

Wege eines Pakets durch das Internet verfolgen:

- Windows: tracert
- Linux: traceroute

Routing Tabelle anzeigen:

- Linux: route
- Windows: route print

MAC-Adresse rausfinden:

- Windows: ipconfig /all -> physische Adresse
- Linux: ifconfig -> ether, oder ip addr

MAC-Adresse ändern:

- Windows: Systemsteuerung -> Geräte manager

Adresszuweisung

- Linux: ifconfig eth0 200.23.16.4 netmask 255.255.255.0 oder ip addr add 200.23.16.4/24 dev eth0 oder persistent: /etc/network/interfaces
- Windows: Systemsteuerung -> Netzwerk- und Freigabecenter -> Adaptereinstellungen

IP Adresse von DHCP Server anfordern

- Linux: dhclient
- Windows (ipconfig /release)

ARP-Tabellen anzeigen

- Linux: arp
- Windows: arp -a

nmap – Portscanner, scannt auf offene Ports im Netzwerk

TCP Verbindungen anzeigen:

- Windows: netstat -p tcp

TODO

Schichtenmodell Aufgaben

Winwos/Linux Befehle