Netzwerke
→ Sicherungsschicht

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Ziele
- Einleitung
- Protokollmechanismen
  - Synchronisation, Codetransparenz
  - Fehlererkennung/-behandlung
  - Flusssteuerung, Medienzugriff
- Lokale Netze
  - Ethernet
  - Weiterentwicklungen
- Zusammenfassung

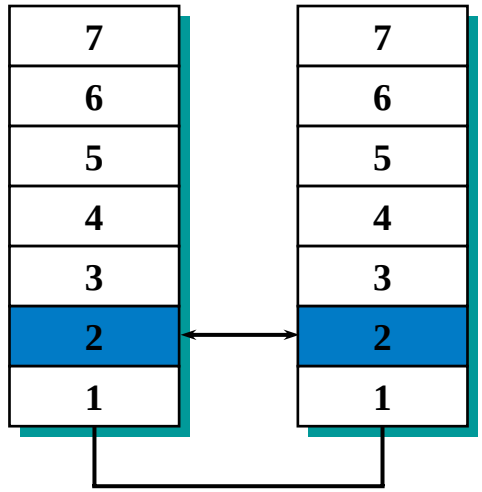
Inhalt

- **Ziele**

- Einleitung
- Protokollmechanismen
  - Synchronisation, Codetransparenz
  - Fehlererkennung/-behandlung
  - Flusssteuerung, Medienzugriff
- Lokale Netze
  - Ethernet
  - Weiterentwicklungen
- Zusammenfassung

Sicherungsschicht
→ Ziele

- Gutes Verständnis für die Anforderungen der Sicherungsschicht.
- Erlangen der Kenntnisse über die Aufgaben, Prinzipien und Mechanismen der Sicherungsschicht



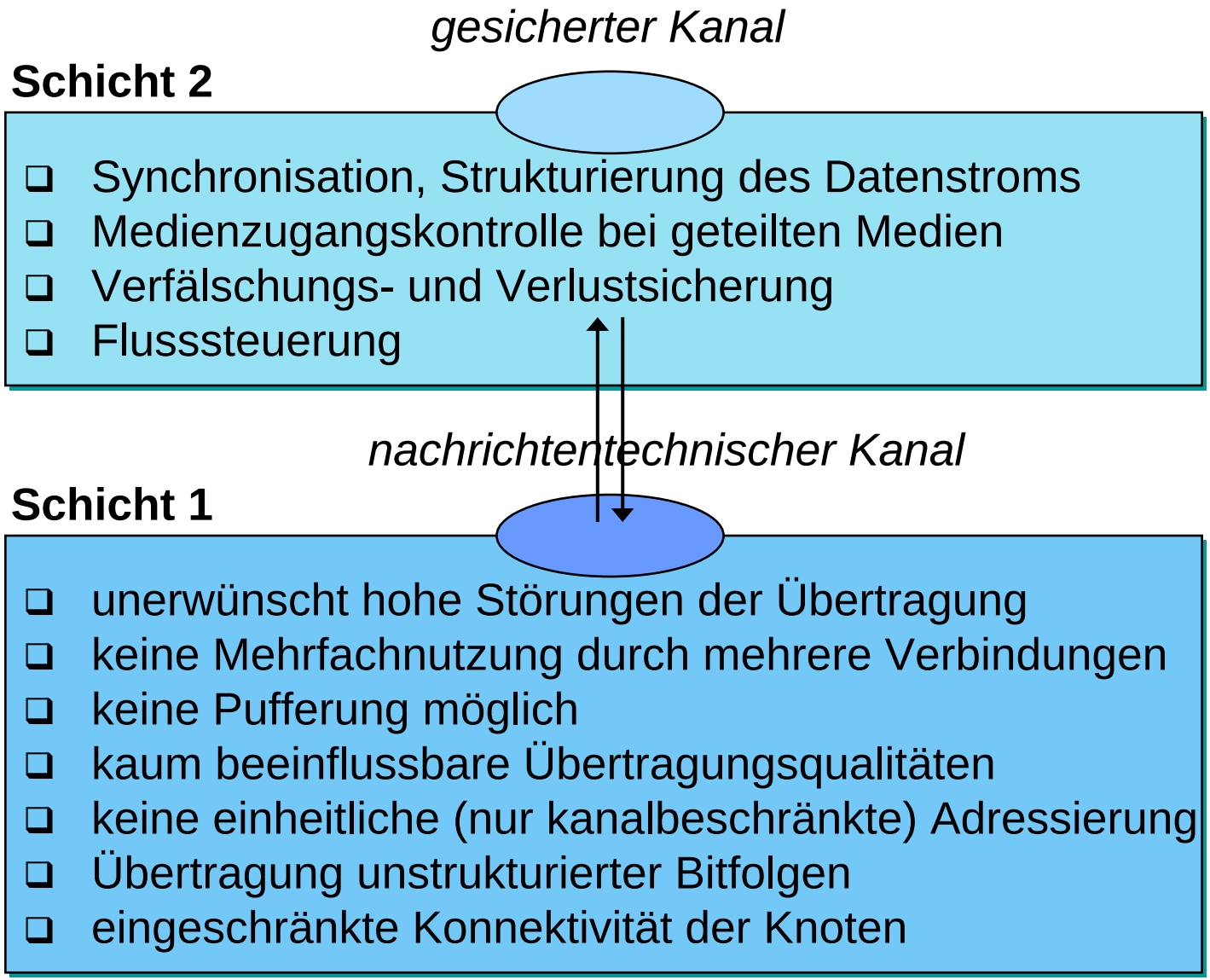
Inhalt

- Ziele

- **Einleitung**

- Protokollmechanismen
  - Synchronisation, Codetransparenz
  - Fehlererkennung/-behandlung
  - Flusssteuerung, Medienzugriff
- Lokale Netze
  - Ethernet
  - Weiterentwicklungen
- Zusammenfassung

Einleitung
→ Aufgaben der Sicherungsschicht



Einleitung
→ Dienste der Sicherungsschicht (nach OSI)

Verbindungsloser Dienst

Dienst	Req	Ind	Rsp	Conf	Beschreibung
DL-UnitData	x	x			Datenaustausch
DL-Connect	x	x	x	x	Verbindungsaufbau
DL-Data	x	x			Datenaustausch
DL-Disconnect	x	x	x	x	Verbindungsabbau
DL-Abort		x			Verbindungsabbruch-Anzeige

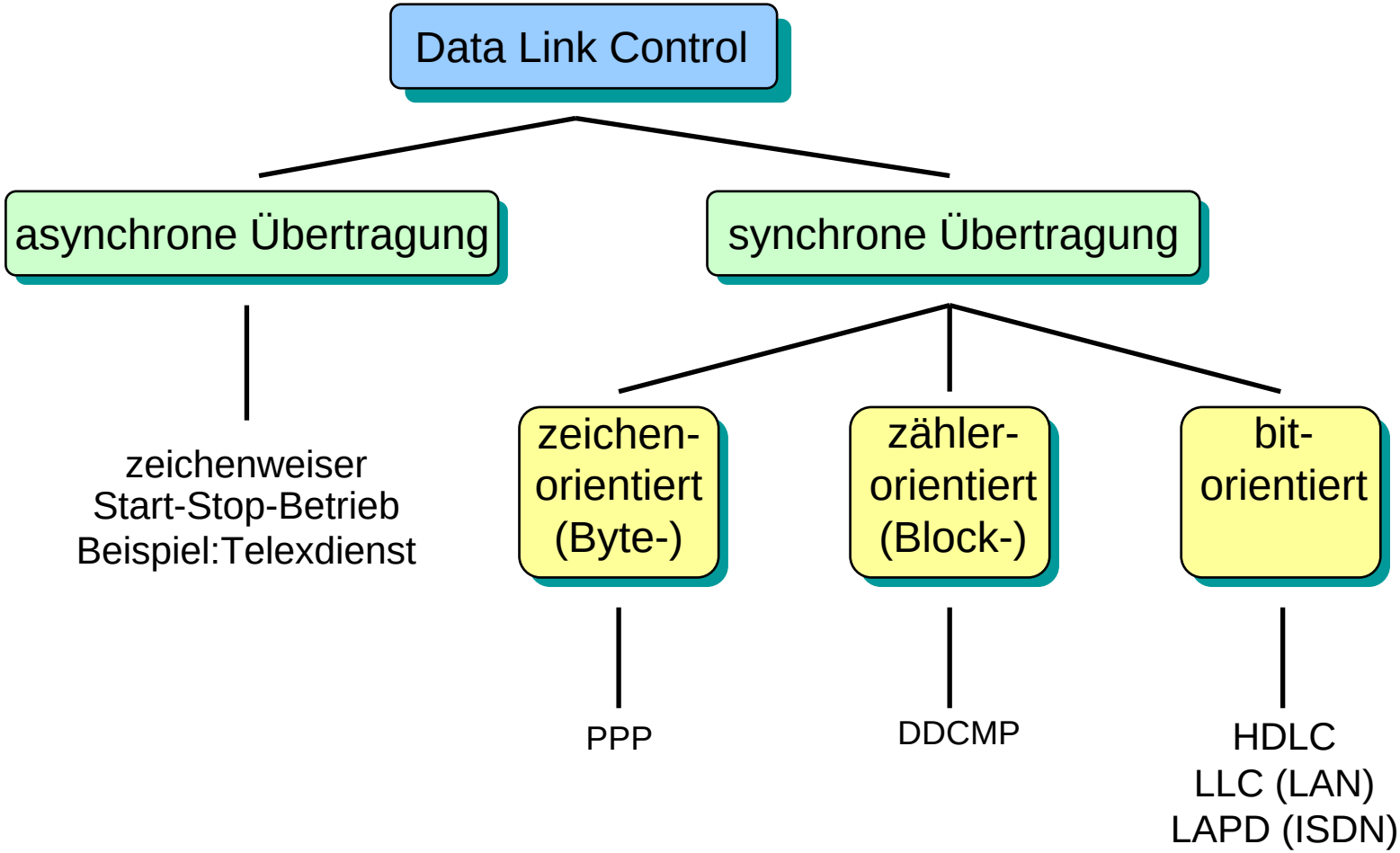
Verbindungsorientierter Dienst

- Die Sicherungsschicht bietet den Dienstnehmern auf Schicht 3 nach OSI Übertragung von Datenblöcken zwischen zwei Stationen an, sowohl verbindungslos als auch verbindungsorientiert.
- Der Verbindungsaufbau erfolgt zwischen zwei benachbarten, d.h. durch einen physikalischen Übertragungsabschnitt verbundenen, Rechnerknoten.

Inhalt

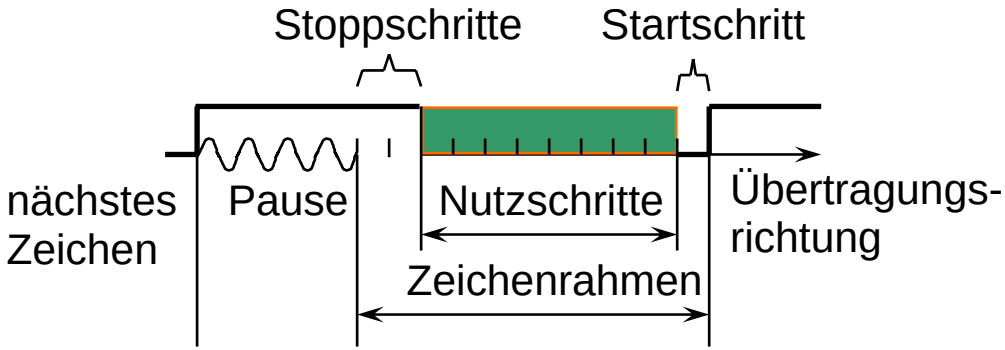
- Ziele
- Einleitung
- **Protokollmechanismen**
  - **Synchronisation, Codetransparenz**
  - **Fehlererkennung/-behandlung**
  - **Flusssteuerung, Medienzugriff**
- Lokale Netze
  - Ethernet
  - Weiterentwicklungen
- Zusammenfassung

Protokollmechanismen
→ Übersicht



Protokollmechanismen
→ Asynchrone Übertragung

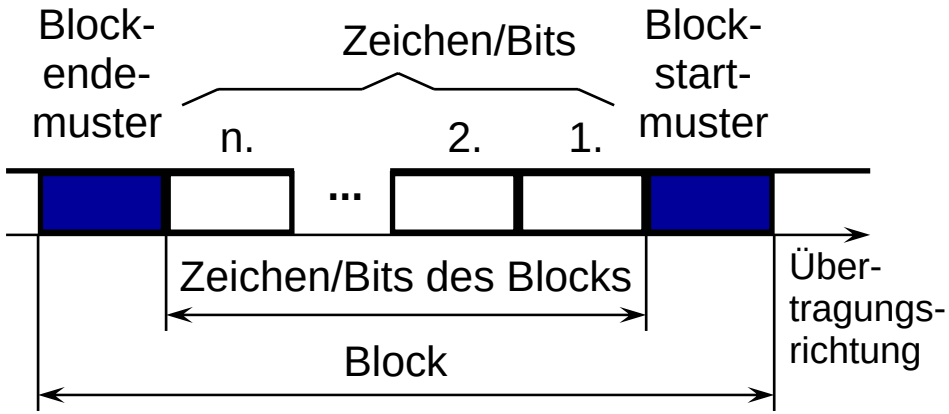
- **Zeichenweiser Start/Stop-Betrieb (Asynchronbetrieb)**



- Voraussetzung:
  - Ruhepegel
  - feste Zahl von Nutzschritten
  - Sender und Empfänger bilden jeweils eigenen Takt
- 3-aus-11 Overhead
  (8 Nutzbits bei 11 zu übertragenden Bits)
- Einsatzfall:
  Zeitlichen Abstände zwischen der Generierung der zu übertragenden Zeichen folgen keinem festen Schema, sondern sind zufalls-basiert, wie z.B. Zeichenübertragung bei Tastatureingaben.

Protokollmechanismen
→ Synchrone Übertragung

- **Blocksynchronisation (Synchronbetrieb)**



- Voraussetzung:
  - Blockstart-/-endemuster muss eindeutig sein!
  - Sender u. Empfänger synchronisieren sich über gemeinsamen Takt
- Modifikation / Rückgängig-machen entsprechender Muster (Blockstart-/-ende) im Block (Zeichen-/Bitstopfen)
- Einsatzfall:
  Bei der synchronen Übertragung wird eine Folge von Zeichen/Bits innerhalb eines Blocks/Rahmens übertragen.

Protokollmechanismen
→ Zeichenorientierte Übertragung

Internationales 7-bit Alphabet (dt. Referenzversion)

$b_4b_3b_2b_1$ \ $b_7b_6b_5$		000	001	010	011	100	101	110	111
0000	0	NUL	TC_7 (DLE)	SP	0	@	P	`	p
0001	1	TC_1 (SOH)	DC1	!	1	A	Q	a	q
0010	2	TC_2 (STX)	DC2	“	2	B	R	b	r
0011	3	TC_3 (ETX)	DC3	#	3	C	S	c	s
0100	4	TC_4 (EOT)	DC4	$	4	D	T	d	t
0101	5	TC_5 (ENQ)	TC_8 (NAK)	%	5	E	U	e	u
0110	6	TC_6 (ACK)	TC_9 (SYN)	&	6	F	V	f	v
0111	7	BEL	TC_{10} (ETB)	´	7	G	W	g	w
1000	8	FE_1 (BS)	CAN	(	8	H	X	h	x
1001	9	FE_2 (HT)	EM	)	9	I	Y	i	y
1010	10	FE_3 (LF)	SUB	*	:	J	Z	j	z
1011	11	FE_4 (VT)	ESC	+	;	K	Ä	k	ä
1100	12	FE_5 (FF)	IS_4 (FS)	,	<	L	Ö	l	ö
1101	13	FE_6 (CR)	IS_3 (GS)	-	=	M	Ü	m	ü
1110	14	SO	IS_3 (RS)	.	>	N	^	n	ß
1111	15	SI	IS_1 (US)	/	?	O		o	DEL

Ursprung:
American **S**tandard **C**ode of **I**nformation Interchange
→ **ASCII**

Protokollmechanismen

→ Synchrone Übertragung: Codetransparenz

- **Codetransparenz:**
  - „Vereinbarung von Regeln zur codetransparenten Übertragung von Nutzdaten (d.h. Übertragung beliebiger Bit- bzw. Zeichenkombinationen im Nutzdatenfeld)“

- Einfacher Lösungsansatz:
  - **Längenangabe der Nutzdaten:**

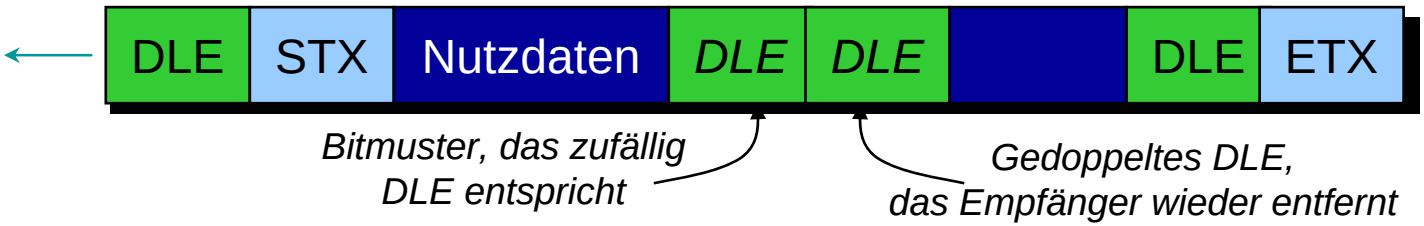
- Problem bei der Längenangabe der Nutzdaten
  - Falls das Längenfeld während der Übertragung verändert wird, kann der Empfänger den Anfang der nächsten Rahmen nicht mehr erkennen.

