Rechnernetze

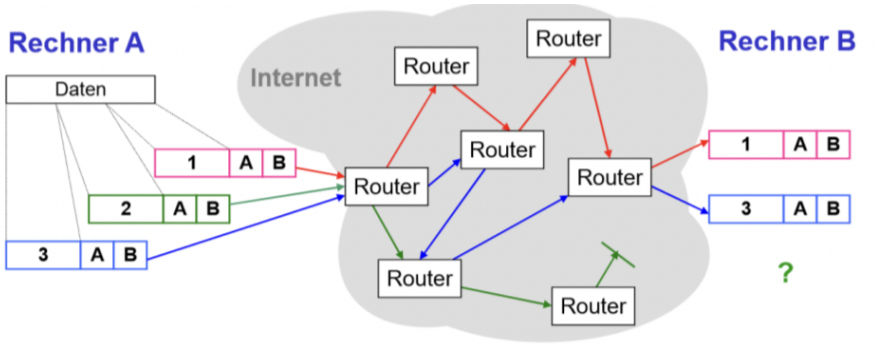
github/bircni

Inhaltsverzeichnis

1 Einleitung

1.1 Datenübertragung im Internet

- Die Bitübertragungsschicht
  - Bit wird in Form physikalischer Signale übertragen
  - Übertragungsmedien
    - Kupferkabel - elektrische Signale
    - Glasfaserkabel - Lichtpulse (Itensität)
    - Funkwellen - Amplitude, Frequenz
  - Problem: Übertragungsfehler wegen Signalverfälschung
- Die Sicherungsschicht
  - Verantwortlich für zuverlässigen Datenaustausch zwischen direkt verbundenen Rechnern
  - Möglichkeiten: Punkt zu Punkt, Bus, Stern
  - Aufgaben:
    - Framing: Generierung der Datenpakete
    - Fehlererkennung: Generierung der Prüfsummen
    - (Bus)Media-Access-Control (MAC): Wer darf wann senden?
    - (Stern)Hardware-Adressierung: Eindeutige Adressierung der Interfaces
- Die Vermittlungsschicht (IP)
  - IP ist optimiert für Datenübertragung über heterogene, nicht zuverlässige Netzwerke
    - Übertragung erfolgt in Form unabhängiger Pakete
    - Einheitliches, übergreifendes Adressschema
    - Keine Mechanismen zur Fehlerbehebung
- Die Transportschicht (TCP)
  - Ziel:
    - Zuverlässigkeit des Datentransports
    - Sicherung der Übertragung zwischen Anwendungsprozessen



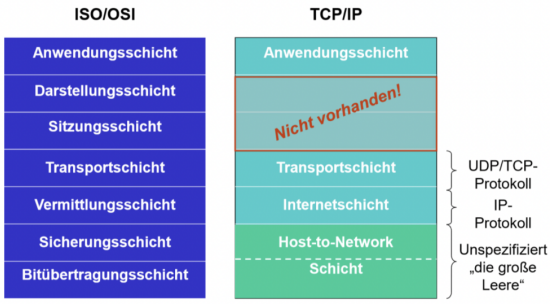
- TCP:
  - Anwendung übergibt Daten an die TCP-Schicht
  - korrekter Transport als Aufgabe von TCP

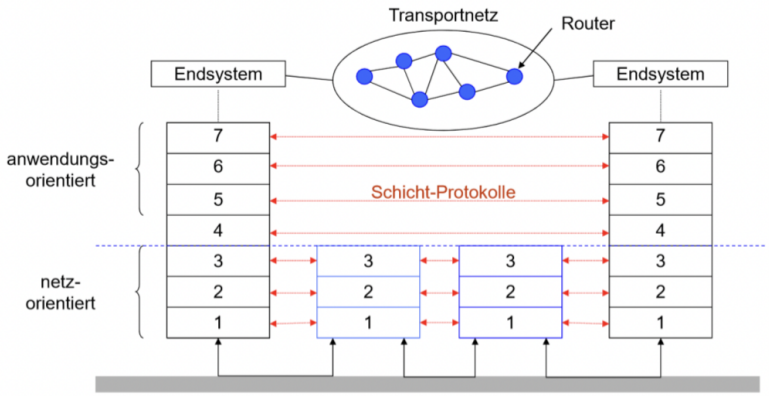
1.2 ISO/OSI-Modell

- 7 Schichten
- Jede Schicht definiert Funktionen die als Dienste der nächst höheren Schicht zu Verfügung stehen
- keine Implementierungsvorgaben
- höhere Schicht nutzt die Funktionen der darunter liegenden Schicht
- Prinzip: "Information Hiding"
- Grobstruktur:
  - Schicht 1-3: Netz orientiert, reine Transportfunktionalitäten, Inhalt irrelevant
  - Schicht 4: Verbindet die Netz- und Anwendungsschicht
  - Schicht 5-7: Anwendungs orientiert, Festlegung des Datenaustauschs und Datenformats