Synchrone Übertragung
→ Character Stuffing / Zeichenstopfen

Anfang und Ende eines Rahmens werden durch STX bzw. ETX symbolisiert:

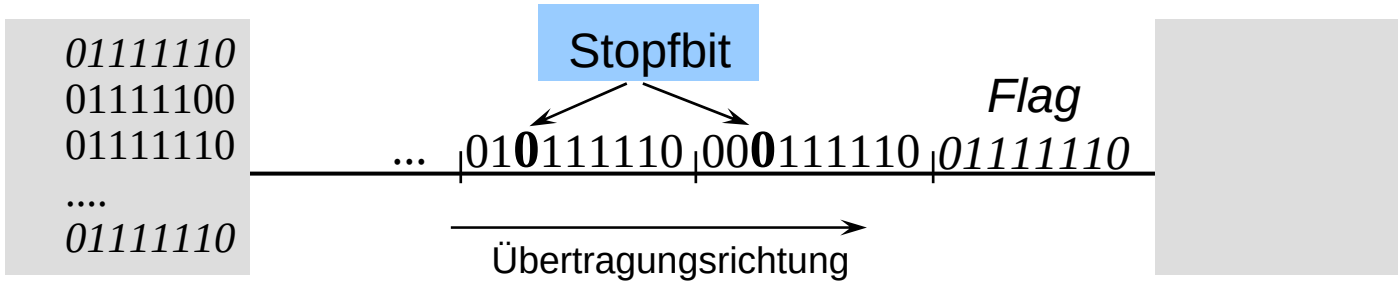
Problem: Ein ETX in den Nutzdaten signalisiert das vorzeitige Ende des Rahmens.
Lösung: Das Sonderzeichen DLE (Data Link Escape) macht Nutzdaten transparent
Ein ETX wird daher nur dann als solches erkannt, wenn ein DLE davor steht.

Problem: Ein DLE in den Nutzdaten könnte jetzt zu einer Fehlinterpretation führen.
Lösung: Der Sender verdoppelt DLEs innerhalb der Nutzdaten.
Der Empfänger interpretiert einfache DLEs als Steuerzeichen, bei doppelten DLEs wird das künstlich eingefügte wieder gelöscht.



Synchrone Übertragung
→ Bit Stuffing / Bitstopfen

- Blockbegrenzung (Flag) ist eine **ausgezeichnete Bitfolge (01111110)**
- Problem: Zufälliges Auftreten von 01111110 in Nutzdaten
- Lösung: **Bit Stuffing**
  - Sender fügt innerhalb der Nutzdaten nach 5 aufeinander-folgenden „1“-en eine „0“ ein.
  - Empfänger entfernt nach 5 aufeinanderfolgenden „1“-en eine „0“.
- Blockprüfzeichen zur Fehlererkennung wird vor dem Bit Stuffing erstellt.



Fehlerursachen

- **Übertragungsfehler**, sind hardwareinduzierte Fehler, die vorzugsweise auf dem Übertragungsmedium entstehen, aber auch in den Anschlusselektroniken der kommunizierenden Stationen.“
- Art und Häufigkeit sind stark vom **Übertragungsmedium abhängig**.
- In der Funktechnik existieren andere Fehlerursachen, Fehlerhäufigkeiten und Fehlerauswirkungen als in der leitungsgebundenen Übertragungstechnik!

- **Störeinflüsse bei der Übertragung digitaler Daten führen normalerweise zur Erkennung von falschen Bits.**

Fehlertypen

- **Einzelbitfehler:**
  - sind Fehler, bei denen nur ein Bit umgedreht wurde,
  - z.B. Rauschspitzen, die die Detektionsschwelle bei digitaler Signalerfassung überschreiten.
- **Bündelfehler:**
  - sind Fehler, die über viele Bit gehen,
  - z.B. länger anhaltende Störung durch Überspannung oder Starkstromschaltprozesse.
- **Synchronisierfehler:**
  - sind Fehler, bei denen der Empfänger falsch synchronisiert ist und alle Bits falsch abtastet.
- **Auswirkung als Einzelbit- oder Bündelfehler abhängig von Übertragungsgeschwindigkeit**

Fehlerwirkungen
→ Rechenbeispiel

- Eine **Störung von 20 ms** führt ...
  - bei Telex (50 Bit/s, Signaldauer: 20 ms) zu einem Fehler ***von 1 Bit***
    ⇨ **Einzelfehler**
  - bei ISDN (64 KBit/s, Signaldauer: 15,625 µs) zu einem Fehler ***von 1280 Bit***
    ⇨ **Bündelfehler**
  - bei B-ISDN
    155 MBit/s, Signaldauer: 6,45 ns: zu einem Fehler
    von ca. 3,1 MBit = ***387,5 KByte***
    622 MBit/s, Signaldauer: 1,61 ns: zu einem Fehler
    von ca. 12,4 MBit = ***1,5 MByte***
    2,4 GBit/s, Signaldauer: 0,4 ns: zu einem Fehler
    von ca. 48 MBit = ***6 MByte***
    ⇨ **Bündelfehler**

Fehlerhäufigkeiten

- **Maß für die Fehlerhäufigkeit:**

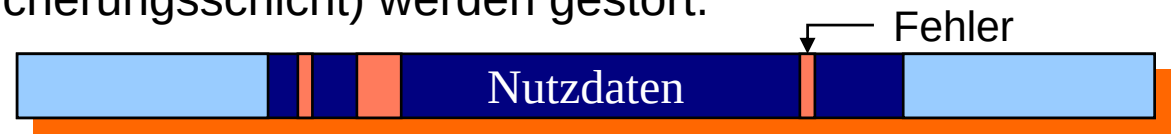
  Bitfehlerrate = Summe gestörte Bits / Summe übertragene Bits

  - Stark vom Übertragungsmedium bzw. Netz abhängig
  - Bitfehlerraten zu übertragender digitaler Daten im analogen Netz sind sehr viel höher als in digitalen Übertragungssystemen. Moderne ISDN/PCM-Systeme haben eine bessere Übertragungsqualität als klassische digitale Netze.
  - Die Übertragungsfehlerhäufigkeit ist auch stark von der Gesamtlänge des Übertragungsweges abhängig

- **Typische Wahrscheinlichkeiten für Bitfehler:**
  - Analoges Fernsprechnetz $2*10^{-4}$
  - Funkstrecke 10^{-3} - 10^{-4}
  - Ethernet (10Base2) 10^{-9} - 10^{-10}
  - Glasfaser 10^{-10} - 10^{-12}

Fehlerwirkungen

- Fehlerwirkungen sind abhängig davon, welche Bits betroffen sind:
  - **(Nutz-)Datenfehler**: Bits innerhalb der Nutzdaten (gesehen z.B. aus Sicht der Sicherungsschicht) werden gestört.



  - **Protokollfehler**: Störungen können Protokollkontrolldaten, Steuerzeichen, Adressen oder sonstige protokollrelevante Daten verfälschen oder vernichten.

⇨ **Fehlererkennungs- und Behandlungsmaßnahmen** (error detection and recovery) erforderlich.

⇨ **Fehlererkennung durch (künstliches) Hinzufügen von Redundanz beim Sender**

- error detecting codes (z.B. Paritätssicherung und CRC)
- (Spezialfall: „error correcting codes“ oder „forward error correction“)

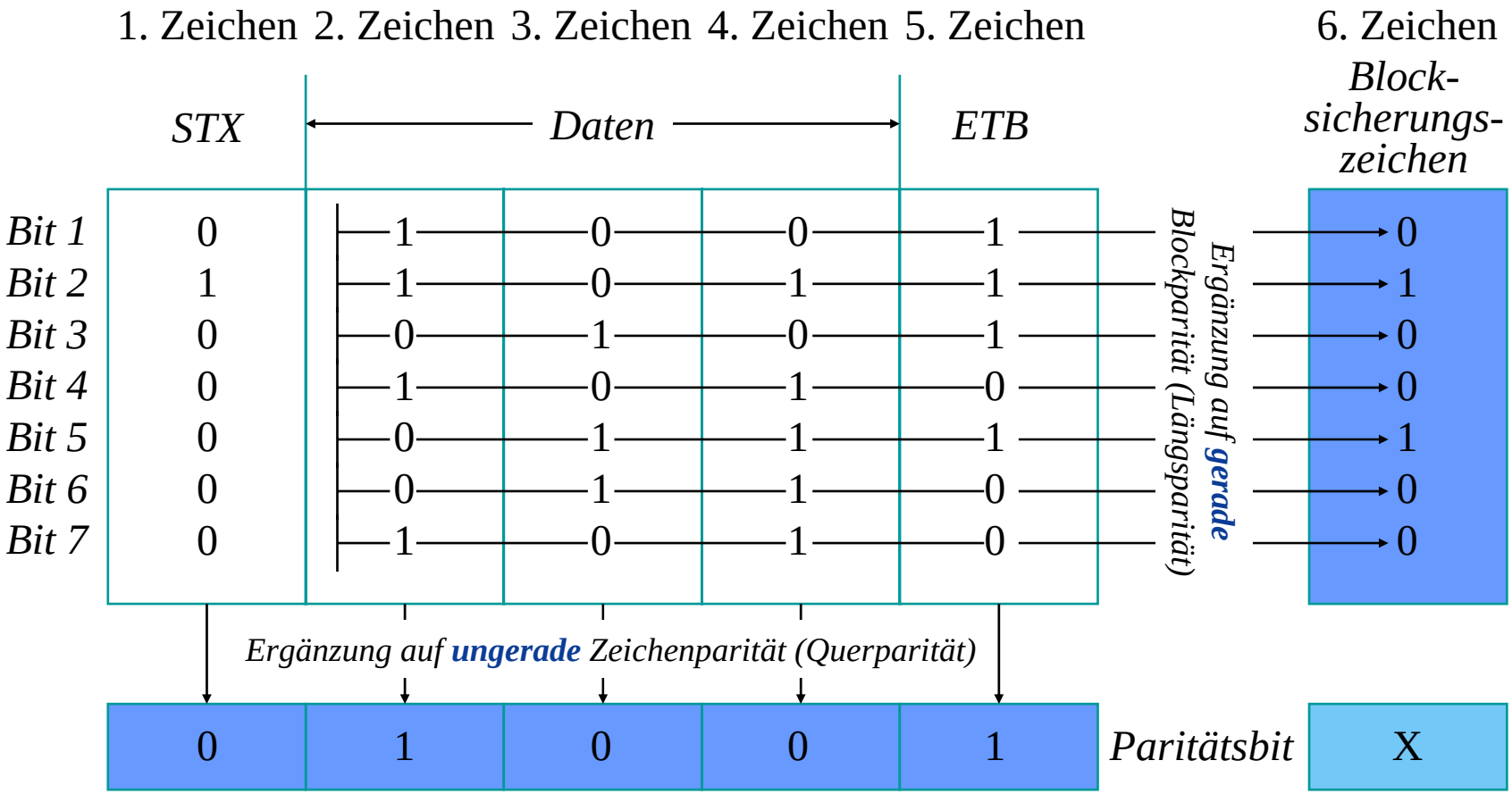
Fehlererkennung
→ Paritätsüberprüfung: Paritätsbits

- Die Bildung eines Paritätsbits lässt sich auf zweierlei Art und Weise vornehmen:
  - Gerade Parität:
    Gesamtzahl der „1“ einschließlich des Paritätsbits ist gerade.
  - Ungerade Parität:
    Gesamtzahl der „1“ einschließlich des Paritätsbits ist ungerade.

Fehlererkennung
→ Paritätsüberprüfung: Verfahren

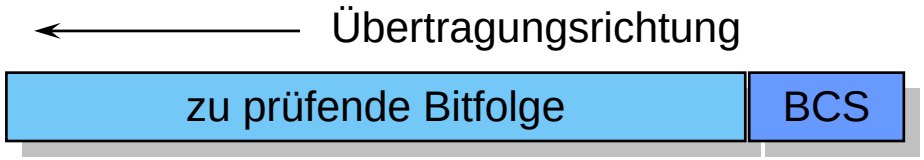
- **Zeichen- oder Querparität:** (VRC: Vertical Redundancy Check) Sicherung von Einzelzeichen. Einziges Verfahren bei asynchroner Einzelzeichen-Übertragung.
- **Block- oder Längenparität:**(LRC: Longitudinal Redundancy Check) Alle Bits gleicher Wertigkeit innerhalb eines aus Zeichen estehenden Übertragungsblocks werden durch ein Paritätsbit (gerade oder ungerade) gesichert.
  Sie bilden ein Blockprüfzeichen (BCC: Block Check Character).
- **Kreuzsicherung:**
  Gleichzeitige Anwendung von Längs- und Querparität. Abstimmung über die Bildung des Paritätsbits des Blockprüfzeichens erforderlich!
- **Hinweis:**
  STX wird nicht in Block-Paritätsprüfung einbezogen, da der Empfänger erst nach START OF TEXT weiß, dass ein prüfenswerter Übertragungsblock beginnt.
- Die Fehlererkennungswahrscheinlichkeit bei Paritätsprüfung ist nicht sehr hoch. Mehrfachfehler (zwei oder eine gerade Zahl in gleicher Zeile oder Spalte liegende Fehler) werden nicht erkannt.

Fehlererkennung
→ Paritätsüberprüfung: Beispiel



Fehlererkennung
→ Cyclic Redundancy Check (CRC)

- Beim **CRC** wird der zu prüfende Block als unstrukturierte Bitfolge aufgefasst, die **Anzahl der zu prüfenden Bits ist beliebig**.
- Die Prüfbitfolge [Block Check Sequence (BCS) bzw. Frame Check Sequence (FCS)] wird an den zu prüfenden Übermittlungsdatenblock angehängt.



Anhängen der Blockprüfdaten an den Übermittlungsblock

- Bildung der Prüfsequenz:
  - Zu prüfende Bitfolge wird als Polynom aufgefasst.
  - Nach Erweiterung um 0-Folge (Anzahl 0-en = Grad des Prüfpolynoms) wird sie durch vereinbartes Prüfpolynom (Generatorpolynom) geteilt.
  - Die BCS/FCS ist Rest der Division, der an die Bitfolge angehängt wird.
  - Beim Empfänger wird neu dividiert (einschließlich Rest). Bei fehlerfreier Übertragung muss das Ergebnis 0 sein.

Fehlererkennung
→ CRC-Beispiel: Senden

- Zu sendende Bitfolge: 110011
- Prüfpolynom: $x^4 + x^3 + 1$
  - ⇨ **Divisor in Modulo-2-Binärarithmetik: 11001**
    - Addition/Subtraktion Modulo-2 entspricht einer bitweisen XOR-Verknüpfung
    - Dividend ist teilbar durch Divisor, falls der Dividend mindestens so viele Stellen besitzt wie der Divisor (führende Bits müssen beide 1 sein)
- Länge der Sicherungsfolge = Grad des Prüfpolynoms = 4

- Berechnung der Sicherungsfolge:

```
11 0011 0000 ÷ 1 1001 = 10 0001
11 001
-------
00 0001 0000
      1 1001
      ------
      0 1001  = Rest
```

- Zu übertragende Bitfolge: 11 0011 **1001**.

Fehlererkennung
→ CRC-Beispiel: Empfangen

- Empfangen einer korrekten Bitfolge:

```
11 0011 1001 ÷ 1 1001 = 10 0001
11 001
-------
00 0001 1001
      1 1001
      -------
      0 0000  = Rest
```

- **Kein Rest, somit sollten Daten fehlerfrei sein!**

- Empfangen einer gefälschten Bitfolge:

```
11 1111 1000 ÷ 1 1001 = 10 1001
11 001
-------
00 1101 1
   1100 1
   -------
   0001 0000
      1 1001
      -------
      0 1001  = Rest ≠ 0
```

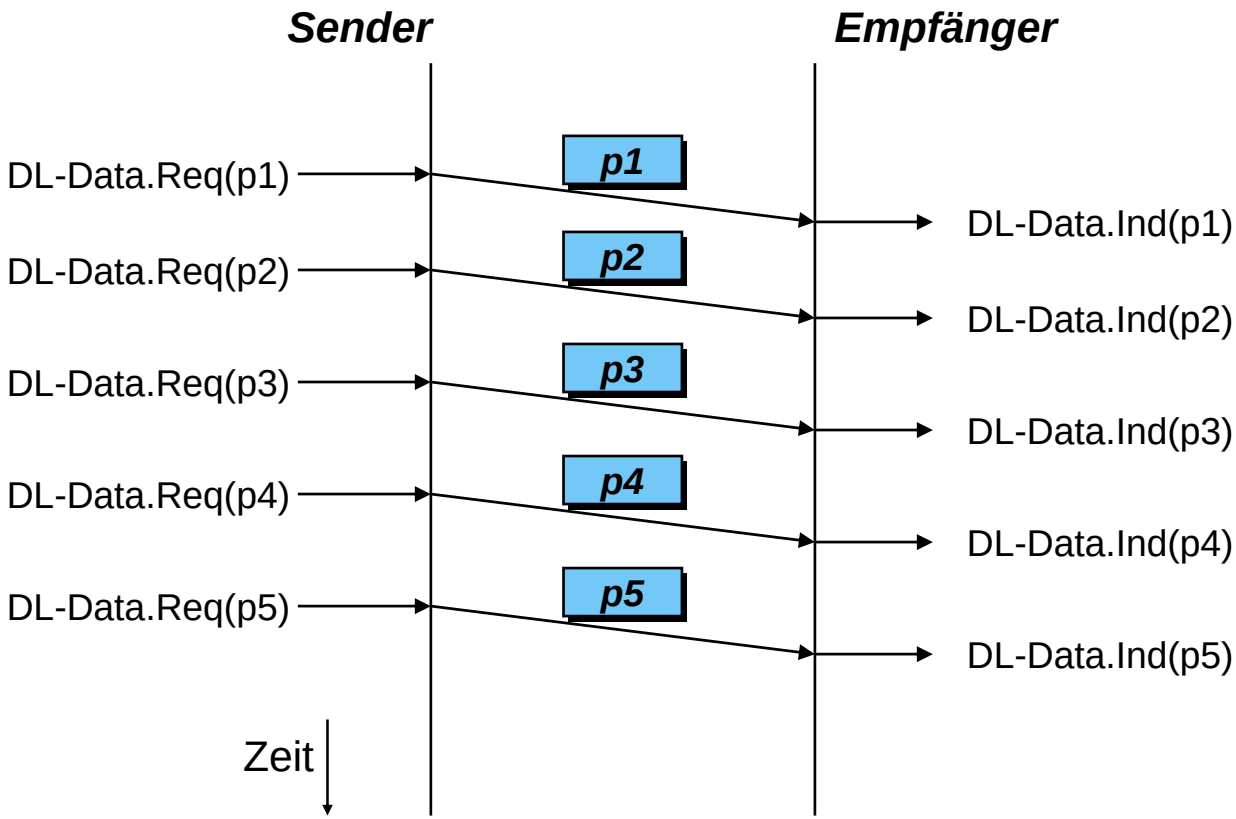
- Es bleibt Rest ungleich 0, somit war ein Fehler in der Übertragung.

Fehlererkennung
→ CRC-Leistungsfähigkeit

- Folgende Fehler werden durch CRC erkannt:
  - sämtliche Einzelbitfehler
  - sämtliche Doppelfehler, wenn $(x^k + 1)$ nicht durch das Prüfpolynom teilbar ist
  - sämtliche Fehler ungerader Anzahl, wenn $(x+1)$ Faktor des Prüfpolynoms ist
  - sämtliche Bündelfehler der Länge ≤ Grad des Prüfpolynoms
- International genormte Prüfpolynome:
  - CRC-12 $= x^{12} + x^{11} + x^3 + x^2 + x + 1$
  - CRC-16 $= x^{16} + x^{15} + x^2 + 1$
  - CRC-CCITT $= x^{16} + x^{12} + x^5 + 1$
- CRC-16 und CRC-CCITT entdecken
  - alle Einzel- und Doppelfehler + alle Fehler ungerader Anzahl
  - alle Bündelfehler mit der Länge ≤ 16
  - 99,997 % aller Bündelfehler mit der Länge 17
  - 99,998 % aller Bündelfehler mit der Länge 18 und mehr

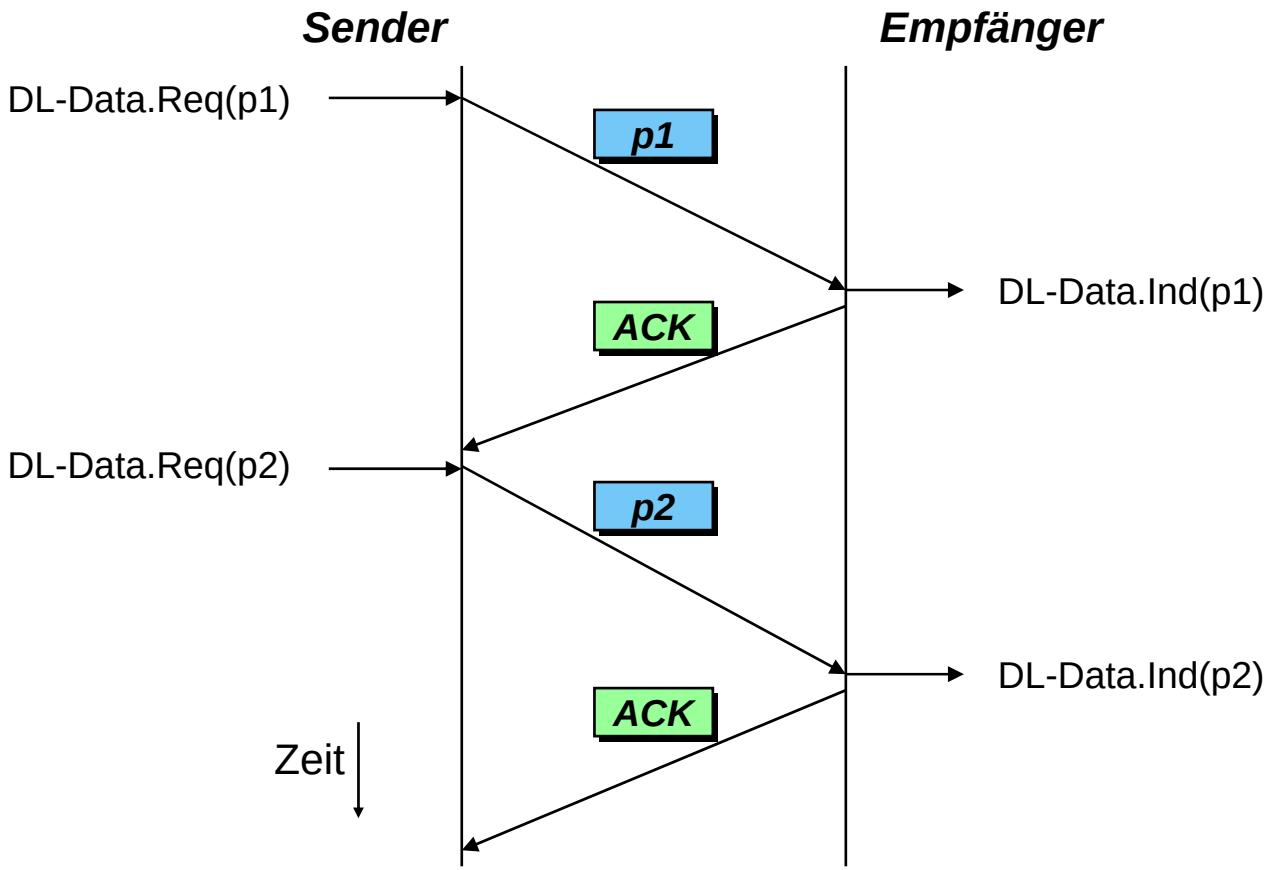
Fehlerbehandlung
→ Übertragung ohne Fehlerbehandlung

- Sender und Empfänger sind immer bereit
- Ständiger Datenfluss vom Sender zum Empfänger.



Fehlerbehandlung
→ Stop-and-Wait

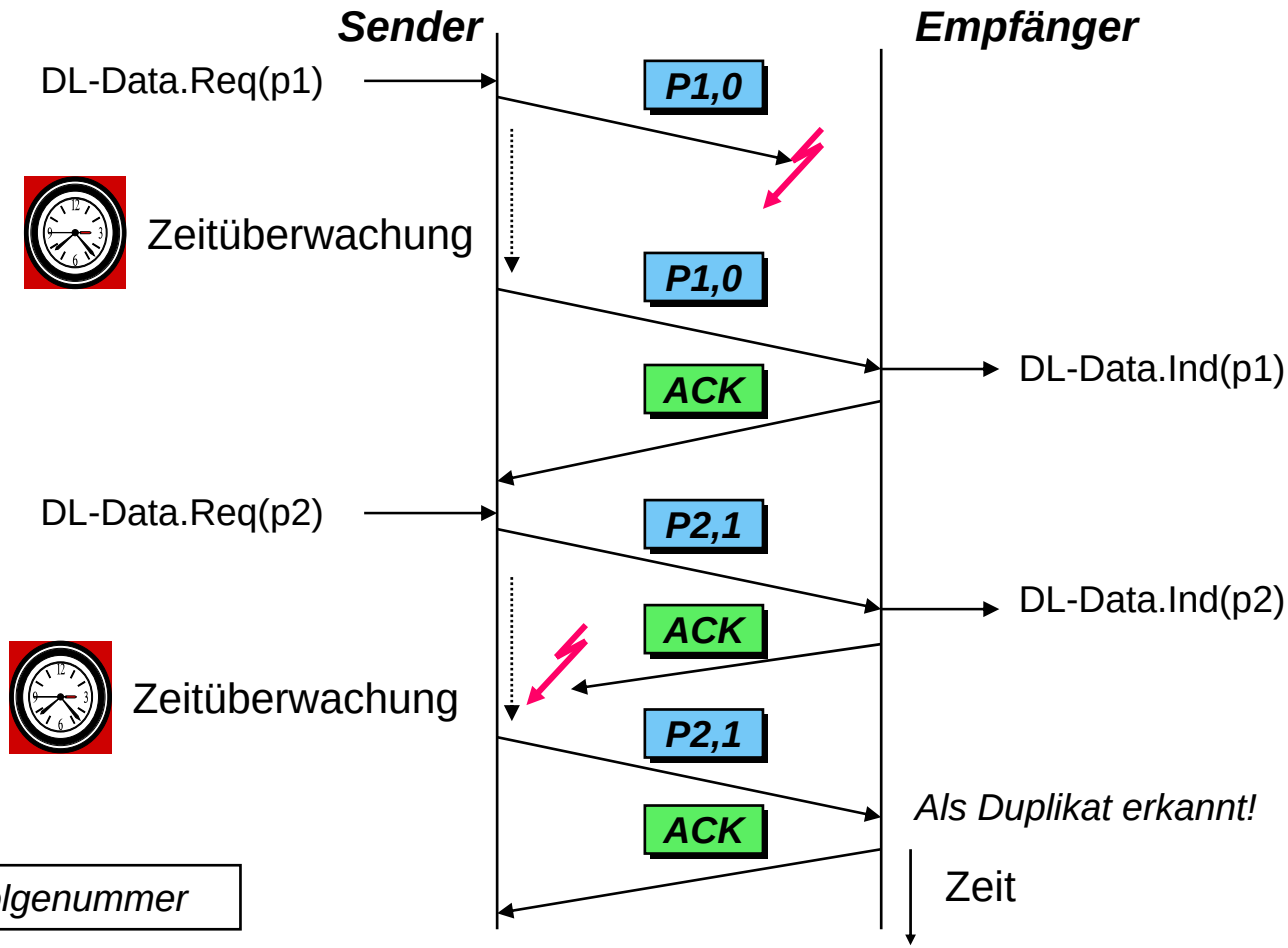
- Empfänger muss durch eine Meldung den Empfang eines Paketes bestätigen.
- Sender muss auf Bestätigung (Acknowledge, ACK) warten, ehe er weiter senden darf, damit ist keine Überlastung des Empfängers möglich!



Fehlerbehandlung

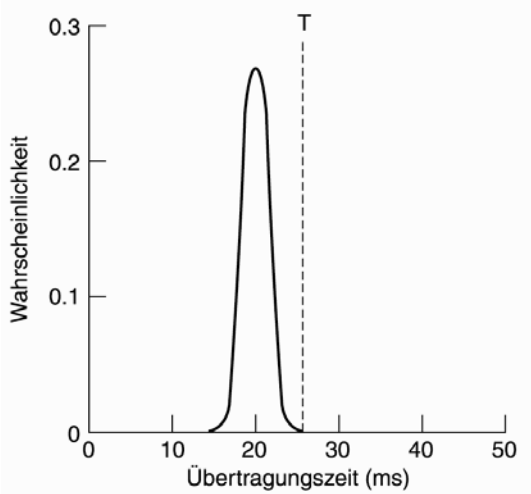
→ implizite Übertragungswiederholung: Ablauf

- Um *verlorengegangene Pakete/Quittungen* behandeln zu können, die sonst einen weiteren Datenaustausch unterbinden würden, muss vom Sender eine Zeitüberwachung durchgeführt werden (Time-out), nach der eine erneute Übertragung erfolgt.



Fehlerbehandlung
→ implizite Übertragungswiederholung: Timer

- Dieser Mechanismus behebt die Fehler, welche durch einzelne Paketverluste entstehen.
- Dabei ist die Größe des Timeouts sehr wichtig:
  - Ein zu niedriger Timeout führt dazu, dass der Sender sehr schnell beginnt, Pakete zu wiederholen. Es kann durch schwankende Verzögerungszeiten allerdings durchaus vorkommen, dass kein Paketverlust auftrat, sondern nur die Verzögerung des Pakets oder dessen Bestätigung etwas später ankommt. Somit wird ein Paket (sinnlos) mehrfach übertragen, was zur Verschwendung von Bandbreite führt.
  - Ein zu hoher Timeout sorgt dafür, dass Paketverluste erst recht spät erkannt werden. Dies behindert die Kommunikation und führt zu einer Leistungssenkung.

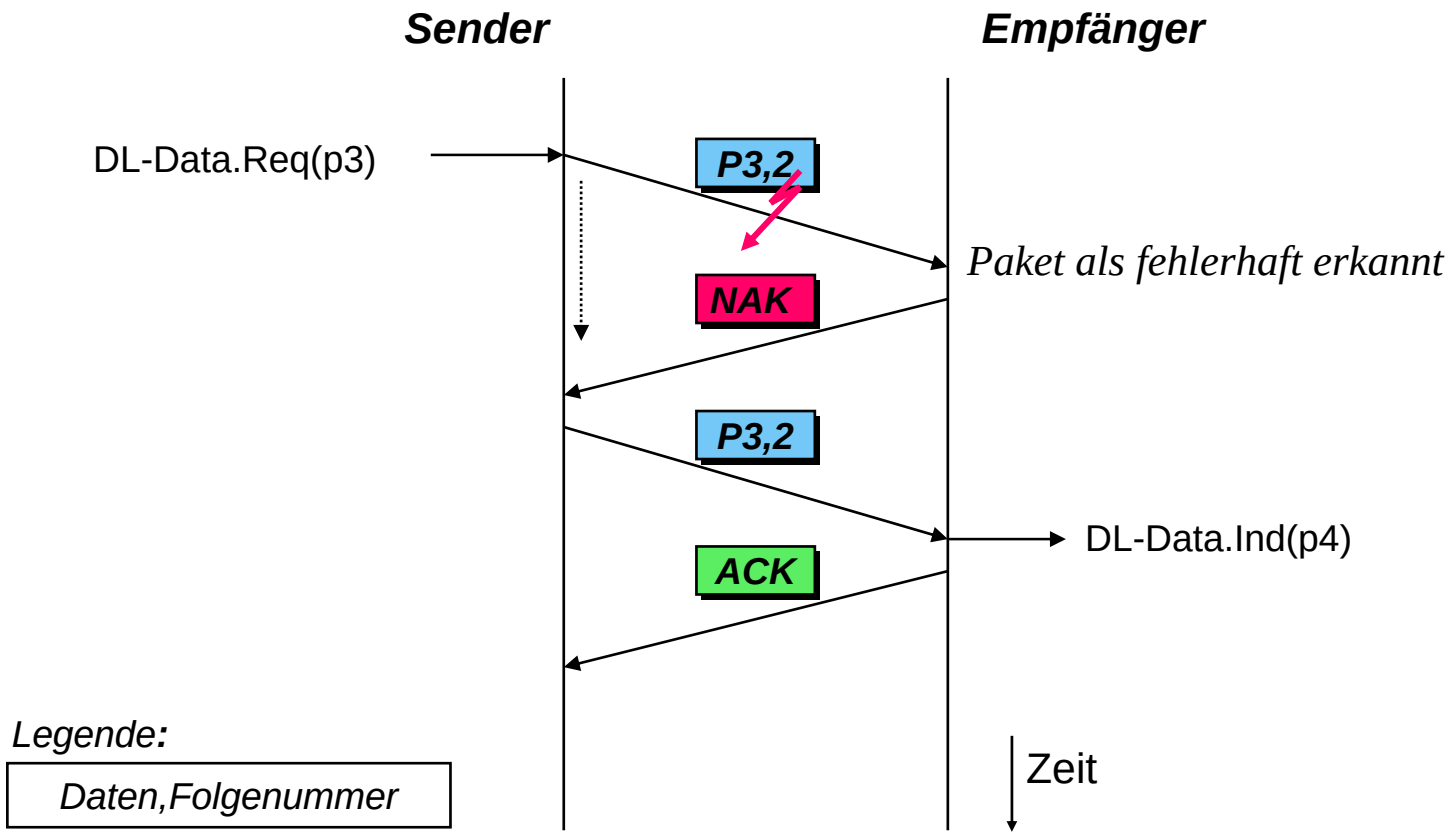


Fehlerbehandlung
→ Folgenummern

- Einen weiteren wichtigen Mechanismus der Protokolldateneinheiten der Sicherungsschicht stellen sogenannte Folgenummern dar.
- Jedem Datenpaket wird hierbei eine ganzzahlige Sendefolgenummer N(S) zugewiesen, die innerhalb des Paketkopfes übertragen wird.
- Dies ist z.B. notwendig, um dem Empfänger eine Erkennung von Duplikaten zu ermöglichen.
- Analog dazu können Empfangsfolgenummern (Quittungen) N(R) in den Bestätigungen ACK bzw. NAK ein bestimmtes Paket quittieren.
- Mit **Piggybacking** lassen sich N(S) und N(R) auch gemeinsam in einem Datenpaket übertragen.