7	Anwendungsschicht
6	Darstellungsschicht
5	Sitzungsschicht
4	Transportschicht
3	Vermittlungsschicht
2	Sicherungsschicht
1	Bitübertragungsschicht

- Funktionen der Schichten:
  1. Bitübertragungsschicht: (Bit-Repräsentation)
     ermöglicht die Übertragung unstrukturierter Bitsröme; z.B. physikalische Darstellung
  2. Sicherungsschicht: (Ethernet)
     dient zur Entdeckung von Übertragungsfehlern und deren Korrektur
  3. Vermittlungsschicht: (IP)
     ermöglicht transparente Übertragung der Daten im Netzwerk (Routing)
  4. Transportschicht: (TCP)
     Sicherung der Übertragung zw. zwei Anwendungen auf versch. Rechnern
  5. Sitzungsschicht: (Dialog-Steuerung)
     sorgt für Synchronisation und den geregelten Dialogablaug zw. zwi Anwendungsprozessen (Login)
  6. Darstellungsschicht:
     Umsetzung der Darstellungen der Informationen
  7. Anwendungsschicht:
     einzige Zugriffsmöglichkeit der Anwendungsprozesse zur Datenübertragung (Mail,DNS)





2 Datenübertragung

2.1 Fourieranalyse

Jede periodische Funktion g(t) mit t (Zeit) und Periode T kann als Überlagerung von Sinus- und Cosinustermen dargestellt werden.

$$g(t) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} [a_n cos(\omega_n t) + b_n sin(\omega_n t)]$$

a_n und b_n sind Fourierkoeffizienten mit $\omega_n = 2\pi n/T$
Der n-te Summand heißt n-te Harmonische.
Ist g(t) der Spanungsverlust eines elektr. Signals dann ist $(a_n^2 + b_n^2)$ proportional zur Leistung, die bei der Frequenz f_n übertragen wird.
Beispiel-Applet: `https://falstad.com/fourier`

2.2 Dämpfung D

Üblicherweise wird die Dämpfung in der Einheit Dezibel angegeben

$$D_{dB} = 10 * \log_{10}(P_{in}/P_{out})[dB]$$

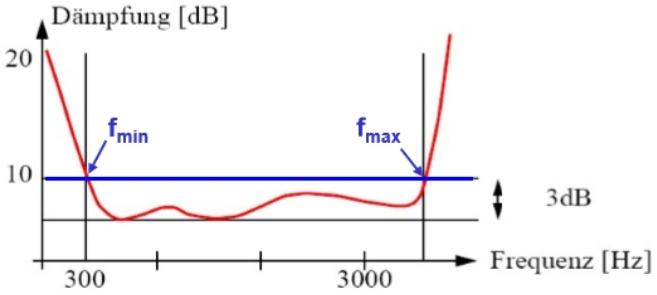
$$D_{dB} = 20 * \log_{10}(U_{in}/U_{out})[dB]$$

→ Unabhängig davon ob Leistung [P] oder Spannung [U] verglichen werden ergibt sich bei der Formel der gleiche Wert. Wird als Einheit dB verwendet, addieren sich die Dämpfungen einzelner Abschnitte.

2.3 Bandbreite B

Bandbreite eines Übertragungskanals $B = f_{max} - f_{min}$

- Frequenzbereich der ohne wesentl. Dämpfung übertragen werden kann.
- f_{max} und f_{min} sind dadurch gegeben, dass die außen liegenden Frequenzen unter 50% der leistungsstärksten Frequenzen liegen.



2.4 Nyquist-Theorem

Zusammenhang zwischen Bandbreite B und der maximal möglichen Datenrate D eines idealen Übertragungskanals:

$$D = 2 * B * \log_2(N)$$

→ B = Bandbreite des Übertragungskanals in [Hz]
→ N = Anzahl der möglichen diskreten Signalstufen pro Signaländerung
→ D = Datenrate in bps (Bit pro Sekunde)

Beispiel:

- Binäres Signal mit N=2 und Übertragungskanal mit 3000Hz → maximal erreichbare Datenrate beträgt 6000 bps

2.5 Shannon'scher Kanalkapazitätssatz

- Maximale Datenrate eines realen Datenkanals
  - D hängt vom "Signal-Rausch"-Abstand (SNR) ab
    $D = B * \log_2(1 + SNR)$
    → B = Bandbreite des Übertragungskanals in [Hz]
    → $SNR = P_S/P_R$
    P_S = mittlere Leistung im Nutzsignal
    P_R = mittlere Leistung im Rauschsignal
  - Die gebräuchliche Einheit von SNR ist [dB]
    → $(SNR)_{dB} = 10 * \log_{10}(SNR)$
- Beispiel
  - Übertragungskanal mit 3000 Hz (Telefon); $(SNR)_{dB} = 30dB$
    → $SNR = 1000$
    → $D = 3000 * \log_2(1 + 1000) \approx 30000bit/s$