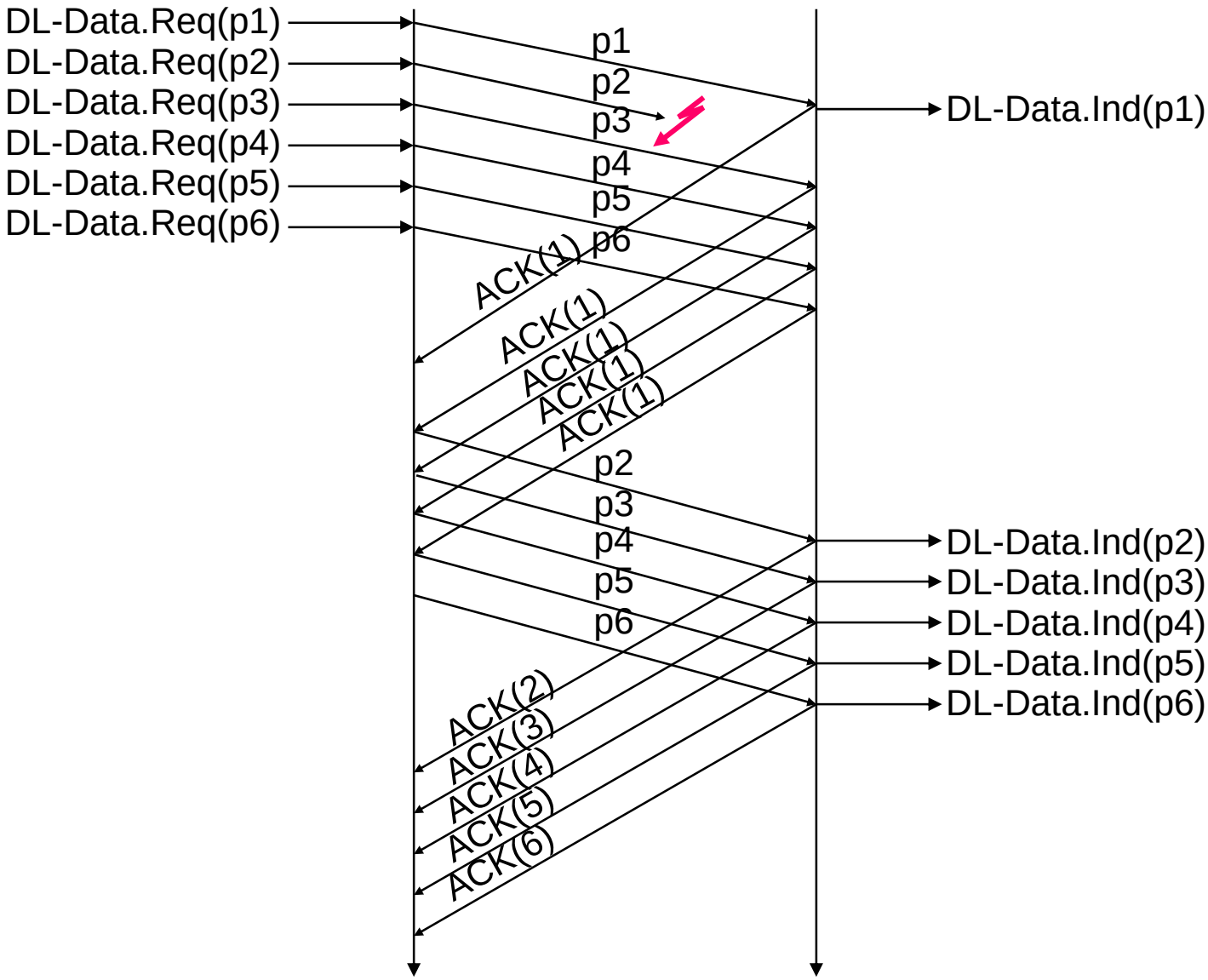
Fehlerbehandlung
→ explizite Übertragungswiederholung

- Um den Ablauf der Übertragungswiederholung zu beschleunigen, können fehlerhafte Pakete explizit durch *NAK* (Negative Acknowledgement) angefordert werden.

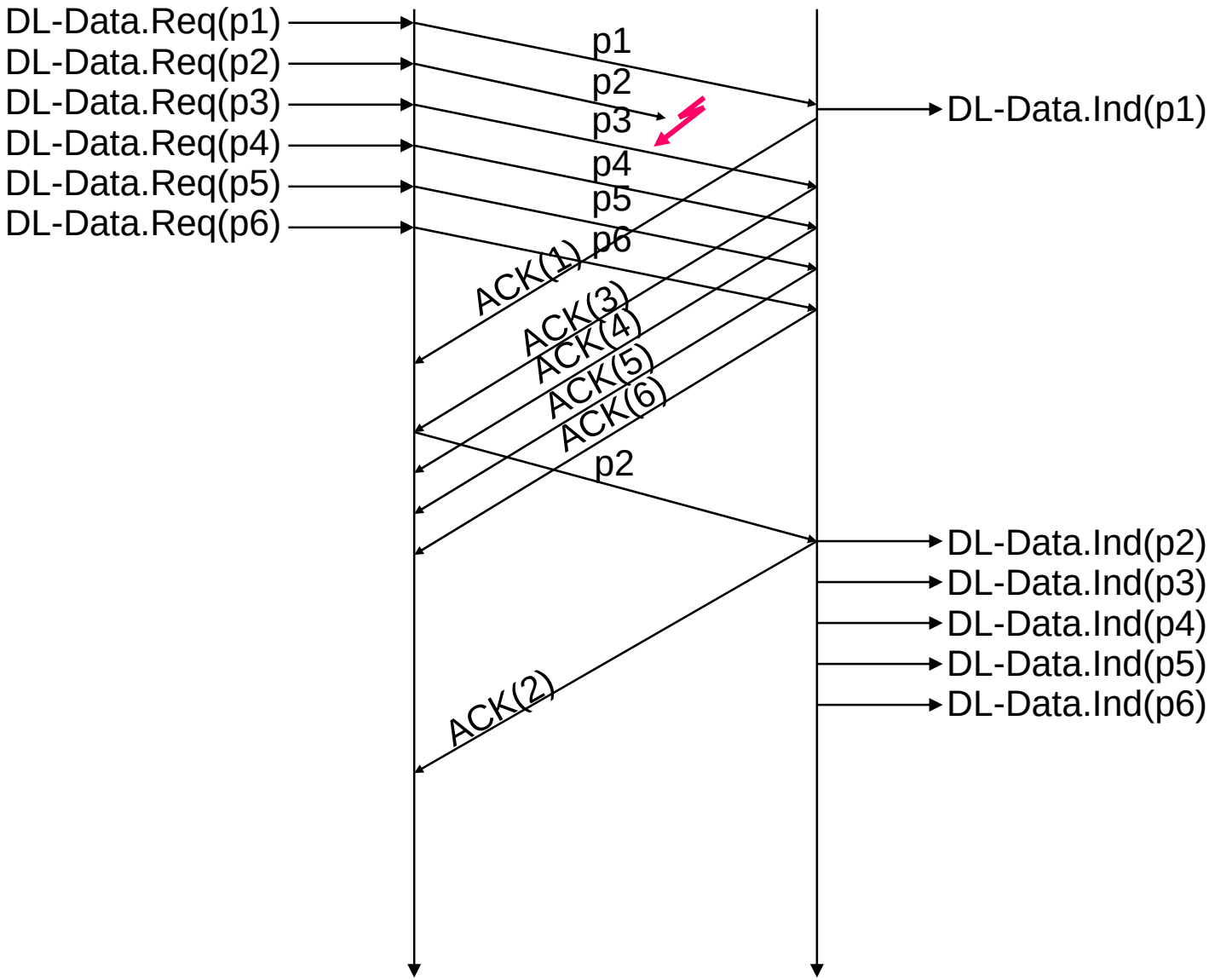


Fehlerbehandlung

→ Go-back-N



Fehlerbehandlung
→ Selective Repeat



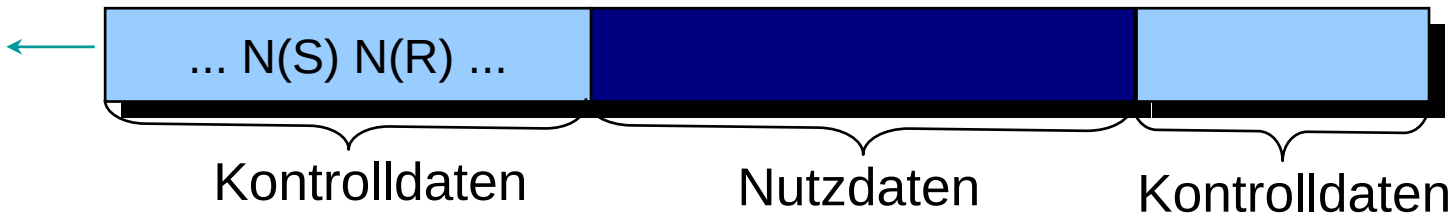
Fehlerbehandlung
→ implizite Bestätigung

- Sendefolgenummer (Sequenznummer) N(S) wird von der Sendeseite in aufsteigender Folge vergeben, ist in jedem gesendeten Paket enthalten

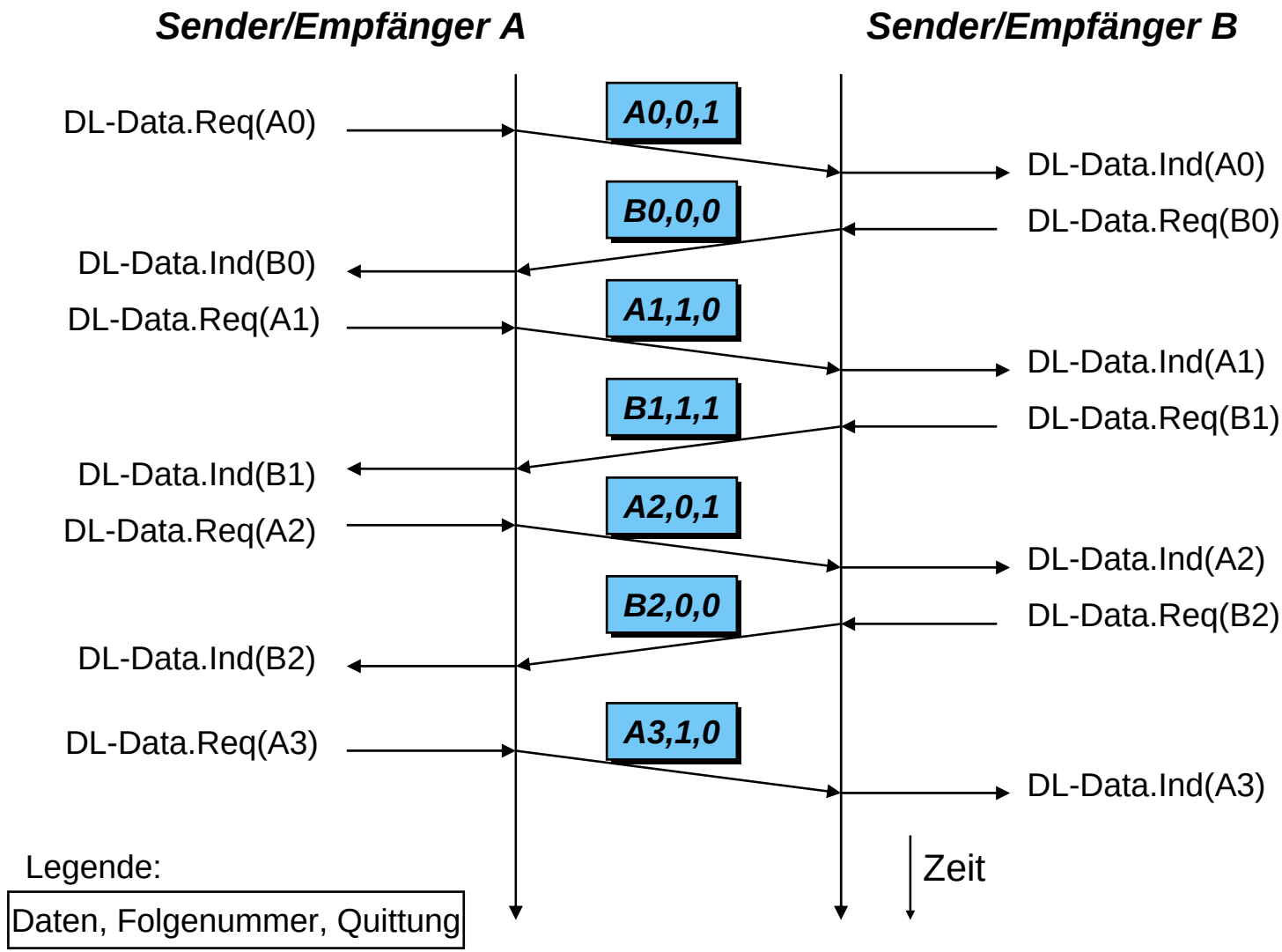
- Empfangsseite zählt mit jedem empfangenen Paket die Empfangsfolgenummer N(R) hoch

- ACK(N(R) = *n*) quittiert das Paket mit Sendefolgenummer N(S) = *n-1* und damit implizit sämtliche zuvor gesendeten Pakete.

- Im strengen Halbduplex-Betrieb reicht ein alternierendes 0 und 1. Im Vollduplex-Betrieb wird ein größerer Wertebereich benötigt, da zu einem Zeitpunkt mehrere Pakete ausstehen können.



Fehlerbehandlung
→ Piggybacking mit Alternating-Bit



Flusssteuerung
→ Überblick

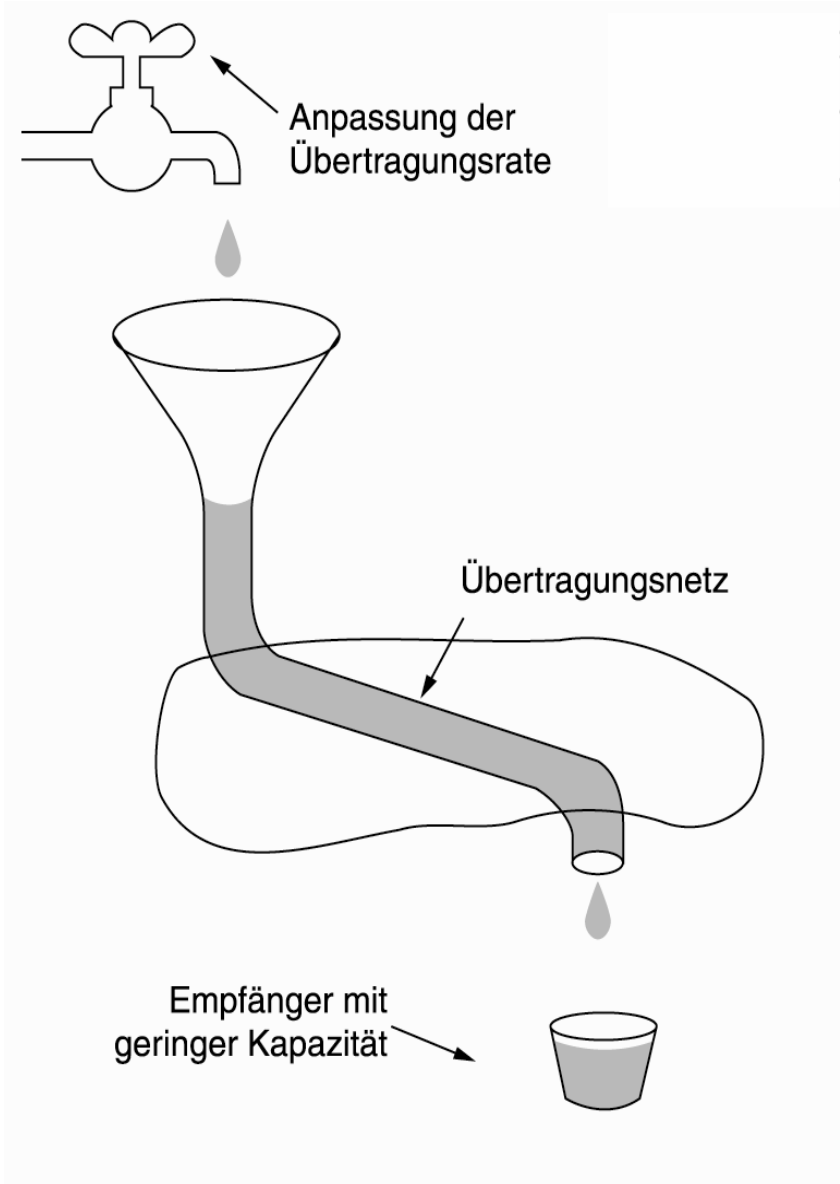
- *Synonyme Begriffe*
  - Flusssteuerung
  - Flussregulierung
  - Flusskontrolle
  - Flow Control

- *Aufgabe*
  - Auf Netzebene ist der Datenpaketempfänger vor einem zu großen Zufluss von Paketen eines Paketsenders zu schützen.

- *Ort der Durchführung*
  - Auf der Sicherungsschicht zum Überlastungsschutz von **Übermittlungsabschnitten**.
  - Zum Überlastungsschutz von Verbindungen auch auf höheren Schichten des OSI-Modells (siehe Transportebene).

Sicherungsschicht
→ Analogie: Empfangspufferüberlauf/

- In dieser Analogie sehen wir ein dickes Rohr, das zu einem Behälter mit geringer Kapazität führt.
- Solange nicht mehr Wasser eingefüllt wird, als der Behälter aufnehmen kann, geht kein Wasser verloren!

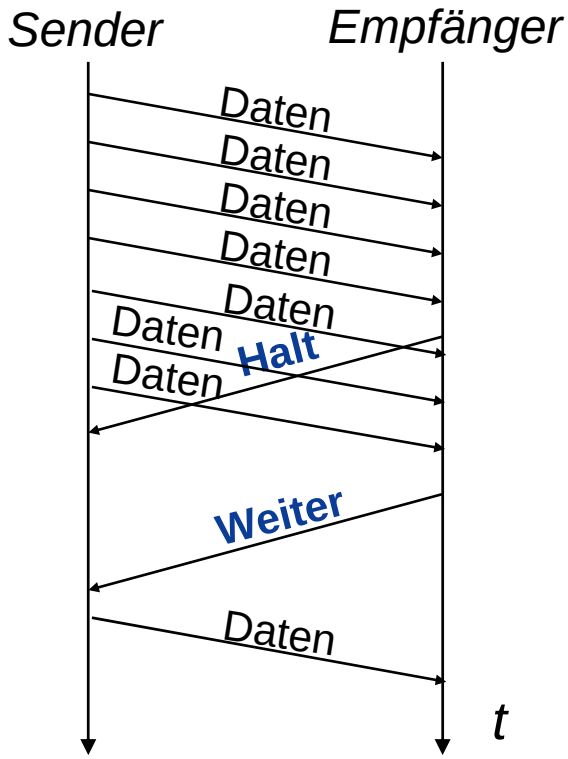


Flusssteuerung

→ Halt-/Weiter-Meldungen

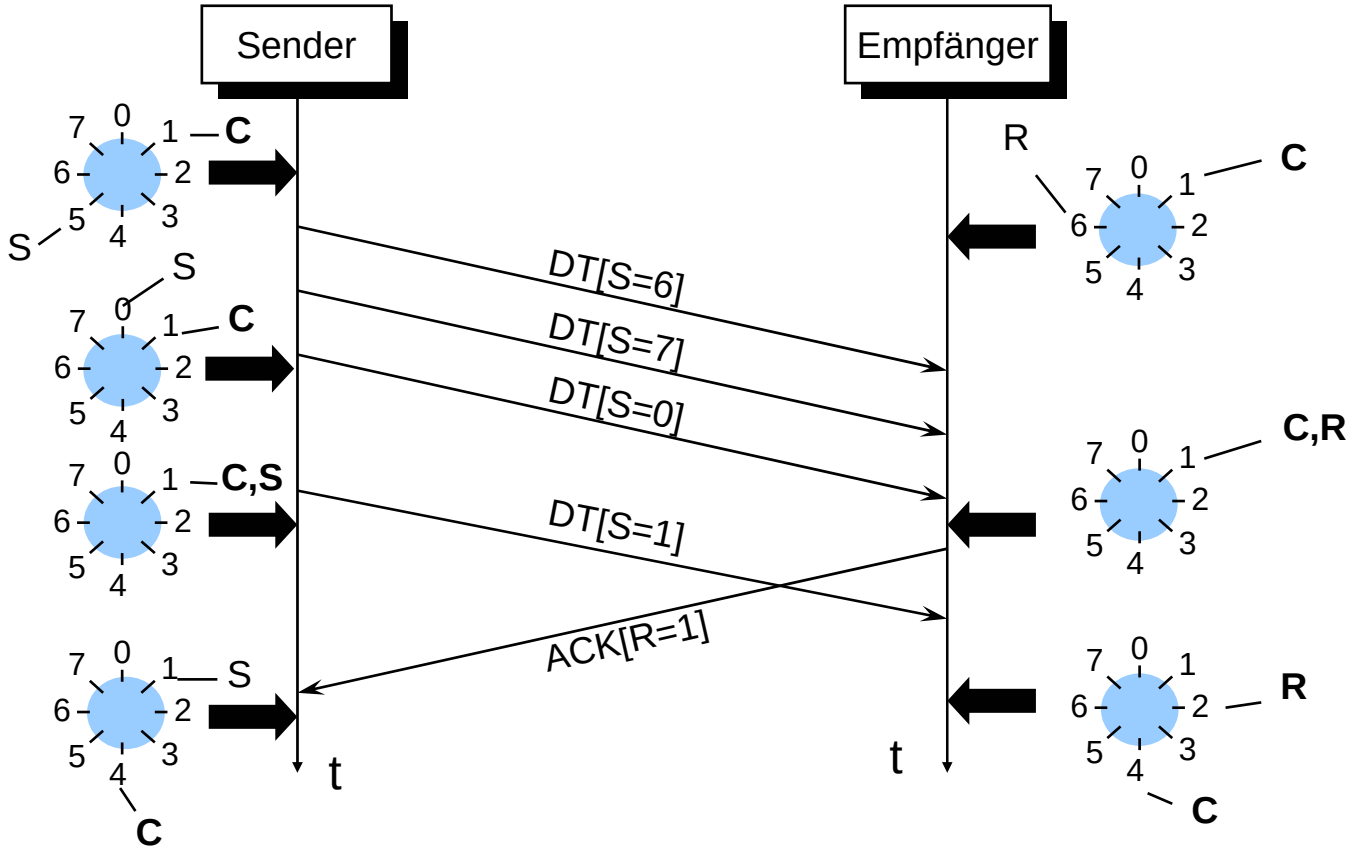
- *Einfachste Methode*
  - Sender-Empfänger-Flusssteuerung
    - Meldungen
      - **Halt**
      - **Weiter**
  - Kann der Empfänger nicht mehr Schritt halten, schickt er dem Sender eine **Halt**-Meldung.
  - Ist ein Empfang wieder möglich, gibt der Empfänger die **Weiter**-Meldung.

- *Beispiel: Protokoll XON/XOFF*
  - Mit ISO 7-Bit-Alphabetzeichen.
  - XON ist DC1 (Device Control 1).
  - XOFF ist DC3 (Device Control 3).
  - Nur auf Vollduplex-Leitungen verwendbar.



Flusssteuerung
→ Sliding Window

- Darstellung zeigt Fenstermechanismus (Kredit 4) für eine Senderichtung

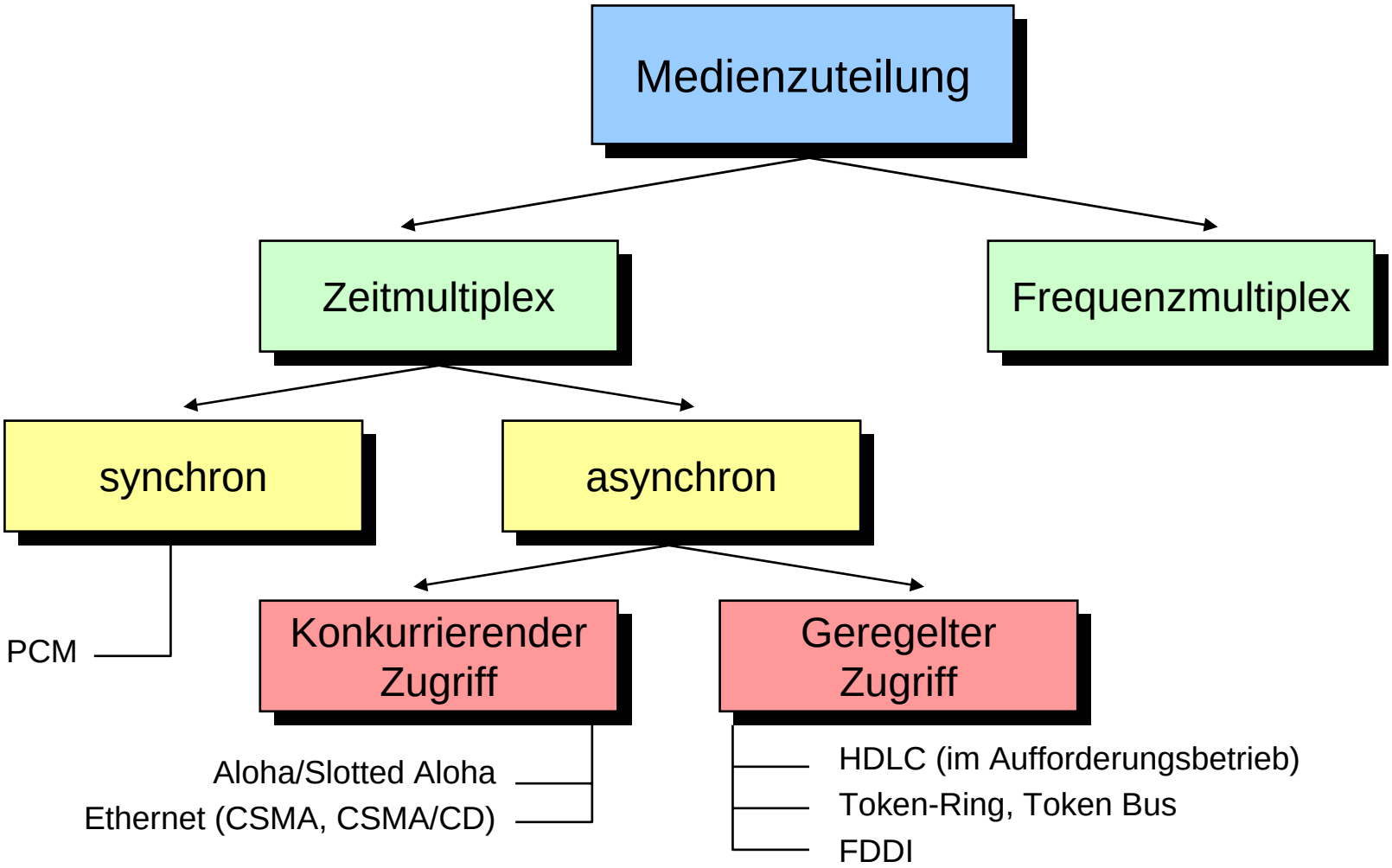


S: Sendefolgenummer (des zuletzt gesendeten Pakets)
R: Nächste erwartete Sendefolgenummer = Quittierung bis Folgenummer R-1
C: Oberer Fensterrand (maximal erlaubte Sendefolgenummer)

Nachteil: Kopplung von Fluss- und Fehlerkontrolle.

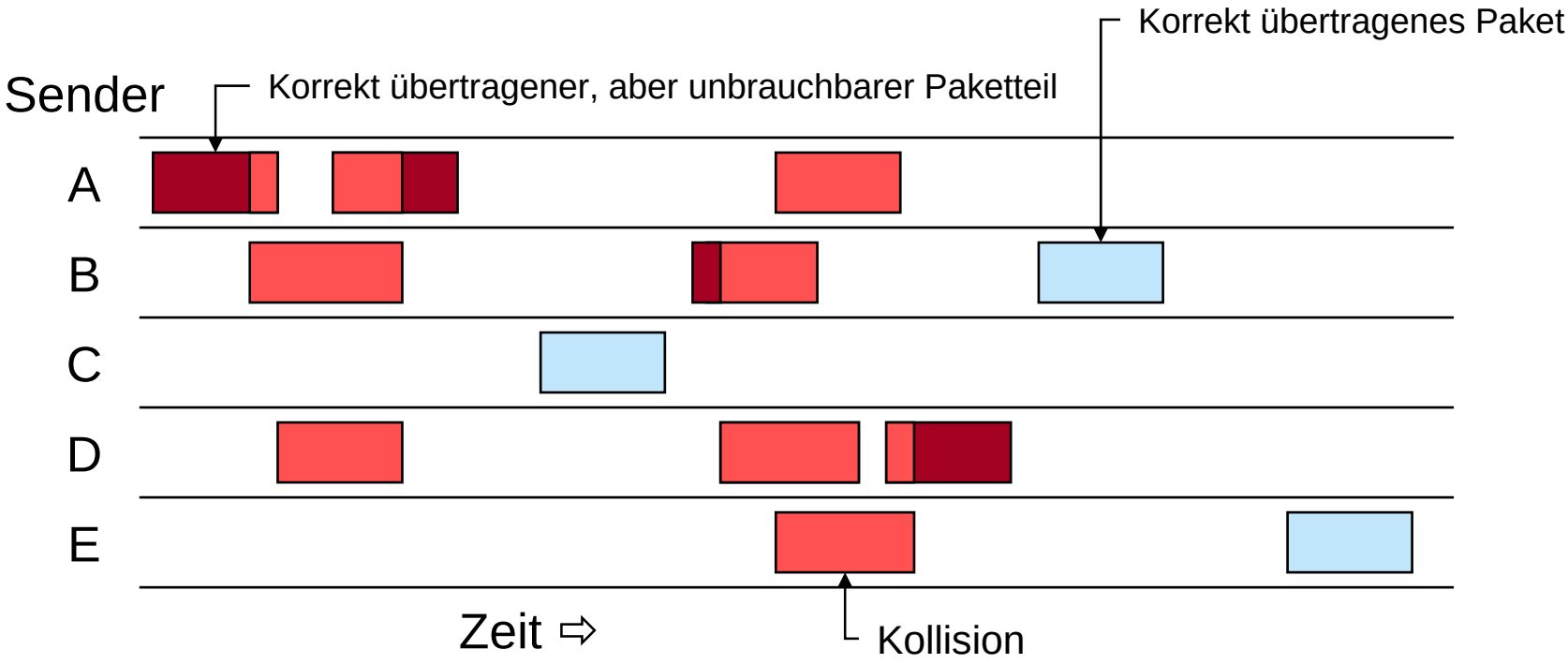
LAN/MAN-Zugriffsverfahren

- Problem: Mehrere Stationen treten als Dienstnehmer eines einzigen physikalischen Mediums auf (shared medium)