2.6 Bitrate vs. Signalgeschwindigkeit

- Signalgeschwindigkeit: Anzahl der Signalwechsel pro Sekunde

- Die Signalgeschwindigkeit wird in Baud [Bd] angegeben
- Oft auch als "Baudrate" bezeichnet

- Bit-Rate: Anzahl der übertragenen Bits pro Sekunde
  - Die Bitrate kann größer als die Baudrate werden
  - Für binäre Signalstufe (2-Stufen-Kodierung) gilt: Bitrate = Baudrate
  - Bei Nutzung einer 4-Stufen-Kodierung gilt: Bitrate = 2x Baudrate

2.7 Die Ende-zu-Ende-Verzögerung von Datenpaketen

- Zeit: Datenpaketübertragung von Quell-Knoten zu Ziel-Knoten
- Verzögerungsarten die zur Verzögerung beitragen:

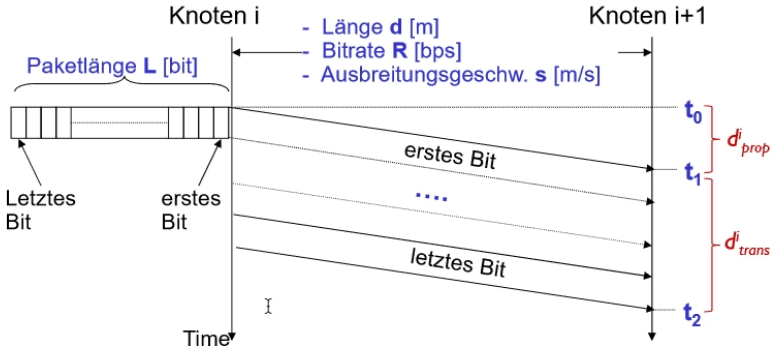
$$d_{end-to-end} = \sum_{i=1}^{N} d^j_{nodal}$$

  - d^j_{nodal} bezeichnet die Verzögerung in einem Knoten i
  - Die Knoten-Verzögerung d^j_{nodal} setzt sich aus folgenden Anteilen zusammen:

$$d^j_{nodal} = d^j_{proc} + d^j_{queue} + d^j_{trans} + d^j_{prop}$$

    * d^j_{proc} = Verarbeitungsverzögerung (processing delay)
    * d^j_{queue} = Warteschlangenverzögerung (queuing delay)
    * d^j_{trans} = Übertragungsverzögerung (transmission delay)
    * d^j_{prop} = Ausbreitungsverzögerung (propagation delay)

- *Die Übertragungsverzögerung d^j_{trans} und die Ausbreitungsverzögerung d^j_{prop}*



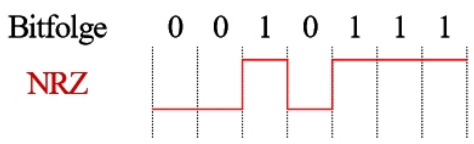
$t_1 - t_0$ = Ausbreitungsverzögerung = **d** [m] / **s** [m/s]
$t_2 - t_1$ = Übertragungsverzögerung = **L** [bit] / **R** [bps]

2.8 Grundlegende Übertragungstechniken

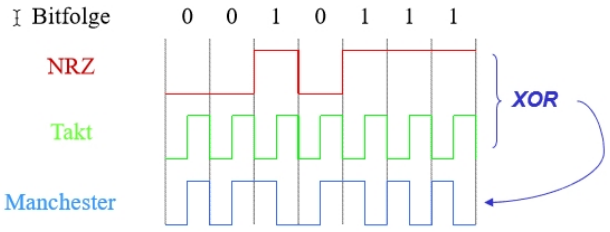
- Digitale Eingabe, digitale Übertragung:
  Digitale Leitungscodierung
  - Beispiel: Ethernet
    → Bits werden direkt als digitale Signale auf die Leitung gegeben
    → Einsatz sog. Basisband-Übertragungsverfahren
- Digitale Eingabe, analoge Übertragung:
  Modulationstechniken
  - Beispiel: DSL-Modemstrecken
    → Binäre Daten werden über eine Trägerwelle übertragen
    → Einsatz sog. breitband-Übertragungsverfahren

2.9 Digitale Leitungscodierung

- Direkte Übertragung rechteckförmiger Signale
  - Signal belegt gesamte verfügbare Bandbreite des Übertragungskanals
- Die Zuordnungsvorschrift Datenelement zwischen Signalelement heißt Signal- oder Leitungscodierung
- Die sich ergebende Signaverläufe heißen Signalcodes oder Übertragungscodes
- Erwünschte Eigenschaften von Übertragungscodes:
  - Bittaktrückgewinnung
  - Codierung mehrerer Bits pro Baud (pro Signalwechsel)
  - Vermeidung von Gleichstromanteilen
  - Erkennung von Signalfehlern auf Signalebene
- Beispiele:
  - *NRZ (Non Return to Zero)-Codes:*
    - *Fester Pegel während eines Bitintervalls, Signalwechsel an Intervallgrenzen*
      → *Max. 1 Signalwechsel pro Bit*
      → *Vorteil: einfach zu implementieren*
      → *Nachteil: Gleichstromanteile und Synchronisationsprobleme bei langen „0“-Folgen*



- *Manchester-Codierung*
  - *XOR-Verknüpfung von NRZ-Kodierung mit internem Taktsignal*
    - → *Codierungsvorschrift: „1“ ⇒ Übergang high/low in der Intervallmitte*
      „0“ ⇒ Übergang low/high in der Intervallmitte
    - → *Effizienz nur 50%: Verdoppelt Baudrate gegenüber NRZ*
      (→ betrachte lange „1“- oder „0“-Folgen…)
    - → *Jedoch keine Gleichstromanteile; gute Synchronisationseigenschaften*
    - → *Eingesetzt bei Ethernet (10 Mb)*

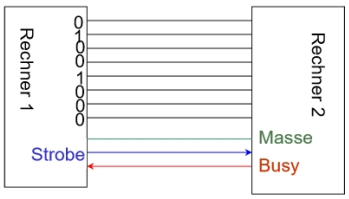


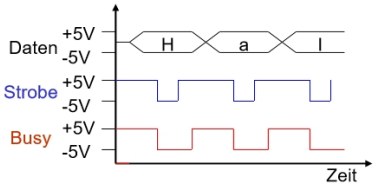
- *4B/5B-Kodierung*
  - *Ziel: Ineffizienz der Manchester-Kodierung umgehen, ohne längere Gleichstromanteile zu erzeugen*
  - *Verfahren: Umkodierung der Daten gemäß 4B/5B-Code und Übertragung gemäß NRZI-Signalcode*
    - → *NRZI-Signalcode verhindert lange „1“-Level-Folgen:*
      1= Übergang in der Intervallmitte
      0= kein Übergang
    - → *4B/5B-Codierung vermeidet lange “0”-Folgen:*
      nie mehr als eine führende Null,
      nie mehr als zwei nachgestellte Nullen
    - → *Effizienz 80%*
  - *Eingesetzt z.B. bei FastEthernet über Glasfaser oder FDDI*

4-Bit Daten	5 Bit Code
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

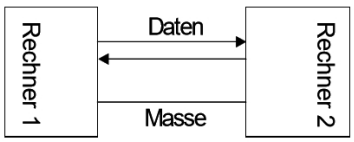
Übertragungsarten

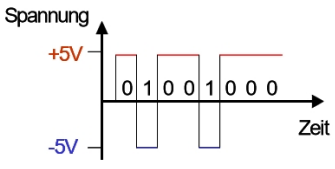
Parallele Übertragung





Serielle Übertragung





- Synchronisation bei Bit serieller Übertragung
  - Beispiel "RS-232-C"-Schnittstelle
    - Standart-Schnittstelle zur Übertragung alphanum. Zeichen
    - Sender und Empfänger sind vor Datenaustausch nicht synchronisiert
      → Sender-/Empfängertakt müssen gleich sein
      → Start/Stop-Verfahren - Signalisierung von Anfang/Ende einer Übertragung
      → Sender-Verhalten:
      Übertragung von Daten beginnt, sobald Daten anliegen, beliebige Wartezeiten
      → Empfänger-Verhalten:
      Ständige Empfangsbereitschaft
    - Spezifikationen
      → "1" Signalpegel von -3V bis -15V
      → "0" Signalpegel von +3V bis +15V
      → Start-Bit setzt Leitung auf "0" und startet Taktgeber des Empfängers
      → Stop-Bit setzt Leitung auf "1"

- Modulationstechniken
  - Nutzung elektromag. Wellen zur Datenübertragung
    - Träger wird vom Sender moduliert
    - Empfänger demoduliert Träger und rekonstruiert Originaldaten
  - Amplitudendarstellung einer Trägerwelle

$$A(t) = A_0 * sin(2\pi ft - \phi)$$

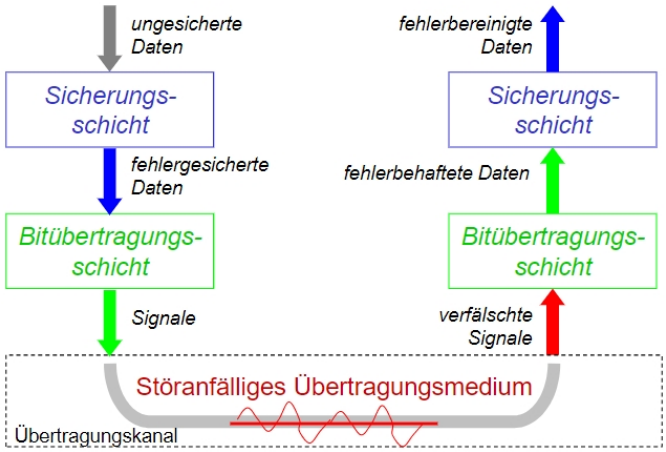
A_0: Amplitude; ϕ: Phasenverschiebung;
$f = 1/T$ =Frequenz; T =Schwingungsperiode;