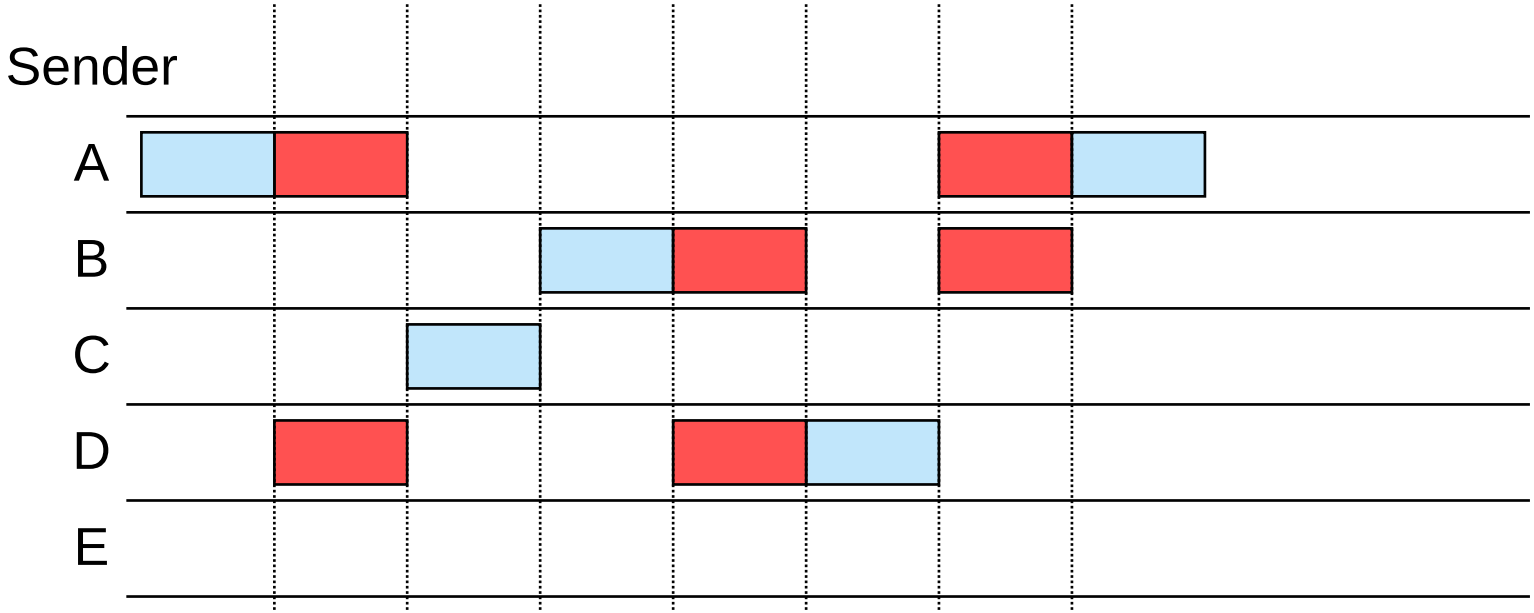
Konkurrierender Zugriff
→ Aloha

- Stationen übertragen genau dann Daten, wenn welche gesendet werden müssen.
- Kollisionen führen zu gestörten Rahmen.
- Empfänger schickt Bestätigung, wenn er einen an ihn adressierten Rahmen korrekt empfangen hat.
- Einsatz beispielsweise im GSM.
- Maximale Kanalauslastung 18%.



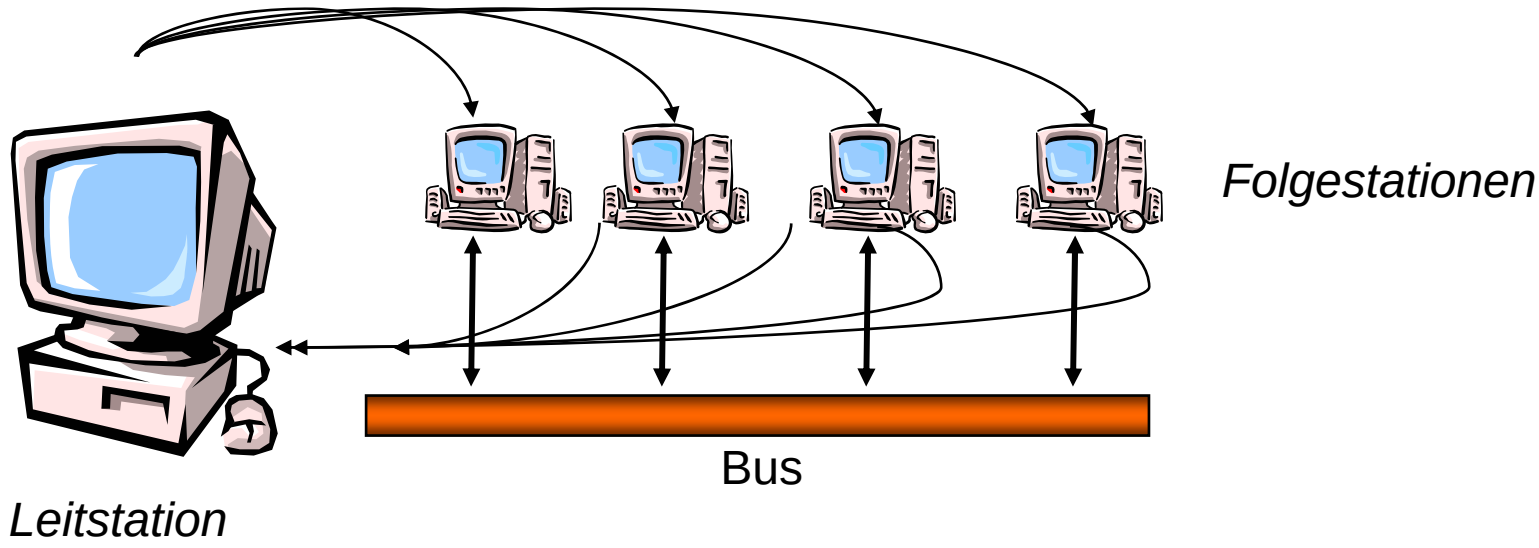
Konkurrierender Zugriff
→ Slotted ALOHA

- Pakete fester Länge werden in festen Zeitabschnitten (Slots) übertragen. Dies erfordert einheitliche Zeitbasis (z.B. durch zentrale Uhr) zur Synchronisation der Stationen
- Paketübertragung nur zu Beginn eines Zeitslots (slot boundary). Es können nur total überlappende Kollisionen auftreten. Damit verkürzt sich die Kollisionszeit von zwei auf eine Paket-Übertragungszeit.
- Maximale Kanalauslastung auf 36% verbessert!



Kontrollierter Zugriff
→ Aufrufbetrieb

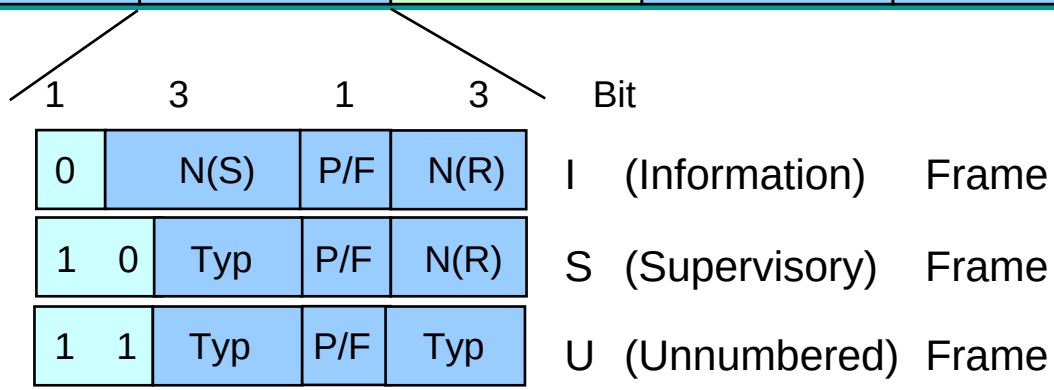
- eine dedizierte „intelligente“ Leitstation
- u.U. mehrere „dumme“ Folgestationen
- gekoppelt über Busstruktur
- Leitstation fragt Folgestationen gemäß Abfragetabelle („Polling Table“) ab
- Folgestationen antworten nur nach Aufforderung
- jegliche Kommunikation erfolgt über Leitstation



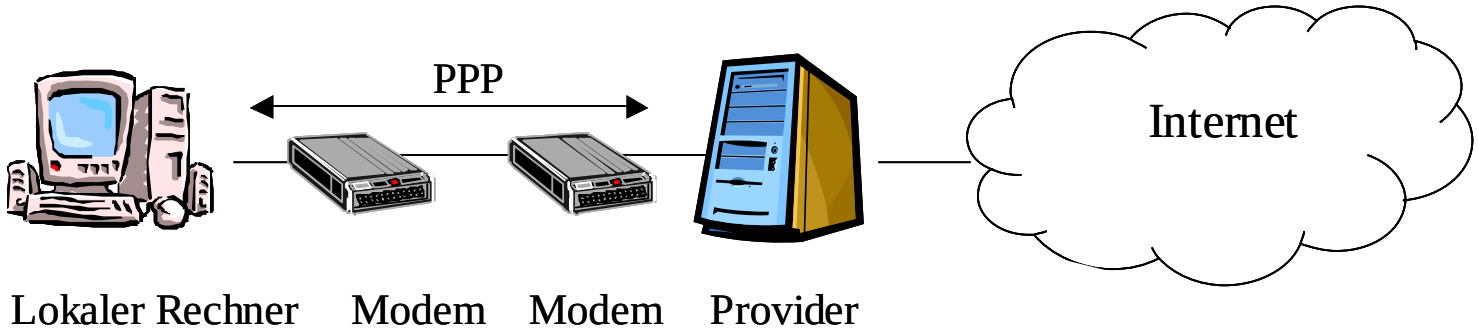
HDLC (High Level Data Link Control)

- **Eigenschaften:**
  - Pakete (Blöcke) werden durch die Blockbegrenzung *01111110* eingeschlossen
  - Im Paket darf diese Sequenz nicht vorkommen ⇨ Bitstuffing
  - Im Steuerfeld sind Sende-/Empfangsfolgenummern enthalten
    ⇨ Quittierung, Flusssteuerung.
  - Blockprüfung erfolgt nach dem CRC-Verfahren
    ⇨ Fehlererkennung.

Block-begrenzung	Adress-feld	Steuer-feld	Daten-feld	Blockprüf-feld	Block-begrenzung
01111110	*8 bit*	*8 bit*	*n bit*	*16 bit*	*01111110*



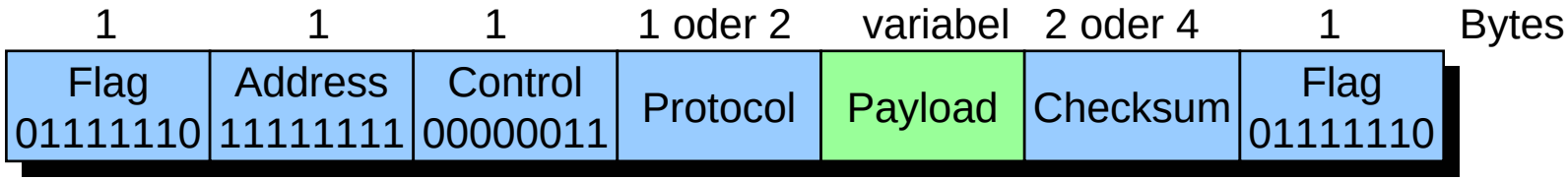
PPP (Point to Point Protocol)



- Ein großer Teil des Internets beruht auf Punkt-zu-Punkt-Verbindungen:
  - Verbindungen im WAN zwischen Routern / Heimanbindung über Modem und Telefonleitung
- SLIP (serial line IP, RFC 1055): keine Fehlererkennung, nur IP, keine dynamische Adresszuweisung, keine Authentifikation
- PPP (RFC 1661/1662):
  - Schicht-2-Rahmenformat mit Fehlererkennung, Rahmenbegrenzung
  - Steuerprotokoll (LCP, Link Control Protocol) zum Verbindungsaufbau, Verbindungstest, Verbindungsverhandlung, Verbindungsabbau
  - Verhandlung von Schicht-3-Optionen unabhängig vom Schicht-3-Protokoll (separates NCP, Network Control Protocol, für alle unterstützten Schicht-3-Protokolle)

PPP – Paketformat

- Paketformat an HDLC angelehnt



- zeichenorientiert (anstatt bitorientiert), d.h. die Länge des Nutzdatenfeldes endet immer an einer Byte-Grenze
- Codetransparenz durch Character Stuffing
- typischerweise werden nur *unnumbered*-frames übertragen, bei hohen Fehlerraten (Mobilkommunikation) kann jedoch auch der zuverlässigere Modus mit Sequenznummern und Bestätigungen gewählt werden
- als Protokolle im Nutzlast-Feld sind u.a. IP, AppleTalk, IPX definiert
- falls nicht anderweitig verhandelt, ist die maximale Länge der Nutzlast auf 1500 Byte begrenzt
- durch zusätzliche Verhandlung kann der Paketkopf verkleinert werden

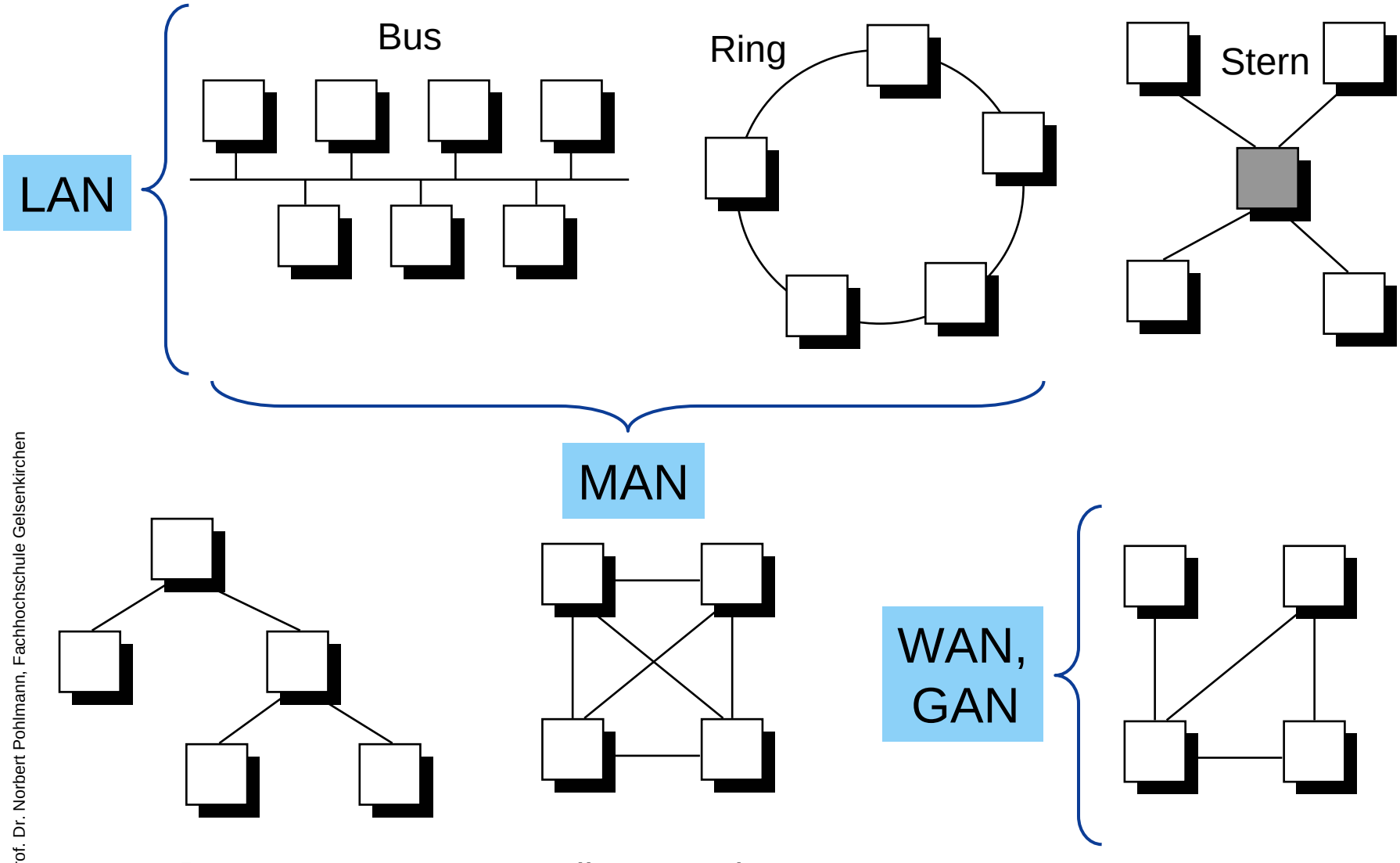
Inhalt

- Ziele
- Einleitung
- Protokollmechanismen
  - Synchronisation, Codetransparenz
  - Fehlererkennung/-behandlung
  - Flusssteuerung, Medienzugriff
- **Lokale Netze**
  - **Ethernet**
  - **Weiterentwicklungen**
- Zusammenfassung