3 Die Sicherungsschicht und lokale Netze

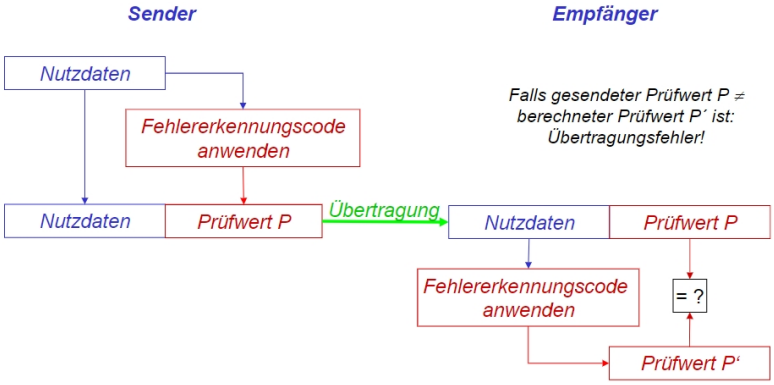
Aufgaben der Sicherungsschicht:

- Bereitstellung einer logischen Verbindung zwischen direkt verbundenen Kommunikationssystemen
- Zuverlässige Zustellung von Daten für die Vermittlungsschicht
  Bereitstellung einer Dienstschnittstelle
  Sicherung der Daten vor Verfälschung bei Übertragung

Funktion der Sicherungsschicht:



Ablauf der Fehlererkennung:



3.1 Rahmenbildung und Fehlererkennung

3.1.1 Rahmenbildung

Zur Fehlererkennung werden Bitströme in kleine Dateneinheiten aufgeteilt (Rahmen).
Wie erkennt der Empfänger Anfang und Ende des Rahmens?
Das Format des Rahmens hängt von der Netztopologie ab (Ethernet, Token Ring, ATM)
Erkennung von Rahmengrenzen:

- Verwendung illegaler Codezeichen auf Bitübertragungsbene
  z.B. Manchester-Codierung: kein SIgnalübergang in der Mitte eines Intervalls
- Längenangabe im Rahmen-Header: Byte-Zählmethode
- Verwendung von speziellen Steuerzeichen: Byte-Stopfen
  Spezielle ASCII-Zeichen werden als Steuerzeichen benutzt (SOH,EOH)
  In den Daten können zufällig Steuerzeichen auftreten

3.1.2 Fehlererkennung

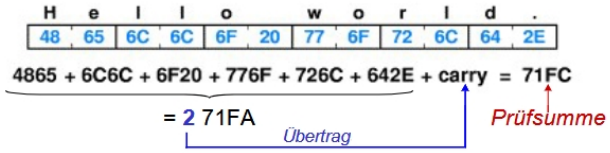
Aufteilung der Daten in einzelne Rahmen durch den Sender
Pro Rahmen wird eine redundante Zusatzinfo geschickt → Empfänger kann Übertragungsfehler erkennen
Hamming-Distanz:

- Erlaubt die Bewertung von Fehlercodes
- Definition:
  Distanz zwischen 2 zulässigen Wörtern (Anzahl unterschiedlicher Bitpositionen)
  Hamming-Distanz ist die minimale Distanz zweier bel. Wörter einer Codierung
- Regeln:
  Für die Erkennung von d Bitfehlern muss die Hamming-Distanz $d+1$ sein
  Für die Behebung von d Bitfehlern muss die Hamming-Distanz $2d+1$ sein

Fehlererkennungscodes:

- Eindimensionale Parität
  Übertragung eines zusätzlichen Bits zu jedem Wort der Länge d Bit
  → Ungerade Parität (d+1)tes Bit wird auf 1 gesetzt, wenn Anzahl der 1sen im d-Bit Wort gerade
  → Gerade Parität (d+1)tes Bit wird auf 1 gesetzt, wenn Anzahl der 1sen im d-Bit Wort ungerade
- Zweidimensionale Parität
  Zusätzliche Paritätsberechnung für jeweilige Bit-Position

- Internet-Prüfsummen
  Sender interpretiert Nutzdaten als Folge von Ganzzahlen und berechnet die Summe
  - *Beispiel einer 16-Bit Prüfsumme: Übertragung von „Hello World“*

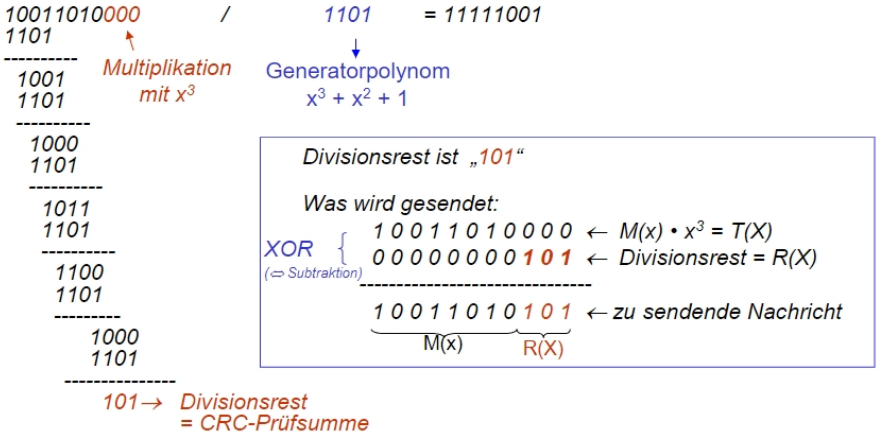


  - *Fehlererkennungswahrscheinlichkeit des Verfahrens*
    → *Besser als Paritätsprüfung; problematisch sind systematische Fehler!*

Daten	Dezimal	Daten	Dezimal
00001	1	00011	3
00010	2	00000	0
00011	3	00001	1
00001	1	00011	3
Prüfsumme	7	Prüfsumme	7

- Cyclic Redundancy Check (CRC)
  1. *Nachricht (Nutzdaten) habe Länge von (n+1) Bits, also z.B. 8-Bit Nachricht 10011010 mit n=7*
     - Darstellung der Nachricht als Polynom n-ten Grades M(x):
     $M(X) = 1 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0$
  2. *Sender und Empfänger einigen sich vor Übertragung auf ein Divisor-Polynom C(x), auch Generator-Polynom genannt, vom Grad k.*
     - z.B. k=3: $C(x) = 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$ *(entspricht 1101)*
  3. *Statt M(x) wird eine Nachricht P(X) vom Grad n+k gesendet (entspricht also n+k+1 zu übertragenden Bits)*
     - die zusätzlichen k Bits sind die Fehlererkennungsbits
     - die k Bits werden so gewählt, dass das korrespondierende Polynom P(x) durch C(x) ohne Rest teilbar ist
  4. *Empfänger dividiert empfangene Nachricht P(x) durch C(X)*
     - verschwindet Divisionsrest → Datenübertragung erfolgte korrekt
     - die Nachricht besteht aus den höchstwertigen n+1 Bits von P(x)

Beispiel: CRC-Berechnung bei Sender



3.2 Prinzipien der gesicherten Datenübertragung

Grundprinzip der gesicherten Übertragung:

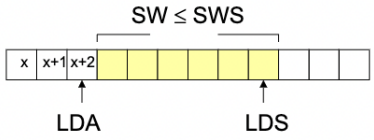
- Prinzip der positiven Bestätigung (ACK+):
  erfolgreicher Erhalt wird mit einem "ACK+"-Paket bestätigt
  Nach Versand des Pakets wird auf das ACK+ gewartet
  Falls Wartezeitüberschritten, erfolgt Sendewiederholung
- Sendepuffer
  Datensegmente können verloren gesicherten
  Sender muss eine Kopie der Daten halten
- Sequenz- & Bestätigungsnummern:
  Datensegmente können verdoppelt werden
- Problem:
  Je nach Ausbreitungsverzögerung sehr geringe effektive Übertragungsrate

Funktionsweise von Sliding-Window-Protokollen:
Bei ACK wird die Übertragungskapazität schlecht ausgenutzt
Jetzt: Sender schickt mehrere Frames, ohne auf ACKs zu warten

- *Sender verwaltet*
  - *einen Sendepuffer der Größe SWS (Send Window Size)*
  - *eine Variable SW*

- Es muss gelten:
$SW = LDS - LDA \leq SWS$

Last Datasegment Sent — Last Datasegment Acknowledged



Bezeichnungen:

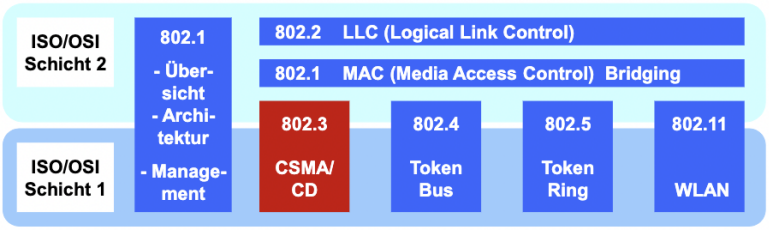
LDA: Sequenznummer des letzten bestätigten Datensegments

LDS: Sequenznummer des zuletzt gesendeten Datensegments (also noch nicht bestätigt)

Varianten von Sliding-Window-Protokollen:

- "Go-Back-n"-Strategie: RWS = 1
  Empfangspuffer des Empfängers kann genau ein Datensegement zwischen puffern
- "Selective Repeat"-Strategie: RWS $\leq$ 1
  Empfangspuffer des Empfängers kann mehrere Datenrahmen zwischen puffern