Netzwerktypen

- **LAN – Local Area Network:**
  - geringe Ausdehnung von wenigen Kilometern
  - große Übertragungsraten im Bereich von 10 Mbit/s bis Gbit/s möglich
  - meist von privaten Firmen und Privatleuten betrieben
- **MAN – Metropolitan Area Network**:
  - erstreckt sich meist über das Gebiet einer Stadt
  - viele Knoten bei hohen Übertragungsraten und geringen Ausfallzeiten
- **WAN – Wide Area Network:**
  - in Ausdehnung nicht begrenztes Netzwerk
  - meist von staatlichen Posteinrichtungen oder TK-Gesellschaften betrieben
- **GAN – Global Area Network:**
  - weltumspannende Netze
  - i.a. mithilfe interkontinentaler Satellitenverbindungen
  - auch Netzverbünde, wie z.B. das Internet

Verbindungstopologien



Aufgabenteilung der LAN-Schichten

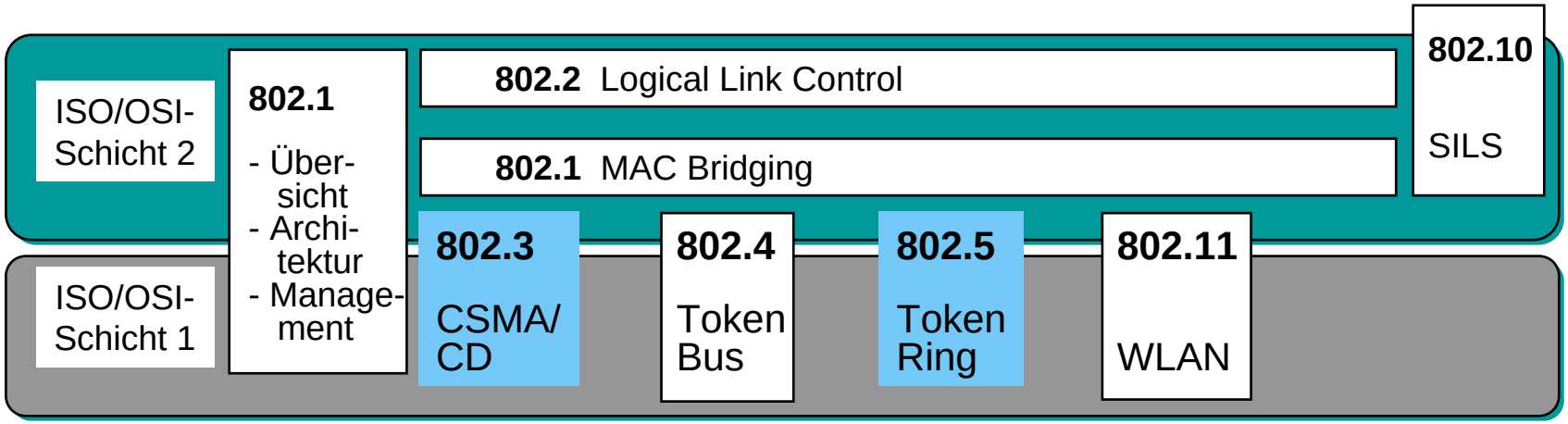
3 **IP und andere**

2b **Logical Link Control (LLC)**
(einheitlich für alle Medien)
- ❒ Verfälschungssicherung
- ❒ Verlustsicherung
- ❒ Reihenfolgesicherung
- ❒ Flusskontrolle
- ❒ Strukturierung der Übertragung

2a **Medium Access Control (MAC)**
(Zugangskontrolle für geteiltes Medium)
- ❒ konkurrierender Zugriff
- ❒ kontrollierter Zugriff

1 **Medien**
- ❒ Verdrillte Kupferadern (von 4 Mbit/s bis 1.000 Mbit/s)
- ❒ Koaxialkabel (10 Mbit/s; theoretisch mehr, doch nicht genutzt)
- ❒ Glasfaser (9,6 Gbit/s, im Laborbetrieb bereits im Tbit/s-Bereich)

LAN/MAN
→ aktuelle Standardisierung nach IEEE 802

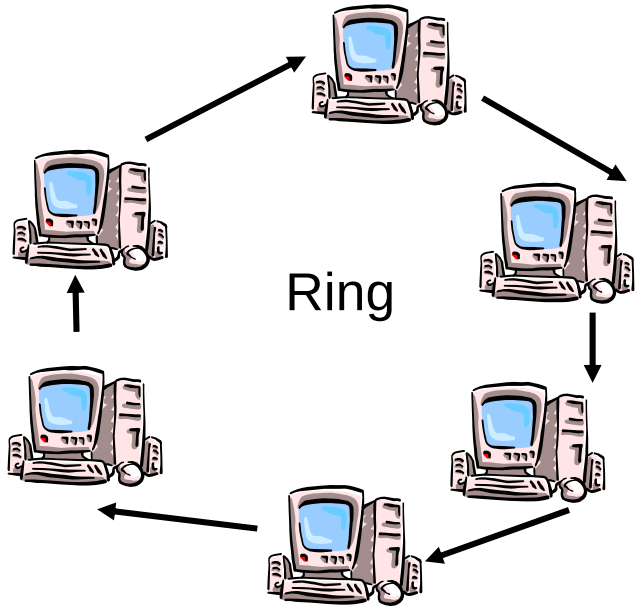


Themen:

802.1: Zusammenhang der Standards und MAC Bridging
802.2: Logical-Link-Control-Dienste/Protokolle (LLC)
802.3: CSMA/CD-Protokoll auf Bustopologie
802.4: Token-Bus-Protokoll auf Bustopologie
802.5: Token-Ring-Protokoll auf Ringtopologie
802.10: Interoperable LAN/MAN Security: Sicherheitsstruktur für 802-Protokolle
802.11: Wireless LAN

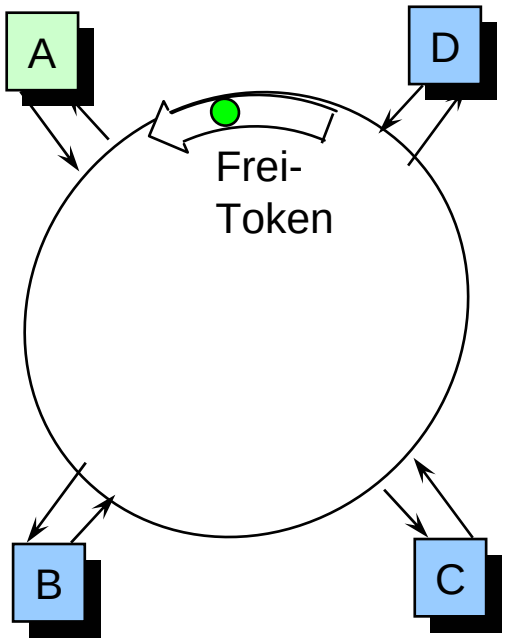
LAN
→ Token Ring (IEEE 802.5)

- Stationen sind Punkt-zu-Punkt zu einem **Ring** verbunden.
- Jede Station hat somit Vorgänger und Nachfolger.
- Stationen sind aktiv an das Medium gekoppelt.
- Einkommende Daten werden regeneriert und evtl. modifiziert.
- Zuteilung des Senderechts erfolgt durch zirkulierendes Steuerpaket, den **Token.**

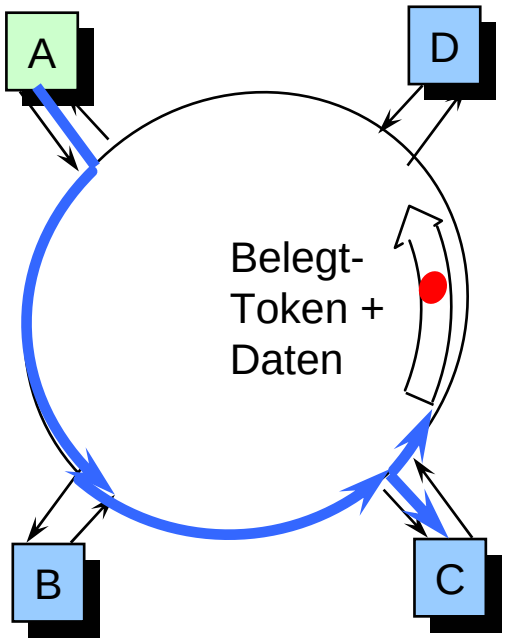


- Kontrollierter Zugriff durch zirkulierendes Senderecht.
- Eine Station, die den Frei-Token empfängt, darf Daten verschicken.
- Die verschickten Daten kommen aufgrund der Ringstruktur wieder bei der sendenden Station an, die diese wieder vom Ring nimmt.
- Danach gibt sie den Token an die Nachfolgestation weiter.
- Es wird ein umfangreiches Token-Management benötigt.

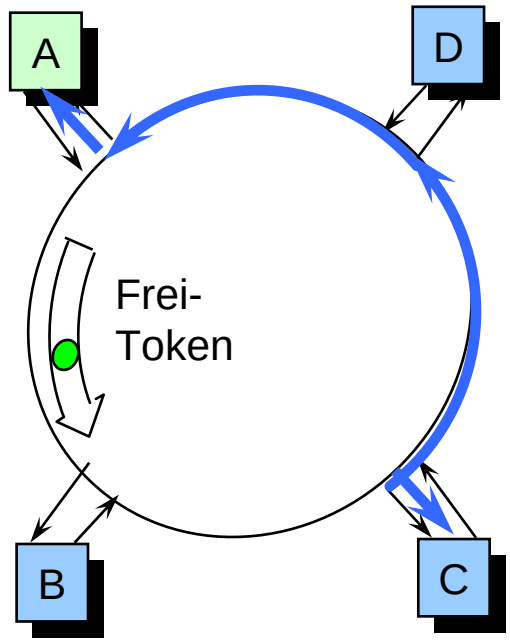
Token-Ring
→ Ablaufbeispiel



- Frei-Token kreist
- A hat Sendewunsch



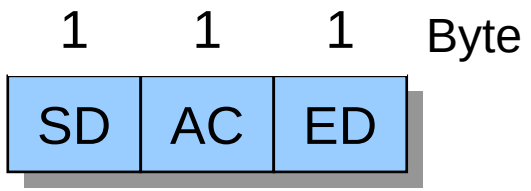
- A hat Token belegt
- A sendet an C
- C kopiert



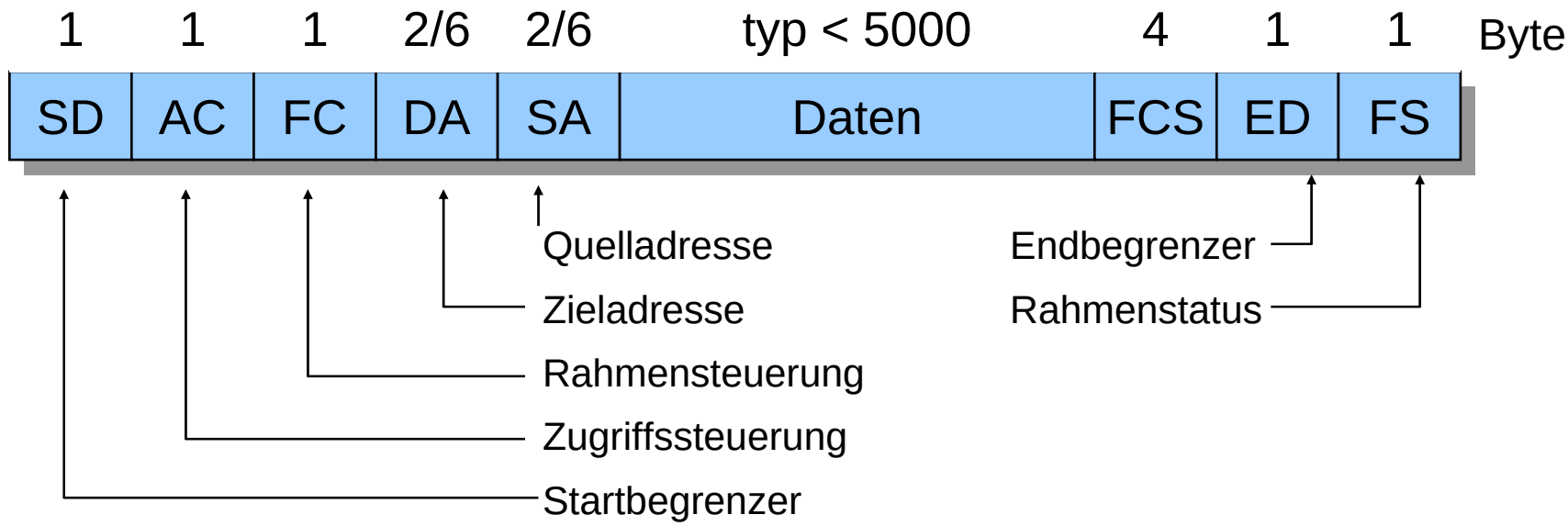
- A vernichtet Daten
- C kopiert und setzt Quittungsbits
- Token wird von A auf frei gesetzt

Token-Ring
→ Paketformat

Tokenformat:



Datenrahmenformat:



Token-Ring und die Weiterentwicklungen

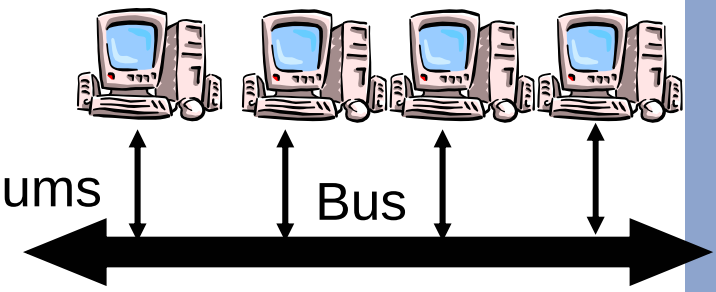
- Wichtige Eigenschaft:
  - garantierte zeitliche Obergrenze für Medienzugriff
- Ursprüngliche Realisierungen:
  - 4 Mbit/s
  - 16 Mbit/s
- Ähnliches Verfahren:
  - **Token Bus:** Bustopologie, d.h. Vorgänger/Nachfolger wird frei festgelegt, Token muss adressiert werden.
- Weiterentwicklung FDDI:
  - 100 Mbit/s
  - Ausdehnung bis 100 km
  - glasfaserbasiert
  - Doppelring zur Ausfallsicherheit
  - isochroner Verkehr möglich

CSMA/CD
→ Ethernet

- Alle Stationen sind an einen gemeinsamen Bus angeschlossen.
- Keine ist eine ausgezeichnete Station.
- Jede Station kann zu einem beliebigen Zeitpunkt senden.

⇨ **Kollisionen mehrerer Sendungen zerstören übertragene Daten!**

- Vermeidung von Kollisionen:
  Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



- Grundlagen von CSMA/CD:
  - vor dem Senden: Abhören des Mediums (***Listen Before Talk***).
  - wenn Medium frei: Beginne mit Senden.
  - während des Sendens: Abhören des Mediums (***Listen While Talk***).
  - wird Kollision erkannt: Breche Sendevorgang ab und benachrichtige die anderen angeschlossenen Stationen.

CSMA/CD
→ Ablaufbeispiel

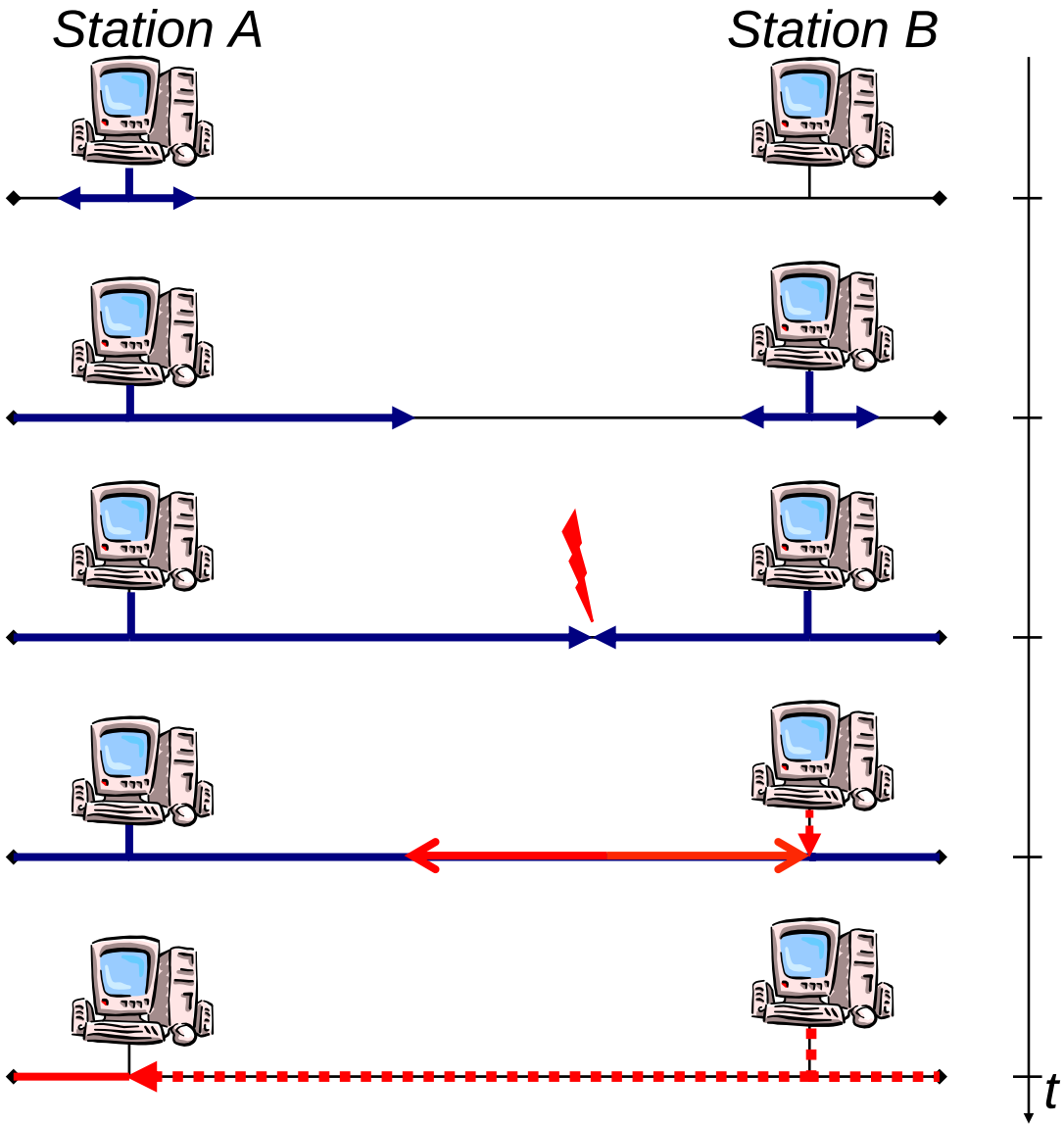
Station A beginnt zu senden, da Medium frei.