3.3 Ethernet (IEEE 802.3)



- *802.1 : Zusammenhang der Standards und MAC Bridging*
- *802.2 : Logical Link Control-Dienste und -Protokolle*
- ***802.3 : CSMA/CD-Protokoll für Bus-Topologie (→ Ethernet)***
- *802.4 : Token Bus-Protokoll auf Bus-Topologie*
- *802.5 : Token Ring-Protokoll auf Ring-Topologie*
- *802.11: Wireless LAN*
- *802.15(.4): Wireless Personal Area Networks (Zigbee)*

3.3.1 Ethernet-Funktionsprinzip

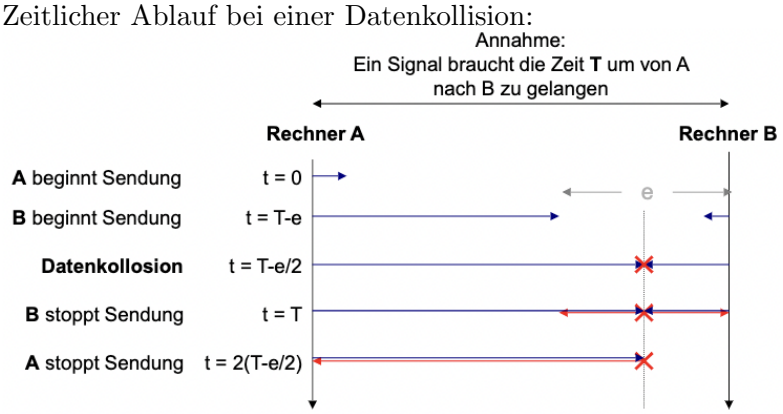
Alle Teilnehmer eines LANs teilen sich die Übertragungskapazität **"shared network"**
Alle Stationen "sehen" alle Daten-Rahmen im LANs
CSMA/CD: Medienzugriffsprotokoll für Ethernet

CSMA/CD: Carrier Sense Multiple Access/Collision Detect

Ablauf:

Sendewilige Station hört Leitung
Bei freier Leitung wird gesendet
Während der Sendung wird überwacht, ob Datenkollision auftritt
Bei Kollision: Sendung wird abgebrochen

Zeitlicher Ablauf bei einer Datenkollision:



Der Konfliktparameter K:

$$K = \frac{\text{doppelte max. Signallaufzeit}}{\text{min. Nachrichtenübertragungsverzögerung}}$$

entspricht RTT_{max}!

$$\text{min. Nachrichtenübertragungsverzögerung} = \frac{\text{min. Nachrichtenlänge [bit]}}{\text{Übertragungsrate [bps]}}$$

- $K>1$
  - Komplette Nachricht kann gesendet werden, bevor Kollision erkannt wird
  - Für CSMA/CD nicht praktikabel !
- $K \leq 1$
  - Für CSMA/CD praktikabel
  - Daraus resultiert Limitierung der Kabel-Länge

3.3.2 MAC (Ethernet)-Adresse

Länge: 6 Bytes bzw. 48 Bits
Broadcast-Adresse: Alle Bits der LAN-Adresse sind auf 1 gesetzt

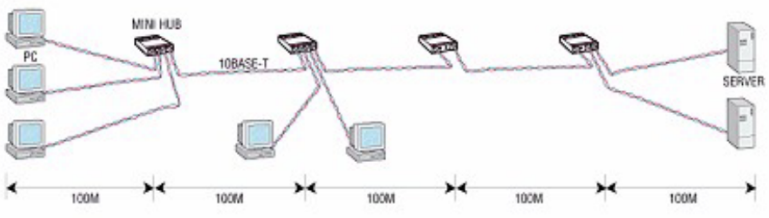
3.3.3 Funktion eines Ethernet-Adapters

Der Ethernet-Adapter überprüft jeden gesendeten Rahmen (Hardware)
Wenn die Ziel-MAC-Adresse eines Rahmen = der lokalen MAC-Adresse des Adapters:
Rahmen wird an das Betriebssystem weitergeleitet
Ausnahme: Promiscuous Mode oder MAC-Broadcast

3.3.4 Netzwerkkomponenten

- Ethernet-Repeater:
  - Zweck
    Längenbeschränkung aufgrund von Signaldämpfung aufheben
    Kopplung gleichartiger Netsegmente
  - Funktion
    Arbeitet auf der Bitübertragungsschicht
    Verstärker wird zwischen zwei Segmente geschaltet
- Ethernet-Hubs
  - Zweck ähnlich wie von Repeatern
    Repeater koppeln Segmente - Hubs bilden den zentralen Bus eines Segments
  - Funktion
    Hubs arbeiten auf der Bitübertragungsschicht
    Das Gesamtnetz bildet eine Kollisionsdomäne
- "Repeater"-Regeln
  Anzahl der kaskadierbaren Hubs/Repeater ist begrenzt (max. 5 Segmente durch

4 Hubs/Repeater)



- Ethernet-Bridges
  - Kopplung zweier Ethernet-Segmente mit folgenden Eigenschaften
    Geschwindigkeitskonversion und Aufhebung der Repeater-Regeln
  - Funktion
    Bridges sind Geräte der ISO/OSI-Schicht 2 (Bit-/Sicherungsschicht)
    Bridges entkoppeln Kollisionsdomänen
- "Multiport"-Bridge
  Bridge mit mehr als zwei LAN-Schnittstellen
  enthält Informationen zur Filterung und Weiterleitung von Rahmen
- Selbstlernende Bridges
  Bridge "lernt" die Tabelleneinträge selbstständig
- Ethernet-Switches
  geringere Durchlaufverzögerung, mehr Ports und höherer Durchsatz als bei der Multiport-Bridge
- VLANs
  Switch verwaltet mehrere unabhängige Broadcast-Domänen
  Rechner können in unabhängige VLANs eingeteilt werden

3.4 Wireless LAN (IEEE 802.11)

Nutzt lizenzfreies 2,4GHz bzw. 5GHz Bandbreite
Erreichbare Datenraten

- IEEE 802.11b 11Mbps
- IEEE 802.11g 54Mbps
- IEEE 802.11a 54Mbps → USA
- IEEE 802.11n 600Mbps
- IEEE 802.11ac 1700Mbps

Erreichbare Reichweiten: 30-50m im Gebäude, bis 1km außerhalb

3.4.1 WLAN-Betriebsmoden

- Ad hoc Modus
  Direkter Verbindungsaufbau zwischen WLAN-Knoten
  Knoten müssen die gleiche Übertragungskanal-Nr. und SSID verwenden
- Infrastruktur-Modus
  WLAN-Clients kommunizieren über den Access Point (AP)
  Access Point wirkt wie eine Bridge zw. Funknetz und drahtgebundenem Netz
  über Broadcast werden Funknetz-Parameter verteilt

3.4.2 Nutzbare Frequenzbänder für IEEE 802.11b/g

13 überlappende Frequenzbänder (Europa)
Standard-Kanal-Nummern: 1,6,11
Überlappungen führen zu Störungen und Bitrateneinbußen

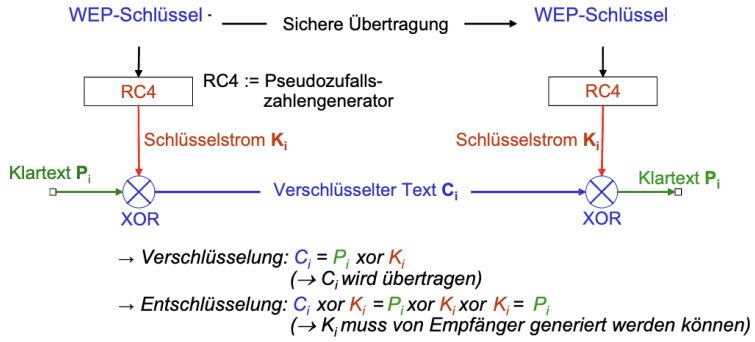
3.4.3 CSMA/CA: Medienzugriffsprotokoll für WLAN

Kapitel 3 S.56-59

3.4.4 Sicherheitsmechanismen für 802.11-Netze

- Alte Sicherheitsmechanismen:
  - (E)SSID, (Extended)ServiceSetIdentity: Kennung des Netzes
    WLAN-Client braucht die Kennung, um sich anzumelden
    wird oft durch Beacon-Frames vom AP selbst bekannt gemacht
  - MAC-ACLs (Media Access Control-Access Lists)
    AP fürht List mit erlaubten Client-MAC-Adressierung
    MAC-Adresse können modifiziert werden
  - WEP (Wired Equivalent Privacy)-Verschlüsselung
- Neue Sicherheitsmechanismen:
  Aktueller Sicherheitsstandard - WPA

WEP-Verschlüsselung



Der WEP-Schlüssel besteht aus zwei Teilen

1. "Geheimer" Benutzerschlüssel:
   Muss auf allen berechtigten Edngeräten eingetragen werden
   WEP64: enthält 40Bit-Benutzerschlüssel

2. 24-Bit-Initialisierungsvektor (IV):
   Wird für "jedes" verschickte Datenpaket geändert

Schwächen der WEP-Verschlüsselung

IV ist zu kurz (nur 24 Bit)

ca. alle 16 Mio Datenpakete wiederholt sich der IV

IV wird im Klartext übertragen

Keine Schlüsselveraltung

Speicherugn der geheimen Benutzerschlüssel in jedem Client

Invalidierung eines Schlüssel erfolgt manuell

Sicherheit von 802.11-Funktnetzen

- ermöglicht den Einsatz fortgeschrittener Authentifizierungsverfahren (digital)
- Enthält eine dynamische Schlüsselverwaltung
  Generierung von temporären Schlüsseln zwischen Client und AP
  Master-Secret-Key: festgelegte Zeichenkette oder eine generierte Zeichenkette
- Verwendung eines besseren geeigneten Verschlüsselungsverfahrens (AES)

Authentifizierung über zentralen Server

Geeignet nur in großen Umgebungen mit zentraler Benutzerverwaltung (eduroam)

RADIUS (remote Authetication Dial-In User Service)

4 Die Internetschicht