Station B beginnt zu senden, da Medium frei scheint.

Es kommt zur Kollision der Datenpakete.

Station B erkennt Kollision, bricht Sendevorgang ab und schickt Jamming-Signal.

Jamming-Signal erreicht Station A, die auch abbricht.



CSMA/CD
→ CSMA – Carrier Sense Multiple Access

- Die CS (Carrier Sense) Verfahren hören im Gegensatz zu Aloha das Medium ab, bevor sie zu senden beginnen.
- Dadurch lässt sich vermeiden, dass eine sendende Station gestört wird.
- Es kann aber auch passieren, dass im Augenblick des Sendewunsches aufgrund der endlichen Signalausbreitungs-geschwindigkeit keine andere Sendung erkannt wird, obwohl eine Station bereits sendet.
- In diesem Fall treffen sich die Signale irgendwo auf dem Medium und überlagern sich.
- Die beiden sendenden Stationen bemerken die Kollision entweder direkt an den Spannungsspitzen (durch Überlagerung) und auf jeden Fall daran, dass innerhalb der Zeit tL (Laufzeit eines Signals von einem Ende zum anderen, auch als propagation delay bezeichnet) gestörte Signale ankommen.

CSMA/CD
→ CSMA/CD – CSMA with Collision Detection (1/4)

- Bei reinen CSMA-Verfahren erkennt eine Station zwar eine Kollision, macht aber weiter nichts.
- Bei CD (Collision Detect) Verfahren hört jeder Sender während dem Senden seiner Nachricht mit.
- Er erkennt dann, ob das gesendete von ihm stammt, oder ob es sich um Signale einer Kollision handelt.
- CSMA/CD benutzt somit CSMA und fügt noch die Kollisionserkennung hinzu (diese Variante wird vereinfachend oft auch als **Ethernet** bezeichnet).
- Der Ablauf gestaltet sich wie folgt:
  - Wenn eine Station senden will, hört sie das Medium ab.
  - Ist es frei, so wartet die Station noch 9,6 μs (Interframe Spacing) und beginnt dann sofort zu senden, ohne noch einmal zu lauschen.
  - Die Station hört während des Sendens mit, ob sie andere Signale außer ihren eigenen hört.

CSMA/CD
→ CSMA/CD – CSMA with Collision Detection (2/4)

- Wenn eine (beliebige) Station bemerkt (an Spannungsspitzen und Codeverletzungen), dass eine Kollision auftritt, so sendet sie ein sogenanntes Jamming-Signal.
- Dieses soll allen Stationen ermöglichen, die Kollision zu erkennen und dauert 4,8 µs.
- Nach Erhalt des Jamming-Signals stoppen alle Sender ihre Sendung.
- Eine Kollision wird auf jeden Fall innerhalb einer Slot-Time, der doppelten Signallaufzeit von einem Ende zum anderen erkannt.
- Ein Sender kann sich also sicher sein, dass nach Ablauf einer Slot-Time, wenn keine Kollision aufgetreten ist, auch keine mehr auftritt.
- Die Sendung muss daher aber auch mindestens so lange wie eine Slot-Time dauern.

CSMA/CD
→ CSMA/CD – CSMA with Collision Detection (3/4)

- Wenn eine sendende Station eine Kollision erkannt hat und aufhört zu senden, wartet sie eine gewisse Zeit lang und hört dann das Medium wieder ab.
- Es kann natürlich weiterhin zu Kollisionen kommen, vor allem weil während des Wartens noch einige sendewillige Stationen dazu kommen können.
- Nach 16 erfolglosen Versuchen bricht die Station ab und verwirft das Paket.
- Die Wartezeit einer Station nach einem erfolglosen Versuch errechnet sich nach dem exponentiellen Backoff-Algorithmus.
- Dieser berechnet die Anzahl der Slot-Times, die gewartet werden müssen.
- Nach der ersten Kollision zieht die Station eine Zufallszahl aus dem Bereich [0, 2] und wartet diese Anzahl von Slots.
- Nach der i-ten Kollision zieht sie eine Zufallszahl aus dem Intervall [0, 2i] und wartet diese Anzahl von Slots.
- Ab dem 10ten Wiederholungsversuch bleibt das Intervall allerdings immer bei [0, 210].

CSMA/CD
→ CSMA/CD – CSMA with Collision Detection (4/4)

- Man wartet somit immer ein Vielfaches der Slot-Time.
- Wenn zwei Stationen die gleiche Zufallszahl ziehen, dann gibt es wieder eine Kollision.
- Der exponentielle Anstieg des Bereichs garantiert, dass bei wenigen Stationen diese nicht allzu lange warten müssen.
- Und wenn es viele Stationen sind, so wird nach einigen Schritten jede voraussichtlich eine andere Zufallszahl ziehen.
- Es ist wichtig, dass immer eine Station zügig senden kann, weil bei einer längeren Wartezeit immer mehr sendewillige Stationen hinzukommen.
- Dies ist auch der Fall, wenn eine Station sendet.
- Wenn sie lange sendet, so merken dies die anderen und ihre Warteschlangen füllen sich.
- Wenn eine Station einmal das Medium hat (die Slot-Time von 51,2 µs entspricht 64 Byte), so kann sie weiter senden, ohne gestört zu werden.
- Man hat deshalb die Paketlänge begrenzt.
- 1526 Byte stellen eine guten Wert dar, der es einerseits einer Station ermöglicht, einen großen Block zu senden, andererseits müssen die anderen Stationen nicht zu lange auf ein freies Medium warten.

CSMA/CD
→ Paketformat nach IEEE 802.3

PR 56 bit	SD (8 bit)	DA (16/48 bit)	SA (16/48 bit)	Länge (16 bit)	Data (≤12.000 bit)	PAD (0-368 bit)	FCS (32 bit)

PR = Präambel zur Synchronisation (1010101010...)
SD = *Start-of-frame Delimiter* zeigt Blockbeginn an (10101011)
DA = *Destination Address*, Zieladresse
SA = *Source Address*, Herkunftsadresse
Länge = Anzahl der Oktette im Datenfeld
Data = Datenfeld, das maximal 1.500 Byte umfassen darf
PAD = *Padding*, um zu kurze Datenfelder auf die nötige Länge zu ergänzen
FCS = *Frame Check Sequence*, Polynomdivision mittels CRC32-Polynom zur Fehlererkennung

Wichtig:
Einzelne Realisierungen von CSMA/CD (z.B. Ethernet 1.0, Ethernet 2.0 oder IEEE 802.3) verwenden manche Felder in leicht unterschiedlicher Bedeutung!

Vergleich von CSMA/CD und Token Ring

CSMA/CD

- Vorteile
  - einfaches Protokoll
  - Installation im laufenden Betrieb einfach möglich
  - passive Kabel
  - keine Verzögerung bei niedriger Last
- Nachteile
  - minimale Rahmengröße von 64 Byte, maximal 1500 Byte
  - keine Prioritäten
  - nicht deterministisch, deshalb kein Echtzeitbetrieb möglich
  - begrenzte Kabellänge
  - geringe Effizienz durch viele Kollisionen, problematisch bei höherer Last

Token Ring

- Vorteile
  - sehr guter Durchsatz und hohe Effizienz unter hoher Last
  - Prioritäten möglich
  - kurze Rahmen möglich
  - Echtzeitbetrieb möglich
- Nachteile
  - zentralisierter Monitor zur Ringüberwachung
  - unnötige Verzögerung unter niedriger Last
  - fehlerhafter Monitor kann den gesamten Ring in Mitleidenschaft ziehen

CSMA/CD
→ Technische Realisierungen

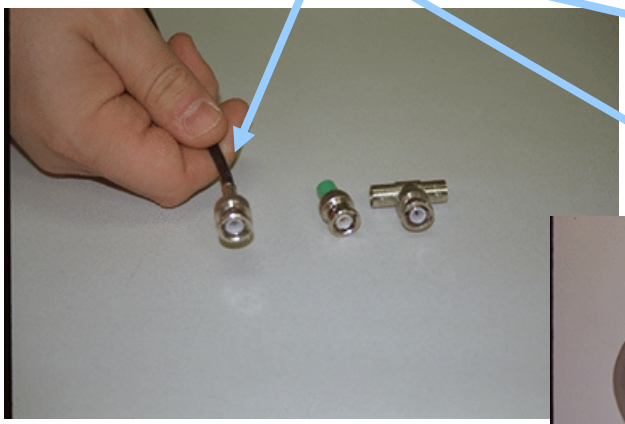
Übertragungsrate 10 Mbit/s

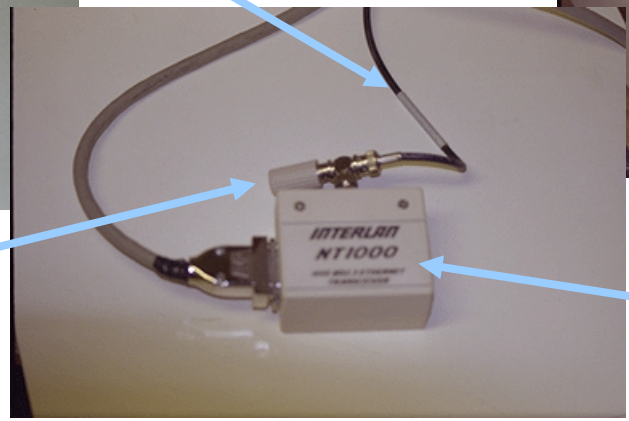
Bezeichnung	Kabel	Segmentlänge	Knoten pro Segment
10Base5 (Thick Ethernet)	Dickes Koax	Max. 500m	Max. 100
10Base2 (Thin Ethernet)	Dünnes Koax	Max. 185m	Max. 30
10BaseT	Verdrilltes Paar (Stern!)	Max. 100m	Max. 1.024
10BaseF	Glasfaser	Max. 2.000m	Max 1.024

CSMA/CD

→ Technische Realisierung: 10Base2

- **10Base2, Thin Wire Ethernet, Cheapernet**
  - 10Base2: 10 MBit/s, Basisbandübertragung, 185 Meter-Segmente
  - 30 Teilnehmer pro Segment im Abstand von mindestens 0,5 m
  - Transceiver meist direkt auf Ethernet-Adapter im Rechner (BNC-Buchse, T-Stück)
  - Koaxialkabel





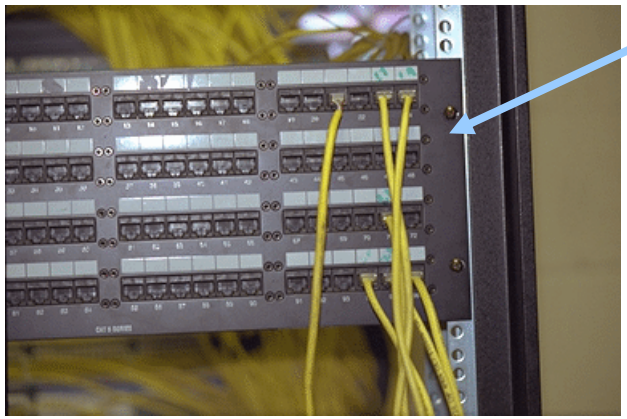
Abschlusswiderstand zur Signalvernichtung

Transceiver

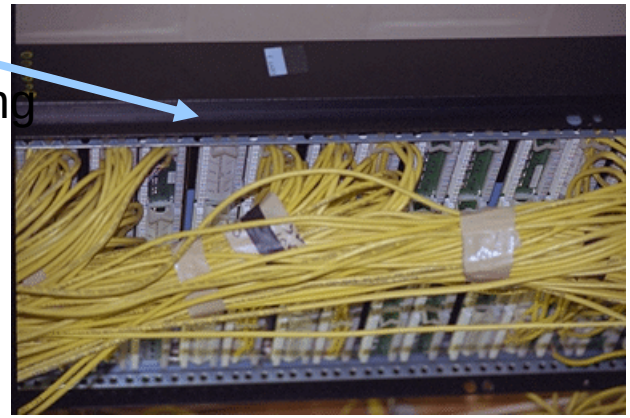
CSMA/CD

→ Technische Realisierung: 10Base-T

- **10Base-T, Twisted Pair**
  - 10 Mbit/s, Basisbandübertragung
  - Verdrillte Leitungen
  - Jede Station (max. 1024) ist über (max. 100 m) Punkt-zu-Punkt-Verbindung an zentralen Verteiler (Hub, Switch) angeschlossen
  - Telefonleitung in USA einsetzbar



„patch-panels“ für die Sternverkabelung



Weiterentwicklungen
→ Fast Ethernet (IEEE 802.3u)

- Sterntopologie
- Übertragungsleistung 100 Mbit/s

Bezeichnung	Kabel	Segmentlänge	Vorteile
100Base-T4	Vier verdrillte Adernpaare	Max. 100m	Gängige Kabel
100Base-TX	Zwei verdrillte Adernpaare	Max. 100m	Vollduplex bei 100 Mbit/s
100Base-F	Glasfaser	Max. 800m	Vollduplex, längere Strecken

Weiterentwicklungen
→ Gigabit Ethernet (IEEE 802.3z)

- Sterntopologie
- Spezielle Codierung notwendig
- Übertragungsleistung 1.000 Mbit/s
- Auch ungeschirmte Doppeladern möglich (aber Standardisierung 802.3ab noch nicht abgeschlossen)

Bezeichnung	Kabel	Segmentlänge
1000Base-T	4 ungeschirmte Adernpaare (UTP-5)	100m
1000Base-CX	2 geschirmte Adernpaare	25m
1000Base-SX	Multimode-Glasfaser	2 - 550 m
1000Base-LX	Multi-/Mono-mode-Glasfaser	2 - 5.500 m

Inhalt

- Ziele
- Einleitung
- Protokollmechanismen
  - Synchronisation, Codetransparenz
  - Fehlererkennung/-behandlung
  - Flusssteuerung, Medienzugriff
- Lokale Netze
  - Ethernet
  - Weiterentwicklungen
- **Zusammenfassung**

Sicherungsschicht
→ Zusammenfassung

- Die ***Sicherungsschicht*** kann in zwei Unterschichten gegliedert werden.
- **Mediumzugangsschicht (MAC-Layer, Schicht 2a)**
  - Die Mediumzugangsschicht kommt dann zum Einsatz, wenn das Übertragungsmedium nicht für zwei Kommunikationspartner dediziert ist, sondern - wie z.B. bei LANs oder bei drahtloser Kommunikation üblich - viele potentielle Kommunikationspartner (Stationen) dasselbe Medium nutzen.
  - Die MAC-Schicht regelt dann die Zuordnung des gemeinsam benutzten Betriebsmittels Übertragungsmedium entweder eines festen Schemas (z.B. Zeitmultiplex, Frequenzmultiplex) oder dynamisch über sog. Vielfachzugriffsprotokolle (Reservierungsverfahren, stochastische Zugriffsverfahren).
- **Logical Link Layer (Schicht 2b)**
  Die Schicht 2b ist zuständig für die Zusammensetzung von Bitsequenzen zu Blöcken (Bytes, Frames), für die Blocksynchronisation, für die Fehlererkennung auf Block- bzw. Frameebene und gegebenfalls für die Fehlerkorrektur.

Netzwerke

→ Sicherungsschicht

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen