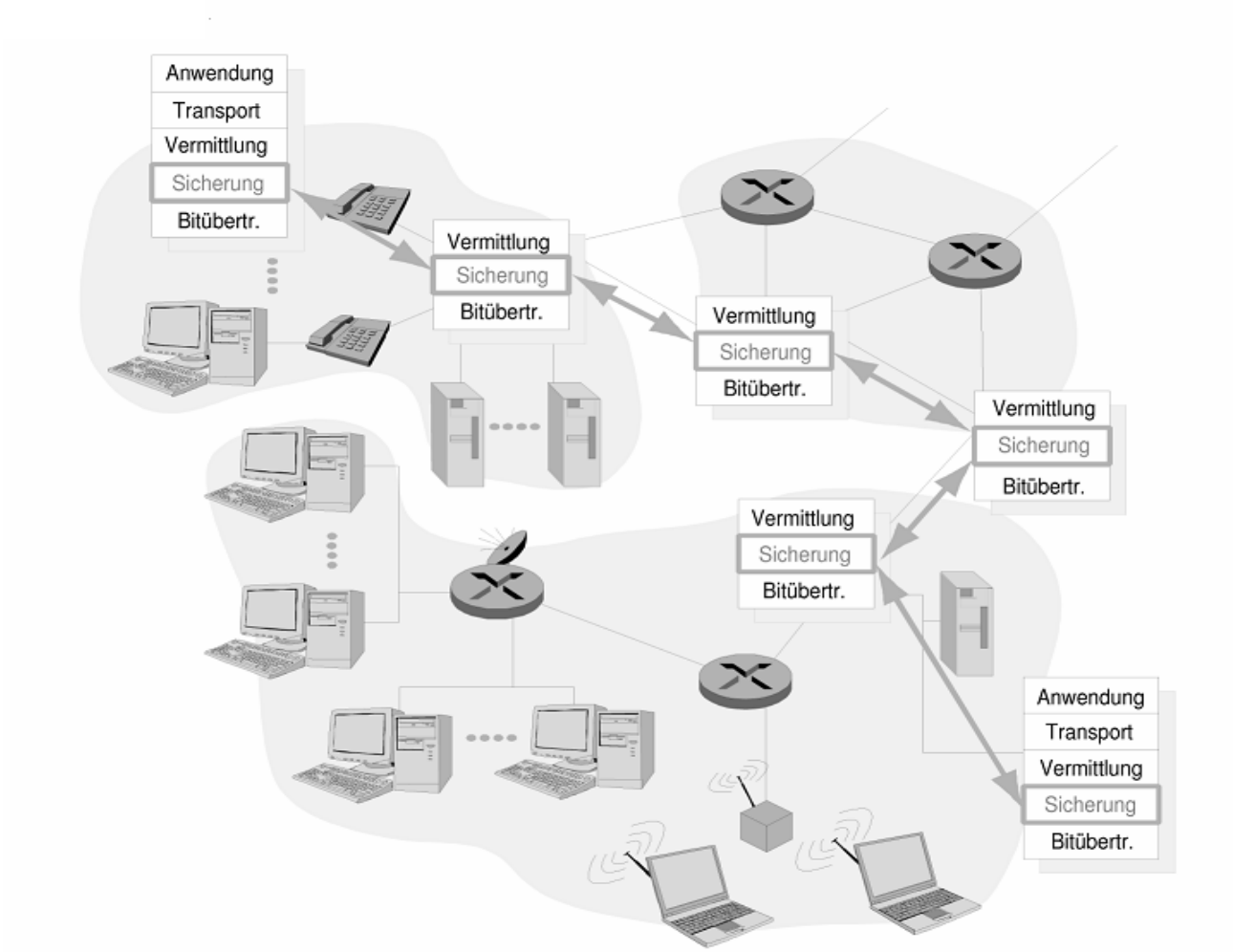
Kap. 4

Sicherungs-Schicht (Data – Link Schicht)

Sicherungs-Schicht (Data-Link-Schicht)



Rolle: Beförderung eines Datagramms von einem Knoten zum anderen via einer einzigen Kommunikationsleitung.

Dienste (allgemein) der Data-Link-Protokolle

- ***Leitungszugang***
  Es wird spezifiziert, wie ein Kanalzugriffs-Verfahren abläuft: z. B. Mehrfachzugriffsprotokolle

- ***Framing:*** spezifiziert die Struktur der Datagramm-Rahmen: Haeder- und Datenfelder

- ***Zuverlässige Übertragung***: Eventuell aufgetretene Fehler auf den Verbindungsleitungen oder Wireless-Verbindungen werden per Protokoll korrigiert.
  Sehr oft bieten DL-Protokolle diesen Dienst nicht an, da Verbindungs-leitungen sehr niedrige Bitfehler aufweisen.

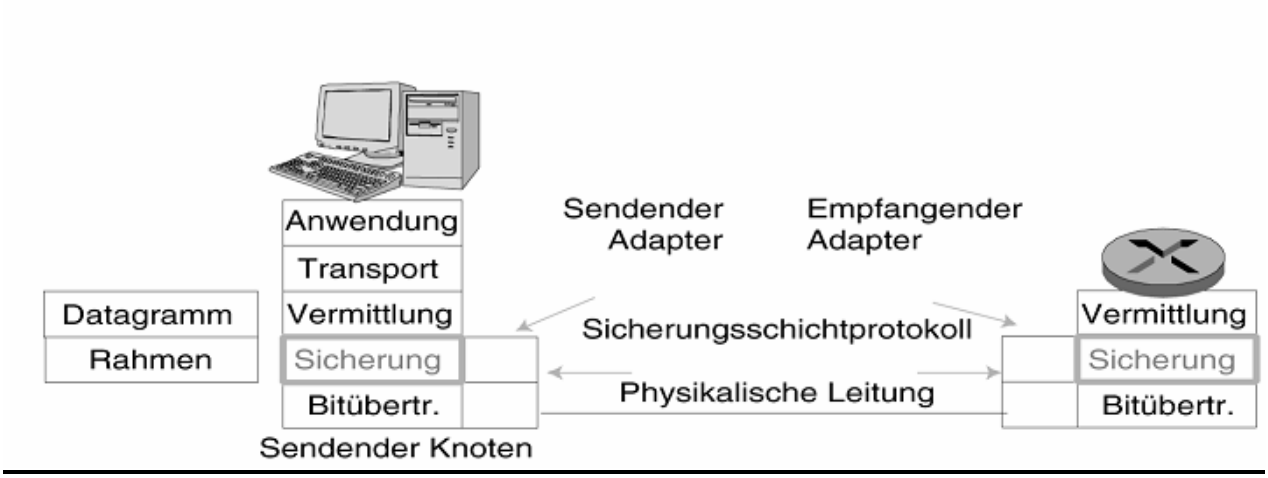
- ***Fluss-Kontrolle***: ähnlich wie im Falle von TCP-Protokoll

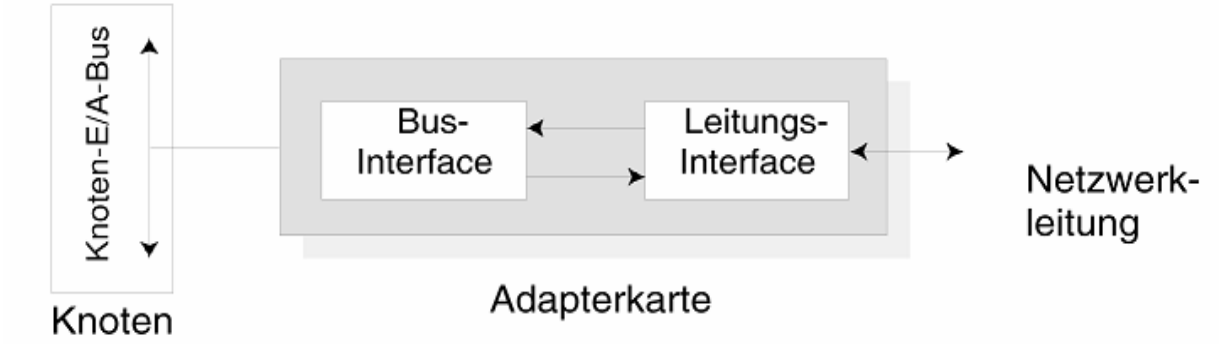
- ***Fehlererkennung***: Sie wird mittels CRC-Verfahren implementiert. Dieser Dienst ist sehr oft auf DL-Ebene im Rahmen verschiedener Protokolle implementiert, und zwar „Embedded“ in Hardware.

- ***Fehlerkorrektur:*** wird oft in Verbindung mit Fehlererkennung implementiert.

- ***Vollduplex:*** Erhöhung der gesamten Bandbreite durch Einsatz von parallelen Verbindungsleitungen (z. B. Server werden per Voll-Duplex-Ethernet-Leitungen ans Netz angeschlossen).

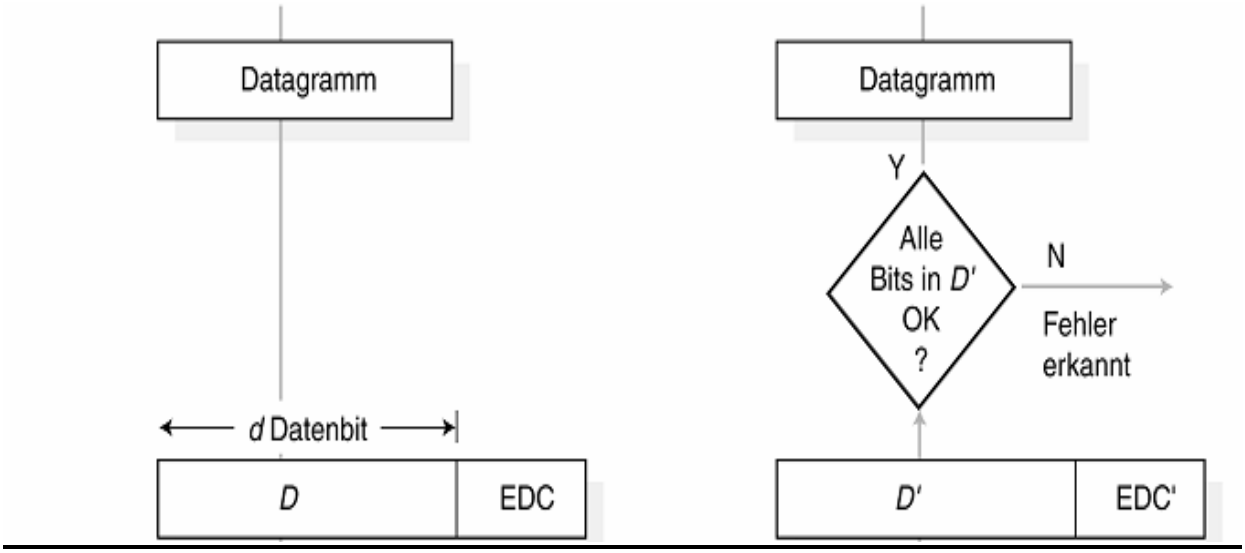
Implementierung der Data-Link-Schicht





- ***Netzwerk-Adapter*** ◘ auch NIC (Network Interface Controller) genannt.
- Viele DL-Protokolle → werden in Hardware (Chip-Set) implementiert.
- NIC muss Standard-Schnittstellen aufweisen, um nach oben bzw. nach unten mit den bereits vorhandenen Schichten zusammen arbeiten zu können.

Fehlererkennung und Fehlerkorrekturen



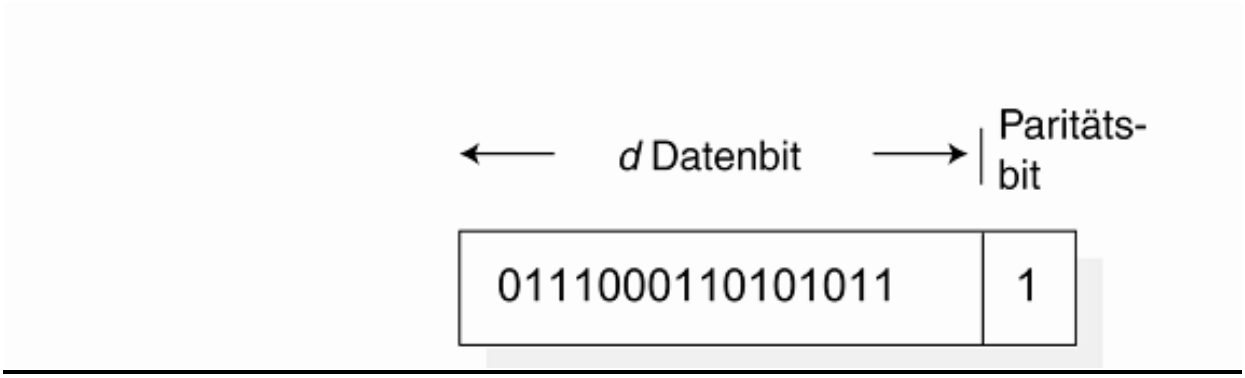
Prinzip:

- Beim Sender werden Data-Bits um ein Extra-Feld (EDC)mit Bits ergänzt. Diese Ergänzung erfolgt gemäß verschiedener „Korrektur-Techniken“.

- Der Empfänger prüft laut Prüfungs-Algorithmen die empfangenen Datenbits und Extra-Feld-Bits und stellt fest, ob während der Übertragung ein Fehler aufgetreten ist.

Fehlerkorrektur-Techniken

1. **Paritätsprüfung**

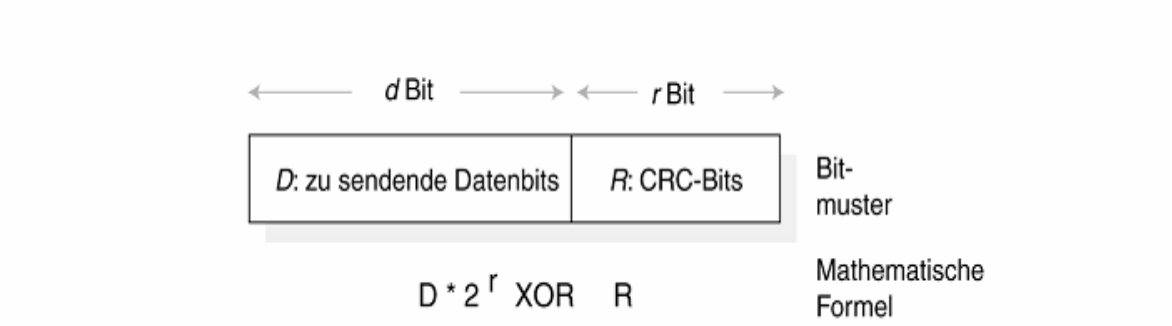


Nachteil:

Im Falle von „Burst“-Fehler (mehrere Bit-Fehler auf einmal) ist die Wahrscheinlichkeit unerkannter Fehler sehr hoch (über 50 %).

Lösung: zweidimensionale gerade Parität

2. **Cyclic Redundancy Check (CRC / Polynom codes)**



Prinzip:

- Empfänger und Sender einigen sich auf einen sog. „Generator" Bitmuster mit der Länge „r+1"

- M(ost)S(emnificative)B(it) von G ◘ 1

- Sender wählt zusätzliche ***r-Bits*** und hängt sie an ***D*** an, so dass:

„d+r" mit G genau teilbar ist (Modulo 2)

- Der Wert der zusätzlich gesendeten ***„r" Bits*** wird wie folgt berechnet:

R = Rest von (D x 2^r) / G

- Der Rest „R" (r - bit lang) wird zum Empfänger gesendet.

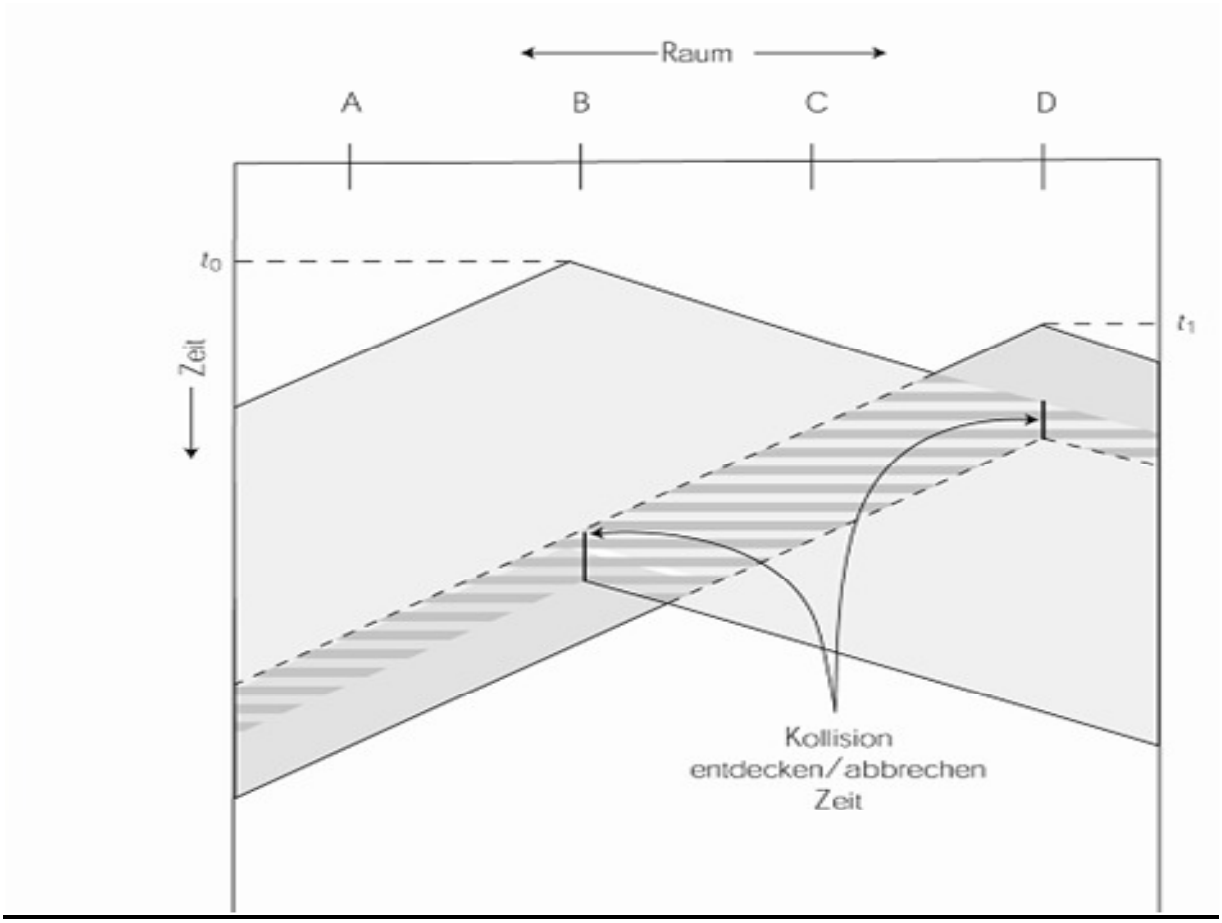
- Der Empfänger teilt die ***„d + r"*** empfangenen Bits durch **G**:

Formel: D x 2^r XOR R = nG

Falls der Rest ◘ 0

dann Fehler bei der Übertragung.

Mehrfach-Zugriffs-Protokolle: CSMA/CD

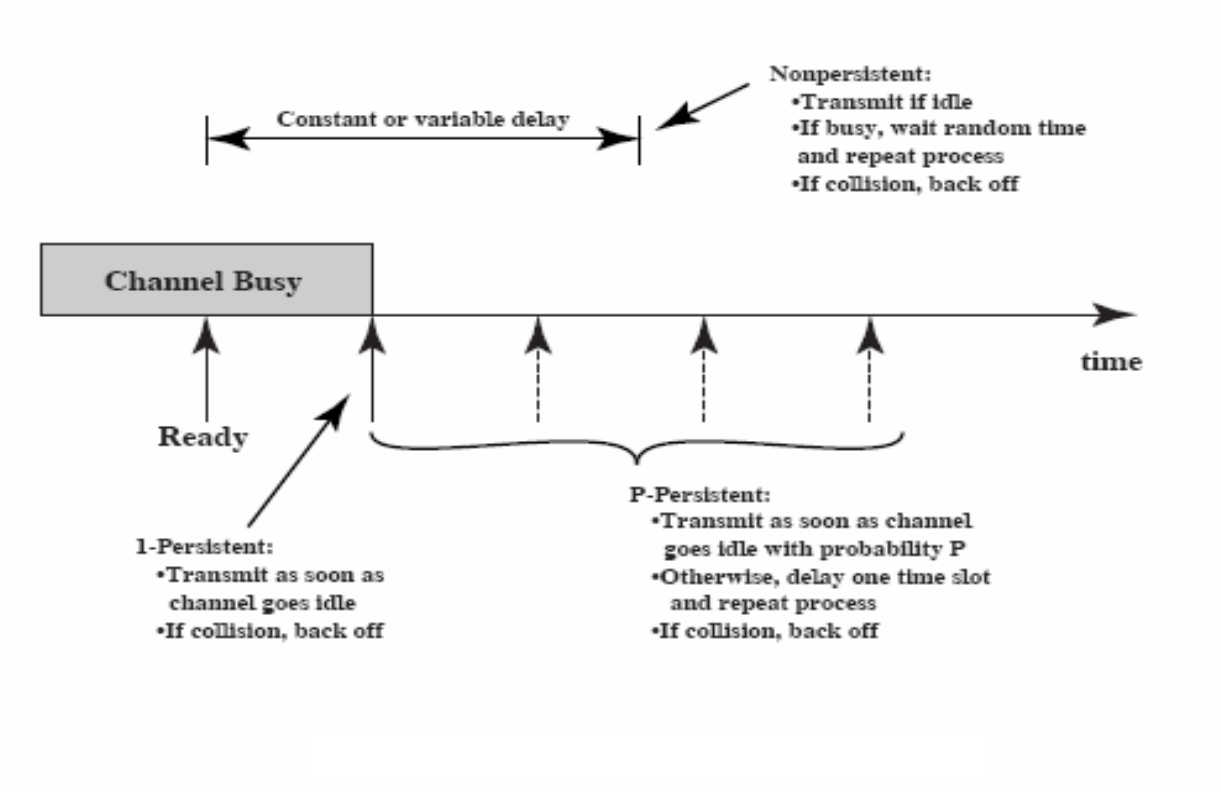


CSMA-Prinzip mit Kollisionserkennung

Prinzip:

- ein Knoten hört dem Kanal zu, bevor er überträgt ◘ ***Carrier-Sense***
- Falls der Kanal belegt ist → wartet er eine zufällige Zeitdauer und probiert es erneut.
- Falls mehrere Knoten quasi „gleichzeitig" feststellen, dass Kanal-frei, dann starten alle diese Knoten deren Sendung => ***Multiple Access***
- Alle Knoten (einschl. die sendenden) tasten während der Übertragung den Kanal ab. Falls Konflikt mit anderen Knoten festgestellt wird, dann stoppt die Sendung und wartet eine zuverlässige Zeitdauer, um erneut zu probieren → ***„Collision Detection"***

CSMA -Varianten



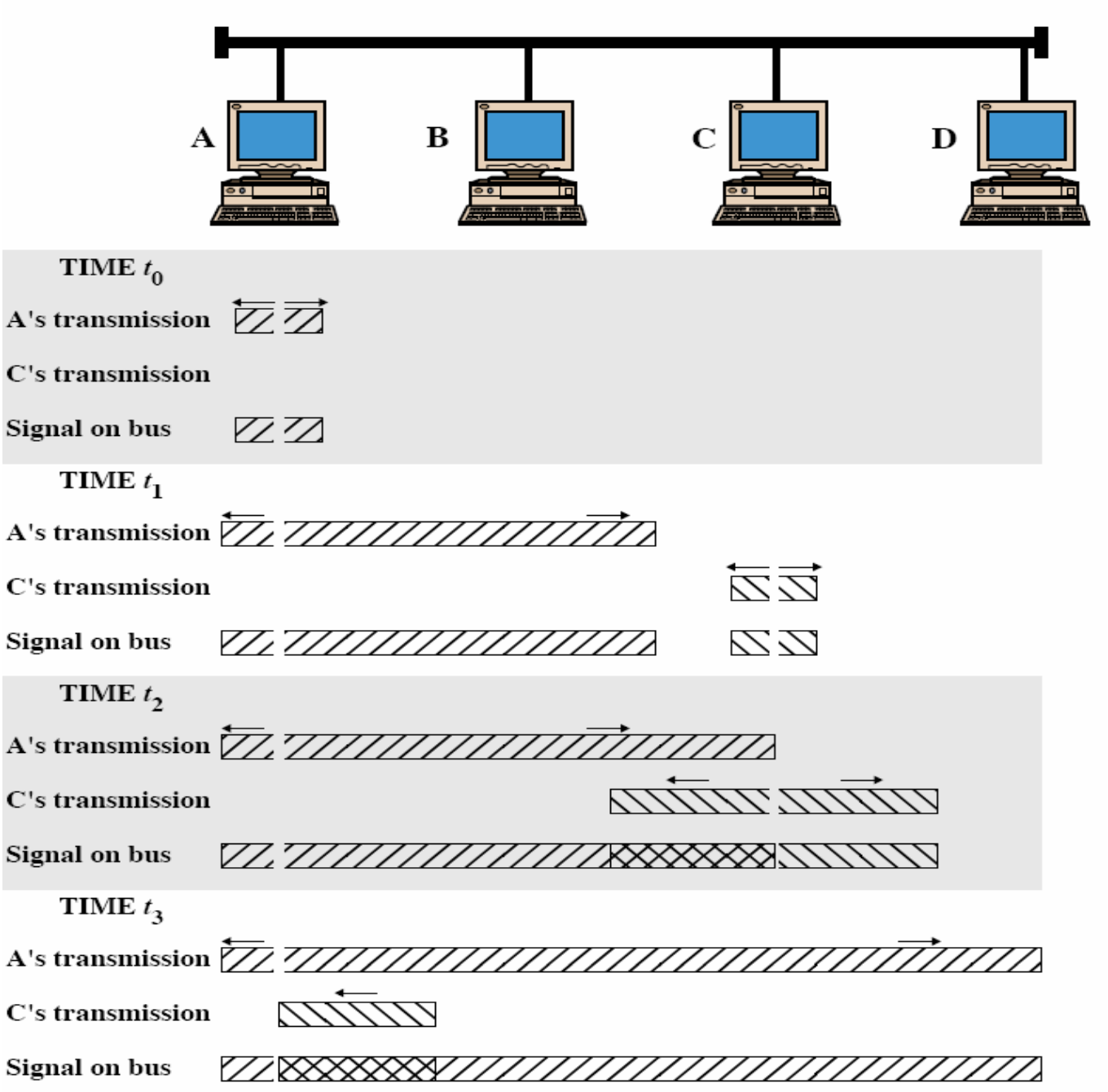
---

1) ***Nonpersistent CSMA***: (Nachteil: lange Idle-Intervalle)
   a) falls Medium frei = > dann Transmitt
   b) falls Medium busy = > dann Warte Zeitinterval (random berechnet) und wiederhole Step1

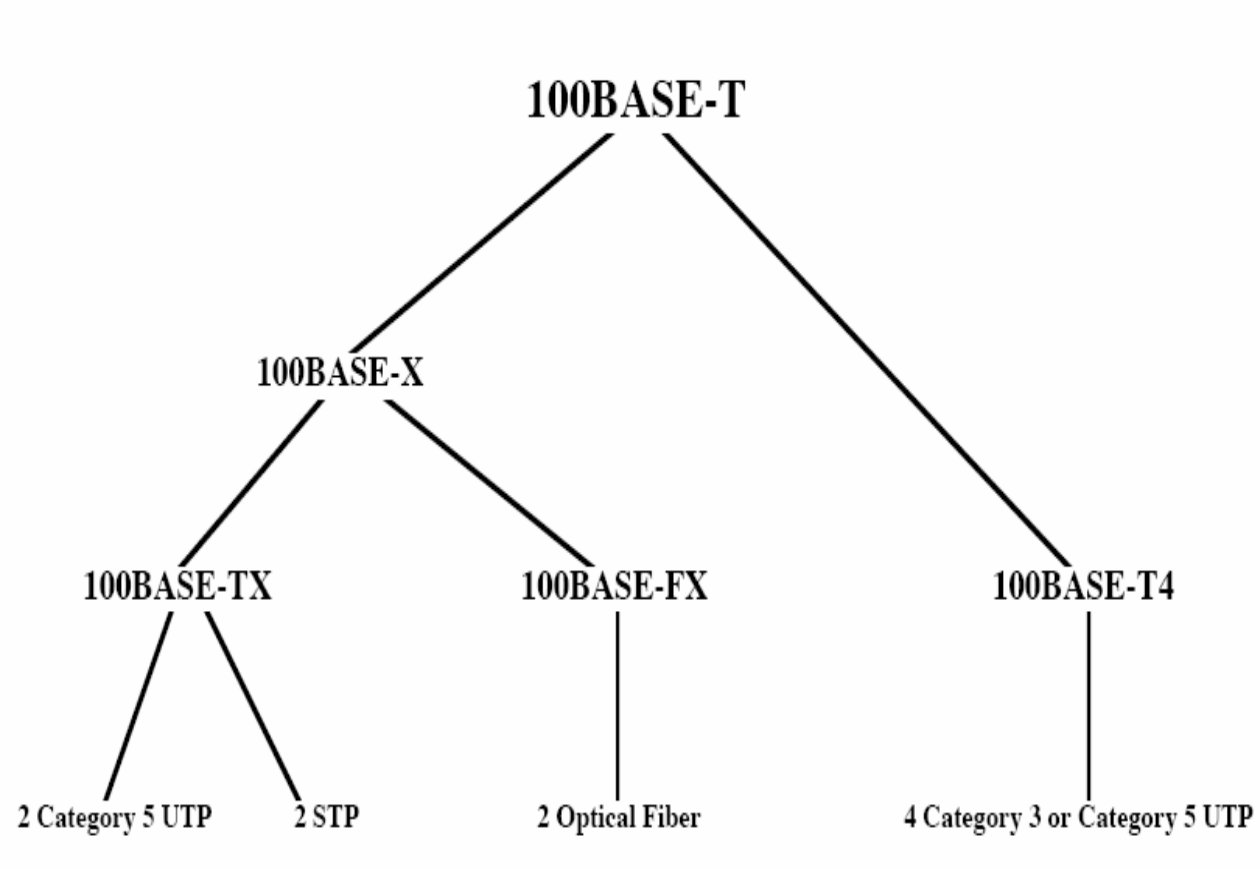
2) ***1- Persistent Protocol:*** (Nachteil: Falls mehere Stationen warten für „Sendung“ dann eine Kollision ist vorprogrammiert
   a) falls Medium frei = > dann Transmitt
   b) falls Medium busy = > dann höre weiter bis medium frei und transmit sofort
   c) falls Collision => dann Warte Zeitinterval (random berechnet) und wiederhole Step1

2) ***P-Peristent Protocol:*** (Vorteil: Verringert Idle time und Kollisionen)
   a) falls Medium idle => transmit mit „Probability“ P und verzögere 1 x Zeiteinheit mit „probability“(1-P)
   b) falls Medium busy => höre bis medium frei und repeat step 1
   c) falls Transmission verzögert 1 x Zeiteinheit = > repeat step 1

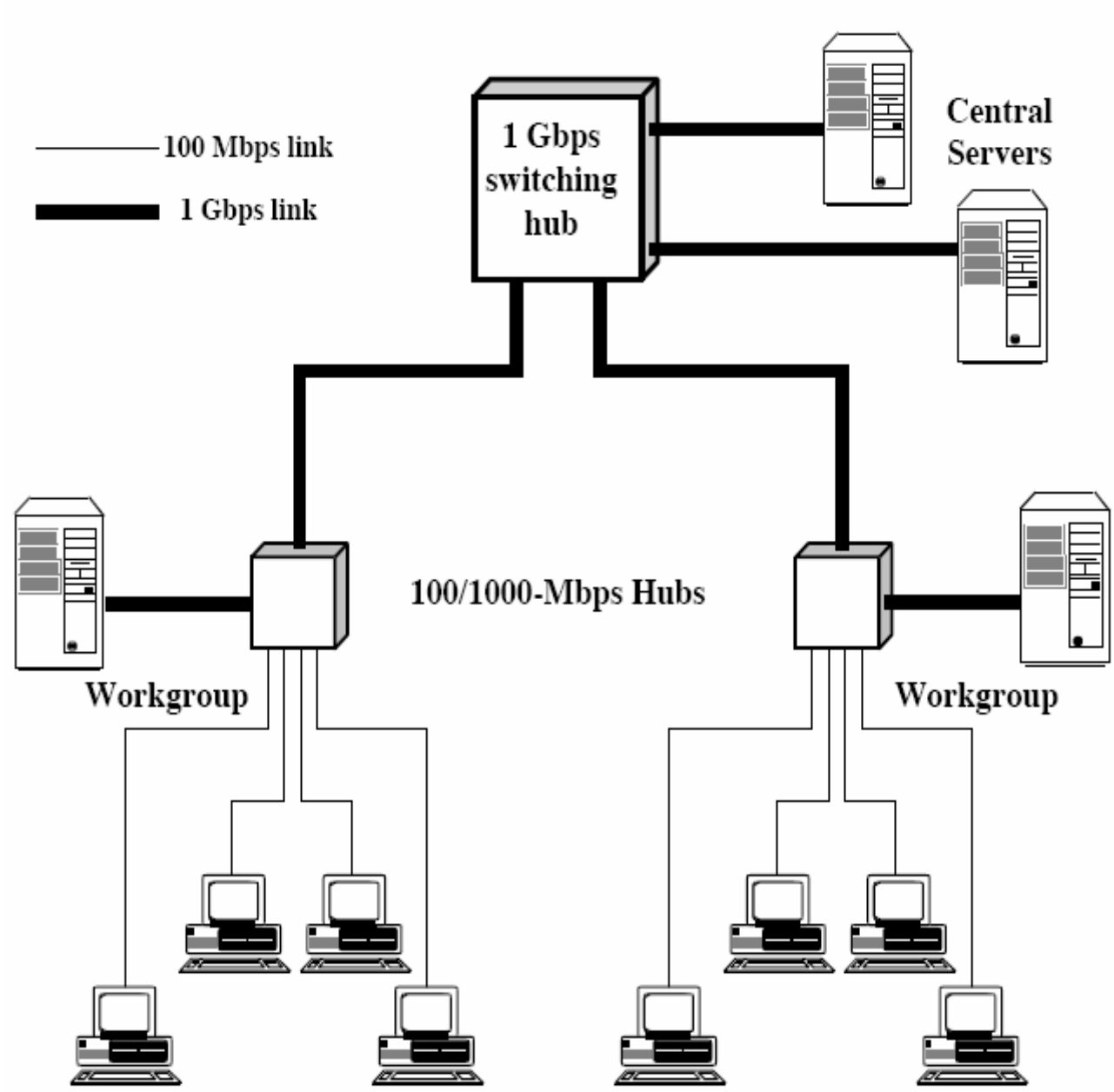
CSMA/-Collision Detection Timing



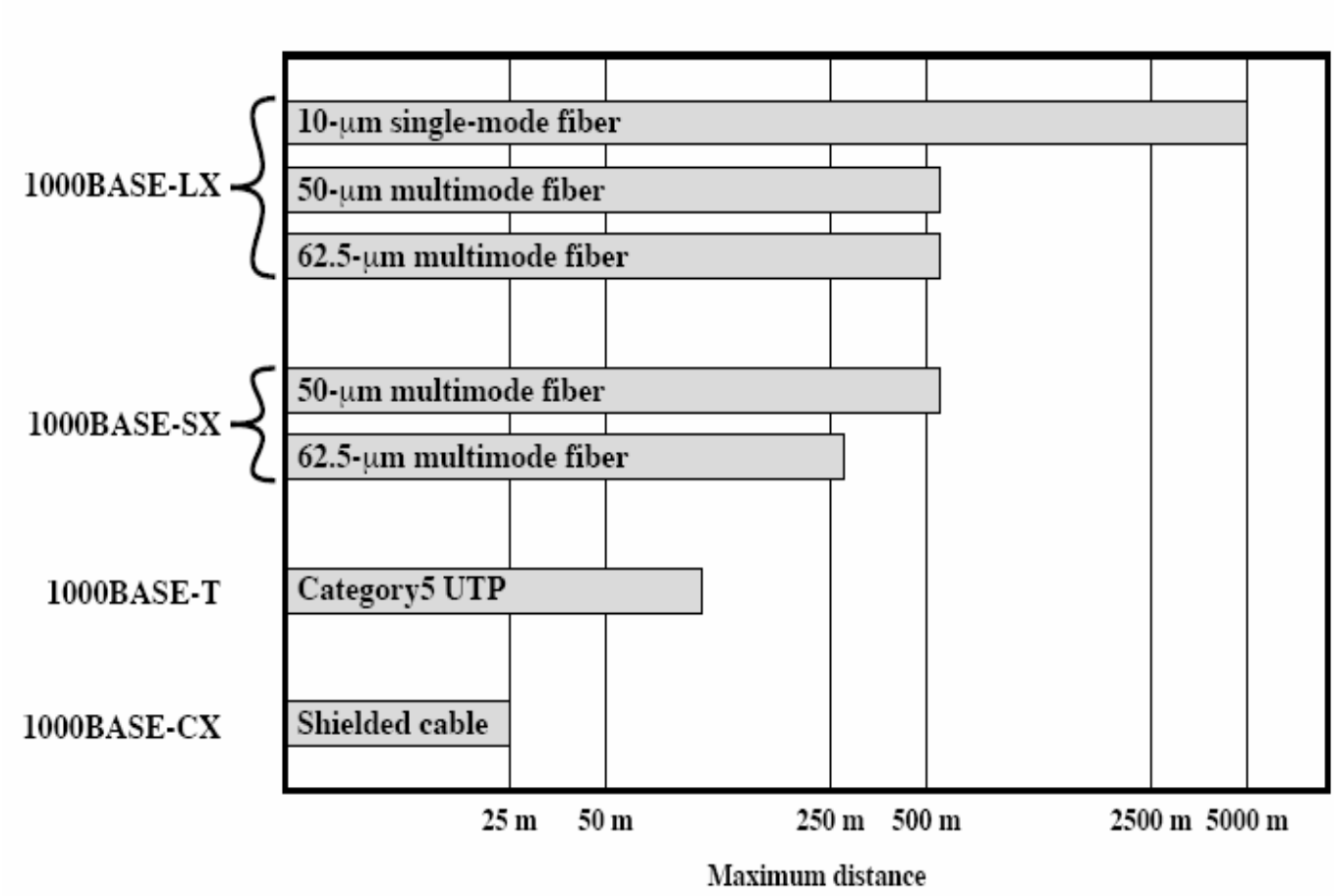
Fast Ethernet - Varianten



Gigabit - Ethernet – Topology Beispiel

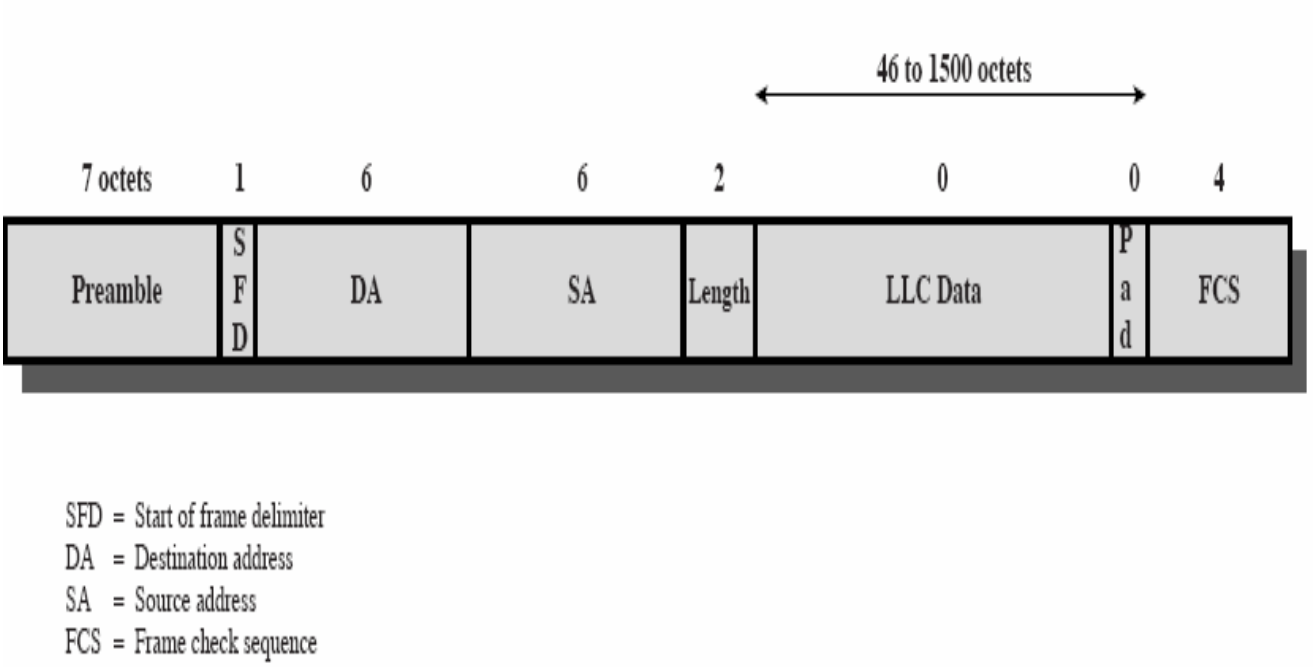


Gigabit – Ethernet: Mediums - Eigenschaften



Gigabit Etehrnet Medium Varianten (logaritmische Skala)

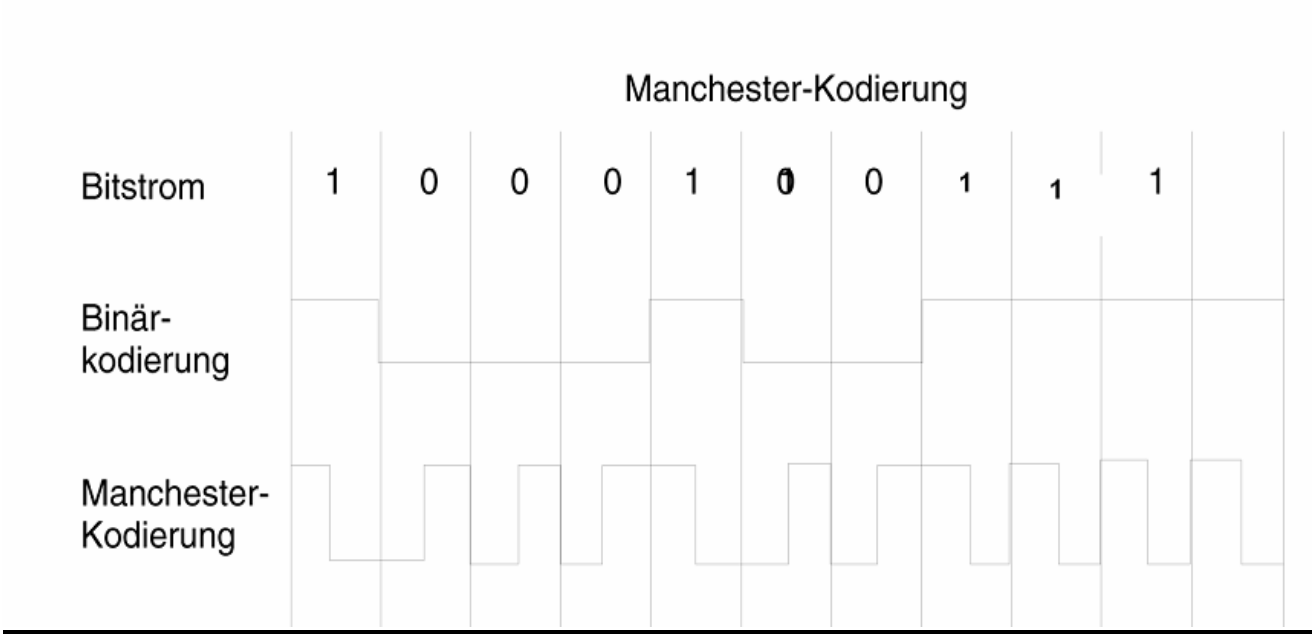
Ethernet-Nachrichtenformate



Felder:

- ***Präambel:*** → Aufwecken der empfangenden Adapter und Synchronisation ihres Takts
- ***Zieladresse*** → MAC-Adresse des Zieladapters oder MAC-Broadcast-Adresse: FF...FF oder MAC-Multicast-Adresse
- ***Quelladresse*** → MAC-Adresse des eigenen Adapters
- ***Typfeld/Länge*** → wird als Typ interpretiert, falls > 1500
  oder als Länge interpretiert, falls $\leq$ 1500
  Typ = welches Netzwerkprotokoll das Datenfeld enthält
- ***FCS (4 Byte)*** → der empfangende Adapter kann damit Fehler bei der Übertragung erkennen.

Basisbandübertragung (Manchester Code)



Manchester Kodierung

Prinzip:

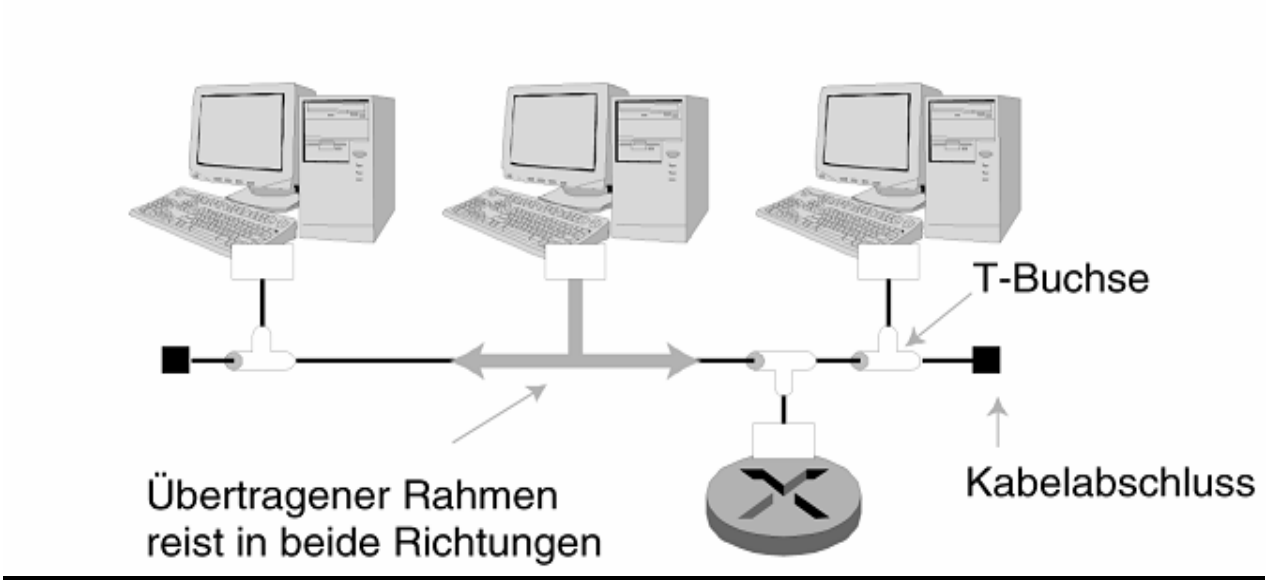
- Bei der digitalen Bitstrom Übertragung können Fehler bei der Erkennung der Bits (0 oder 1) am Empfänger entstehen
  (Der Takt beim Sender und Empfänger ist nicht perfekt synchronisiert).
- ***Lösung:*** Verwendung von sog. ***Manchester-Kodierung (MK)***
- MK → Jedes Bit enthält einen Übergang

  1 → Übergang von H → L

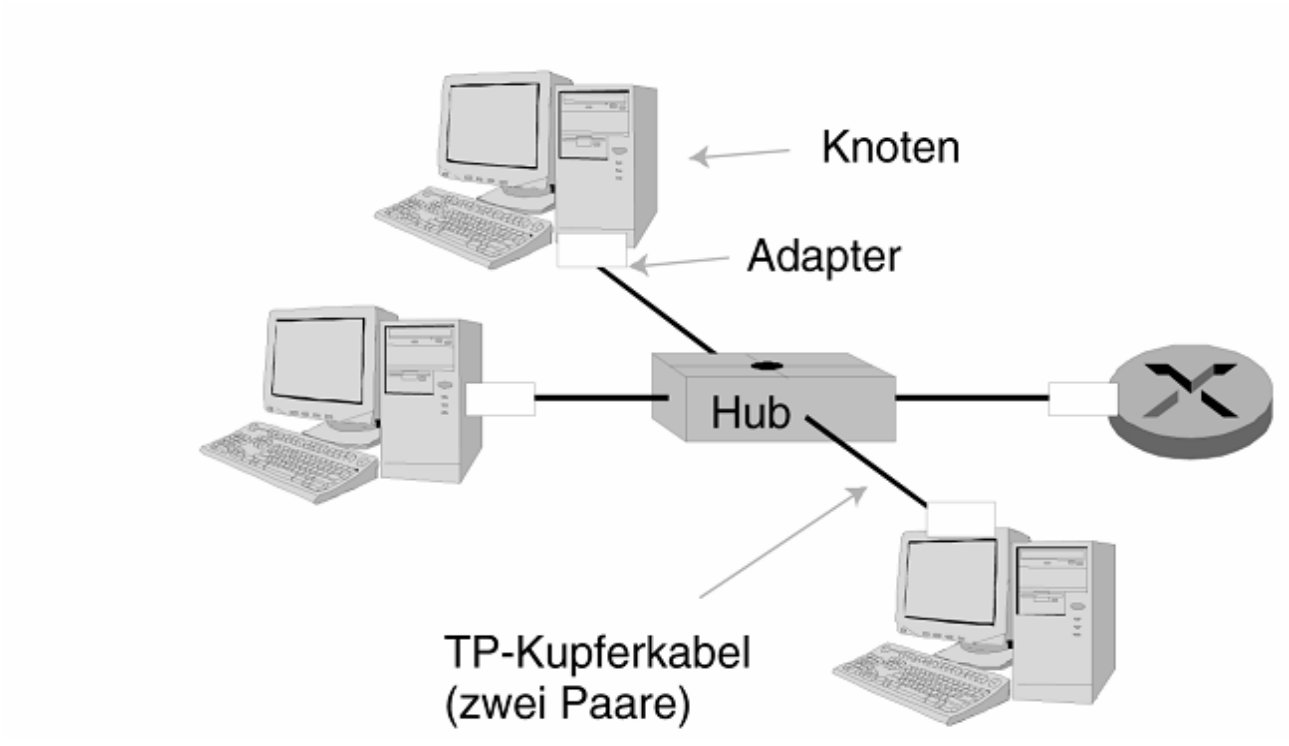
  0 → Übergang von L → H

Ethernet-Konfigurationen

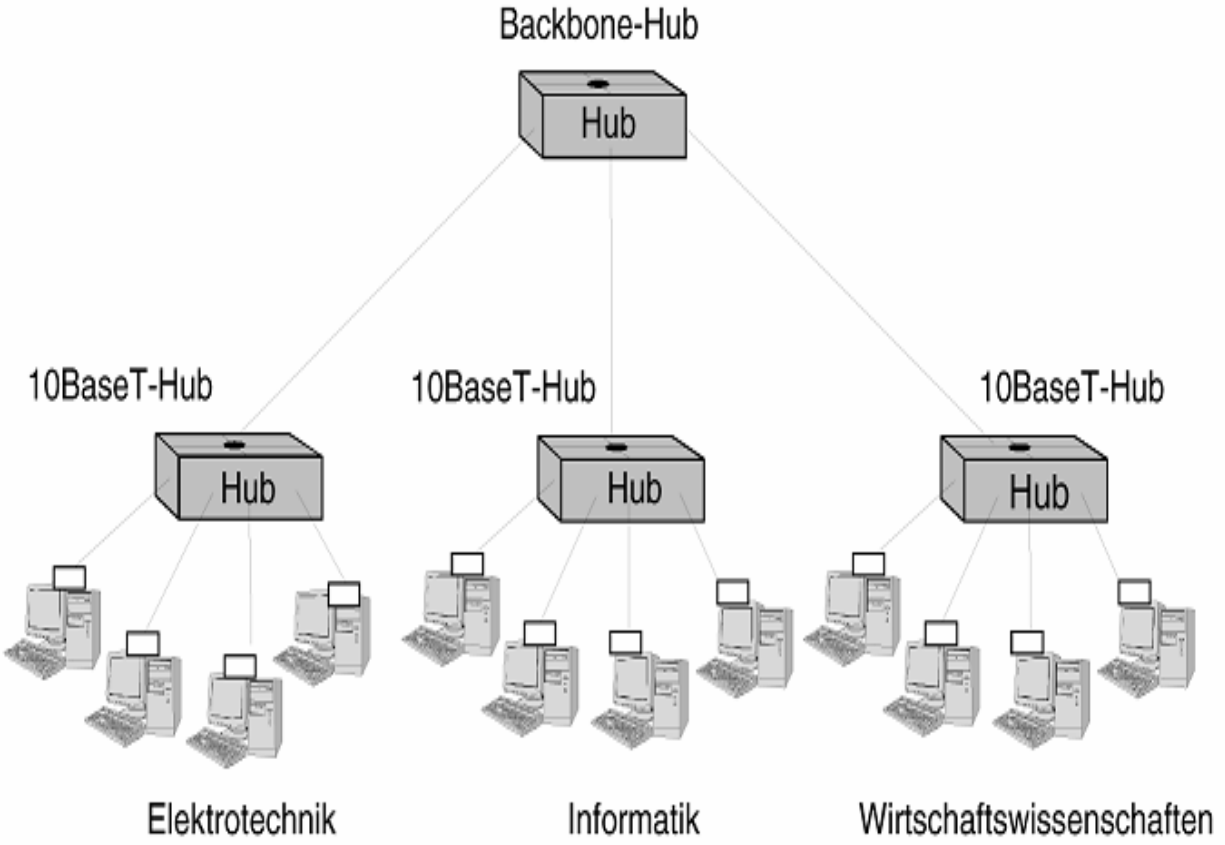
10Base2- Ethernet Variante



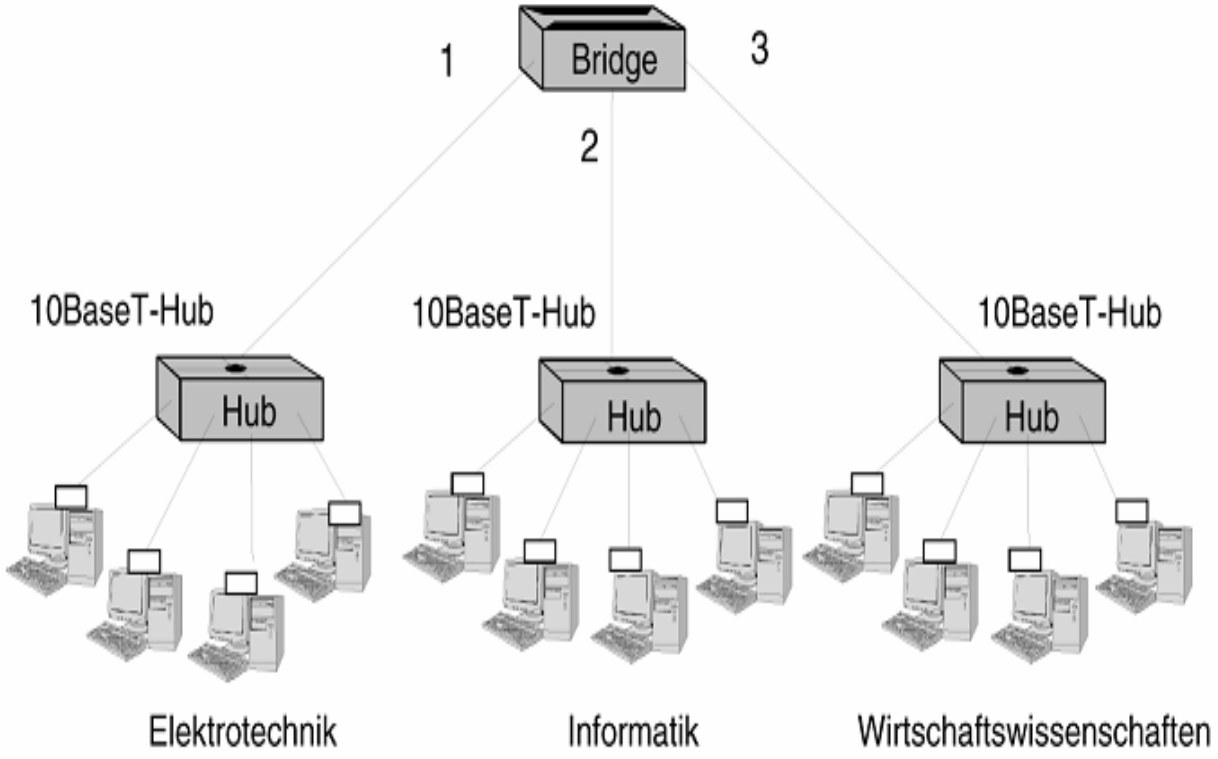
Sterntopologie für 10BaseT und 100BaseT



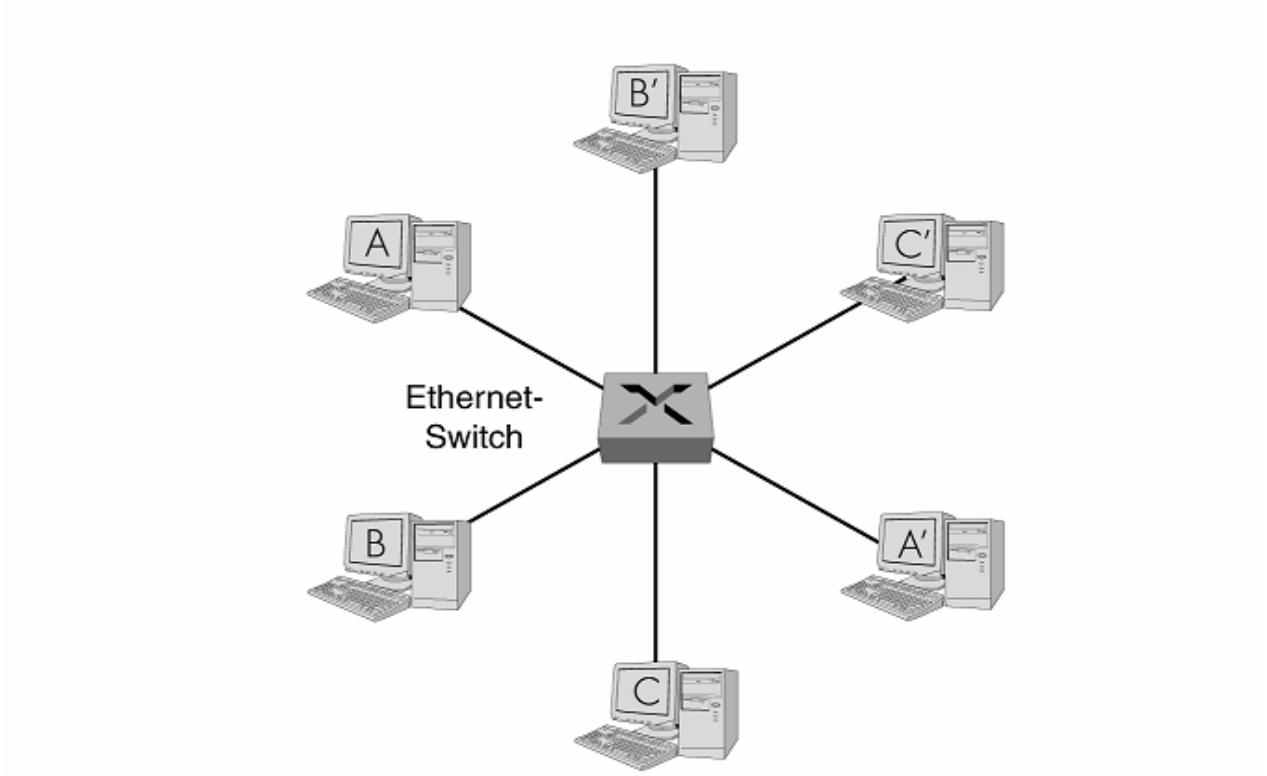
Ethernet LANs die via HUBs verbunden sind



Ethernet LANs die via Backbone Bridge verbunden sind



Switch vs. Bridge

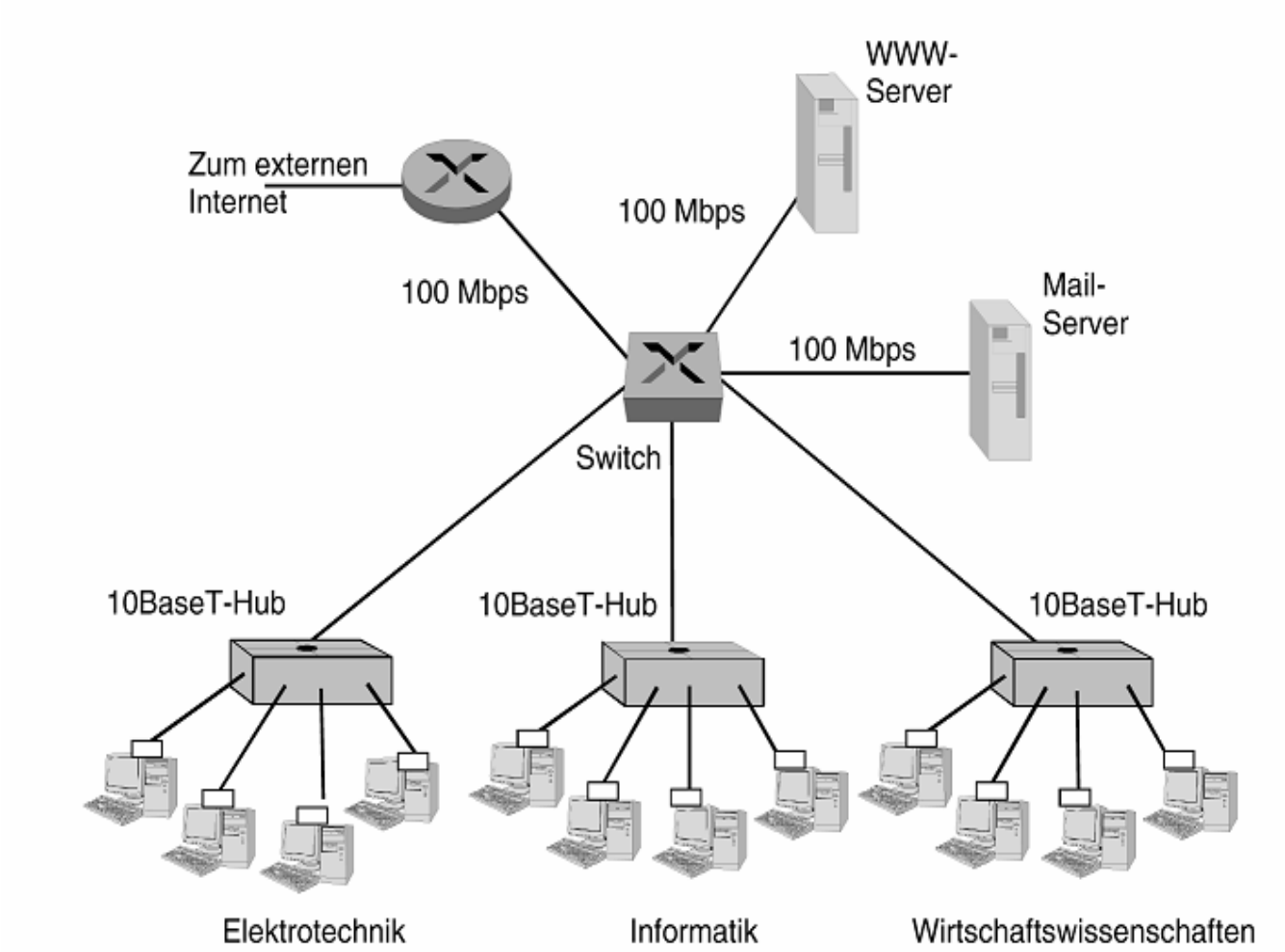


Prinzip:

- ***Switch*** → Leistungsfähige Bridge mit mehreren Schnittstellen
- Switch leitet Nachrichten weiter basierend auf den MAC-Zieladressen
- Switch → verwaltet MAC-Adresstabellen für jede Schnittstelle
- Die Switches haben insgesamt (basierend auf der sog. Hardware Switching-Fabric) eine ***sehr hohe Gesamt-Weiterleitungsrate***
- Sie können auch „Vollduplex“ arbeiten, wenn eine Station einen sog. ***„dedizierten Zugriff (Anschluss)***“ auf den Switch hat.

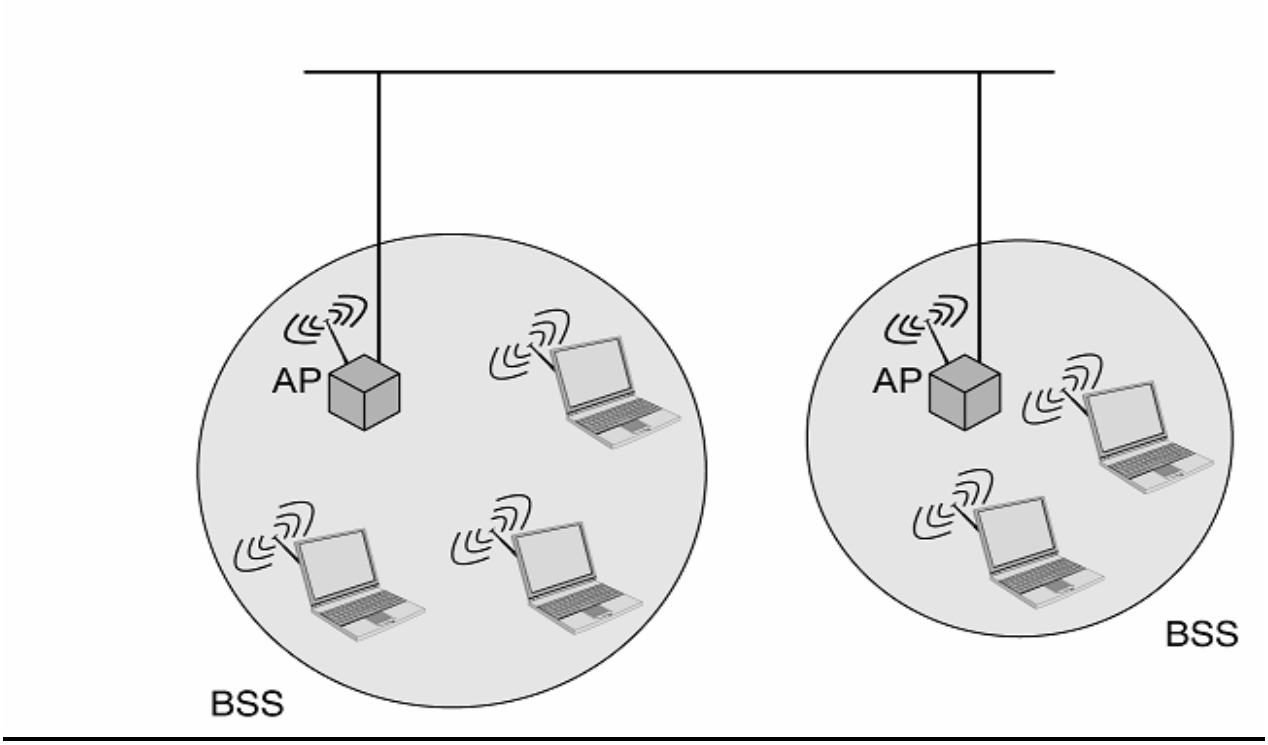
Shared vs. Switched-Network

Unternehms-Netzwerk mit einer Kombination von Netzwerk-Komponenten: HUB, Switch, Router



Wireless LAN gemäss IEEE 802.11

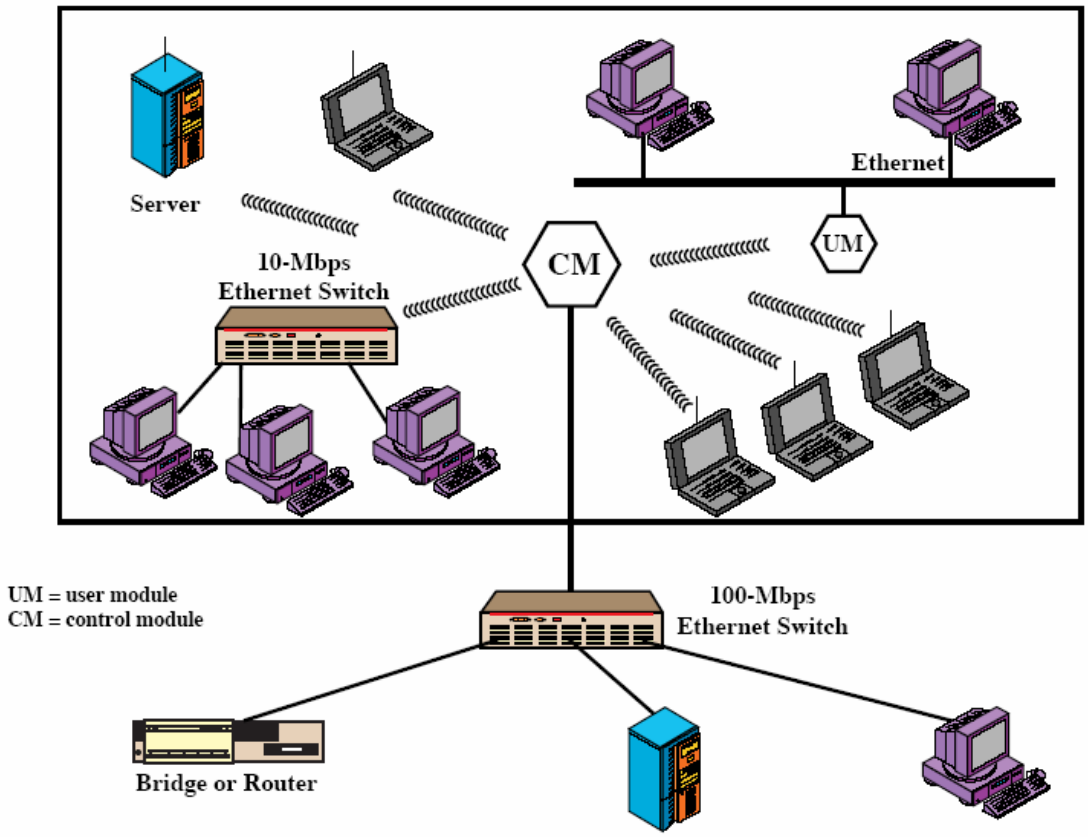
Architektur eines IEEE802.11 - LAN



Komponenten:

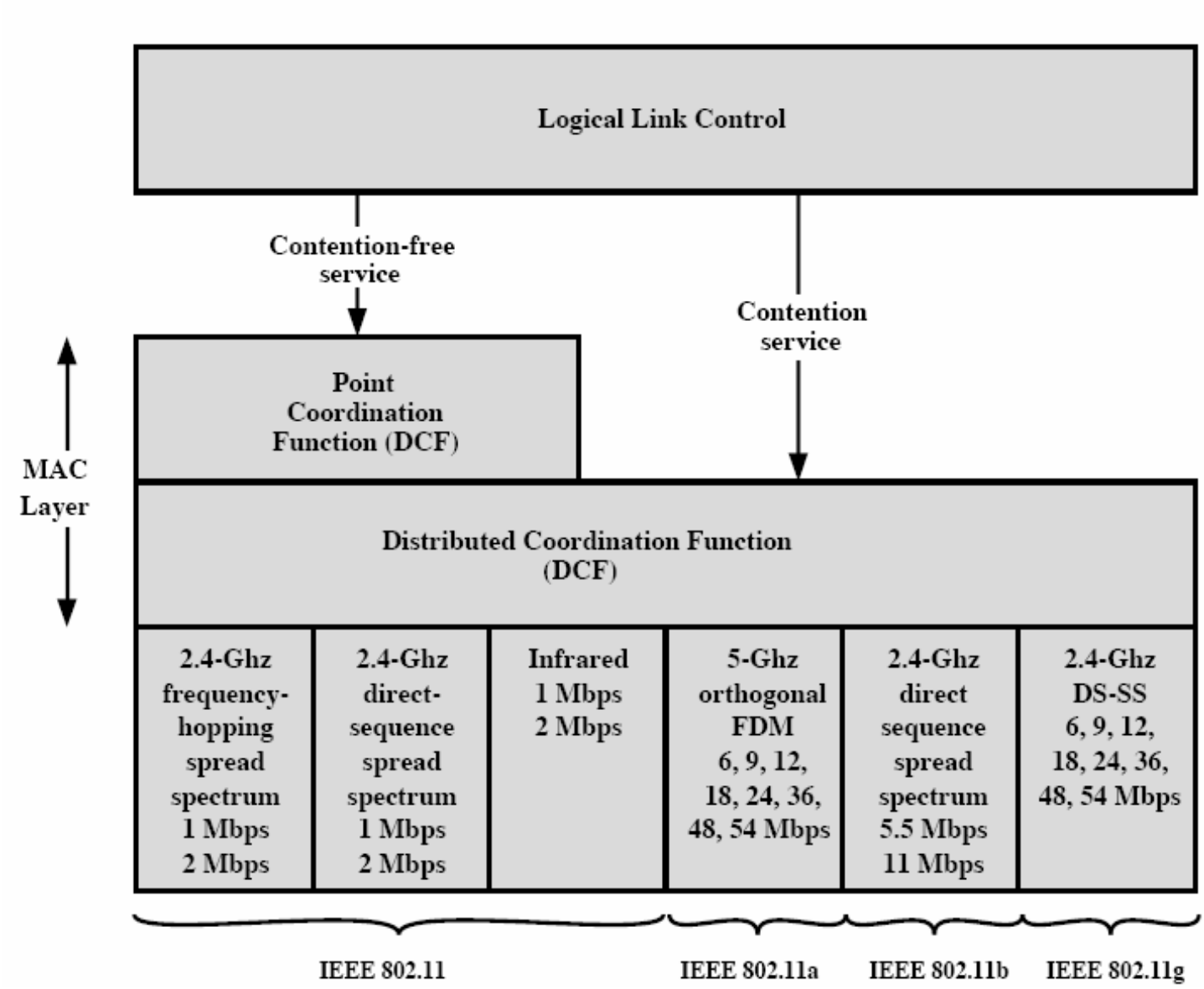
- ***BSS*** → Basis Service Set enthält:
  - Eine oder mehrere drahtlose Stationen
  - Ein Access Point (AP): Zentrale Basisstation

- Mehrere APs können ein ***Distribution System (DS)*** bilden.
- Höhere Schichten Protokolle betrachten ein **DS** als ein normales 802-Netzwerk (z. B. Ethernet)


Server
Ethernet
CM
UM
10-Mbps
Ethernet Switch
UM = user module
CM = control module
100-Mbps
Ethernet Switch
Bridge or Router

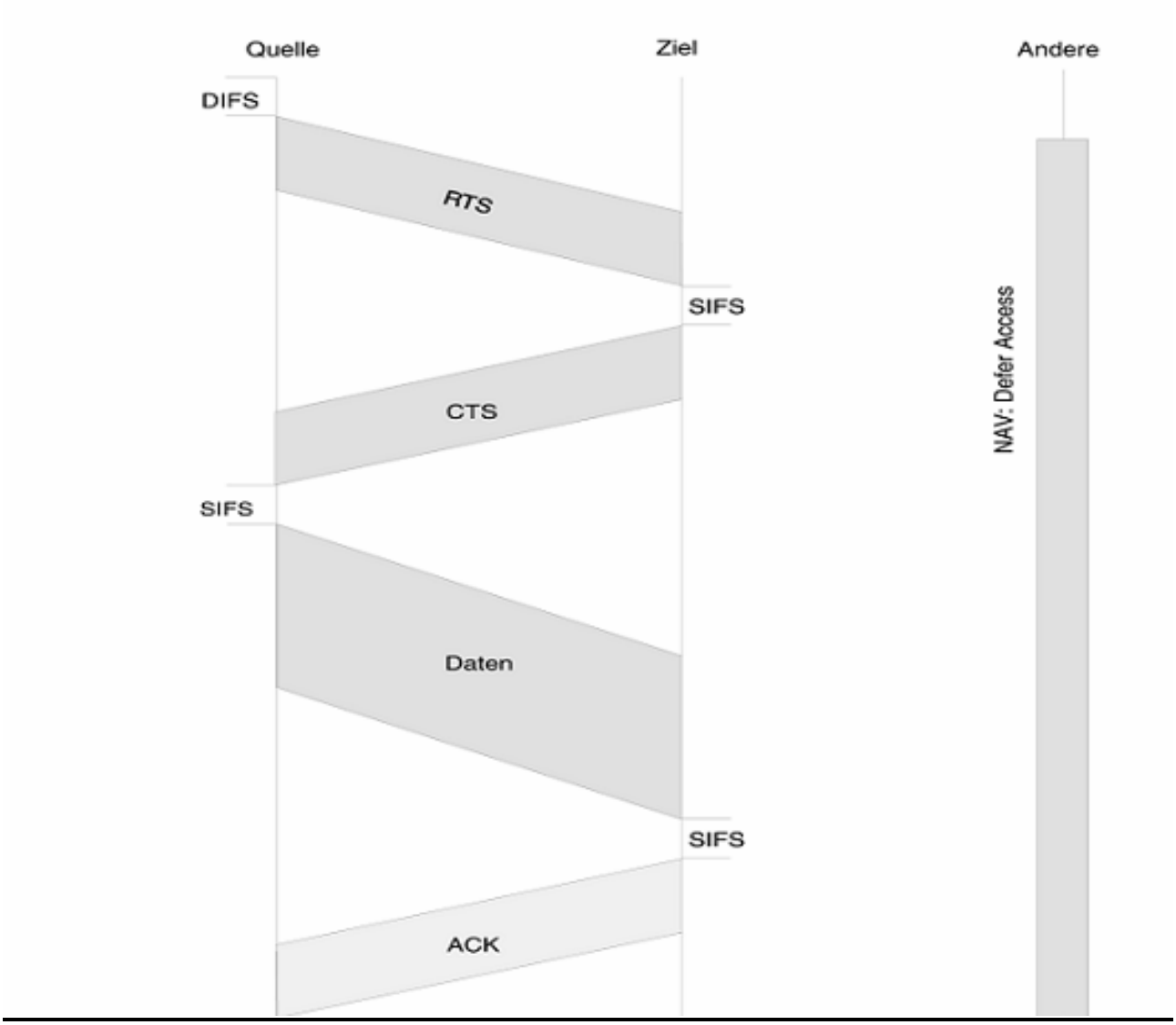
IEEE 802.11 – Medium Access Protokoll (1)

Protokoll-Architektur



IEEE 802.11 – Medium Access Protokoll (2)

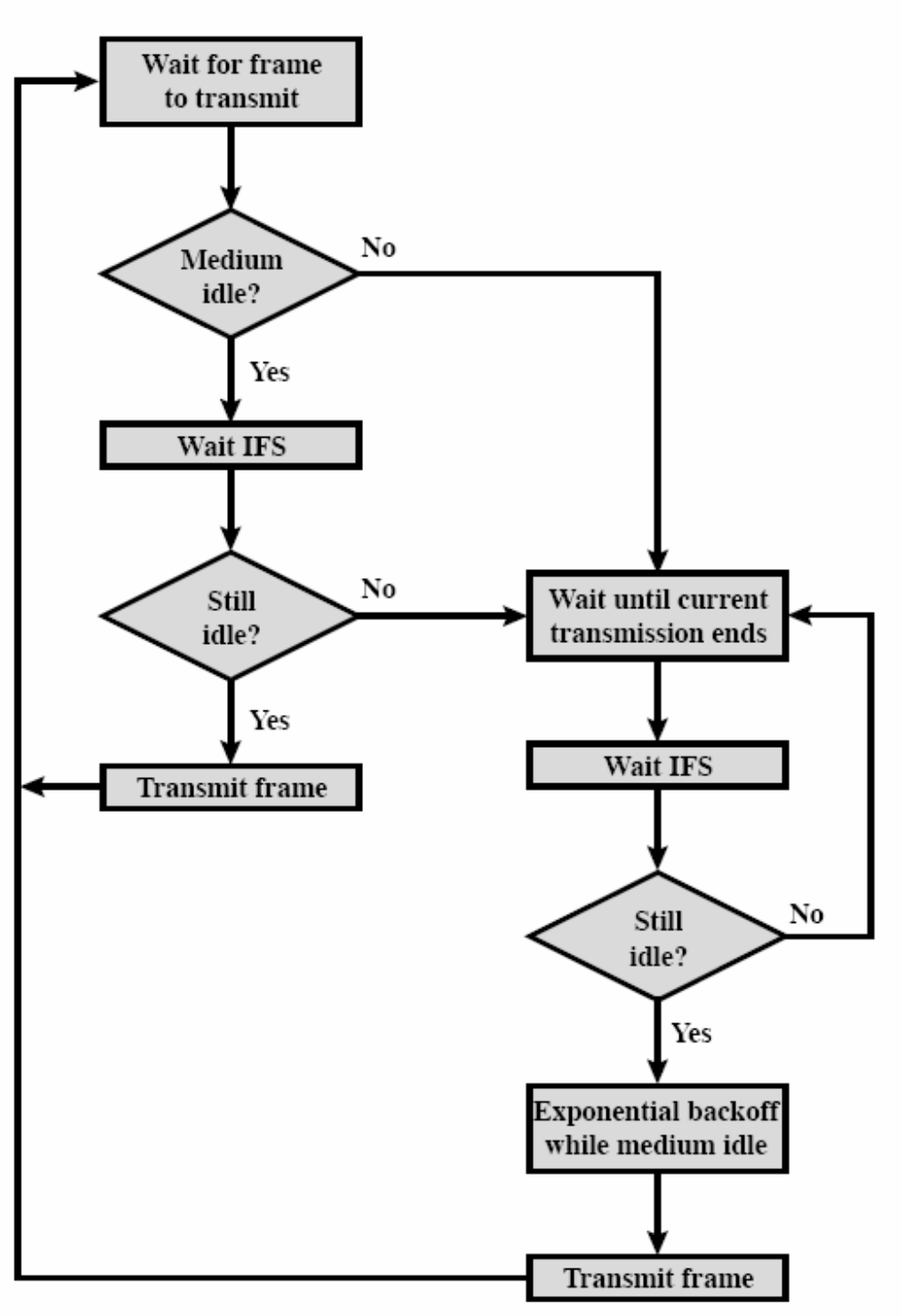
CA-Prinzip (Kollisionsvermeindung) mittels RTS und CTS Meldungen



Prinzip:

- 802.11 ist ein sog. ***CSMA/CA (Collision Avoidance)*** Protokoll
- Zuerst wird der Kanal abgetastet, um festzustellen, ob er besetzt ist: „Carrier Sense“.
  (Dies erfolgt mittels Überwachung des Energie-Pegels auf der Funkfrequenz)

MAC - Ablauf Diagramm



Ablauf:

- Falls der Kanal ein gewisses Zeit-Intervall untätig ist:

  Zeit > Distributed Inter Frame Space (DIFS)-Interval

  dann sende RTS – Rahmen (***Request to Send)***

- Empfänger wartet eine kurze Zeit:

  Short Inter Frame spacing (SIFS)

  und sendet seine Bereitschaft Verbindung aufzunehmen:

  CTS-Rahmen (Clear To Send)

  Nach dem erfolgreichen ***RTS-CTS-Austausch*** wird der Zugriff auf den Kanal von den beteiligten Stationen reserviert. D.h. keine anderen Stationen werden auf den Kanal zugreifen.

  So werden die „Kollisionen" vermieden (d.h. Collision Avoidance)

- Sender sendet ***nach SIFS-Zeit***

  "Daten"

- Empfänger bestätigt die Daten mit

  "ACK"

Vermeidung von Kollisionen:

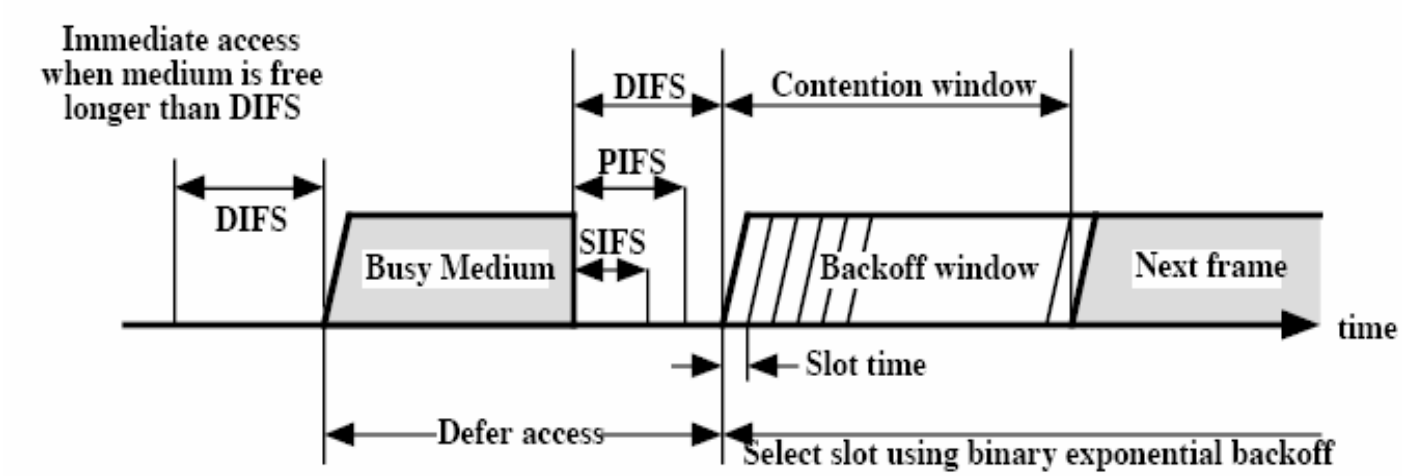
- Berechnung der ***DIFS***-Zeit

  Falls erkannt wird → Kanal frei

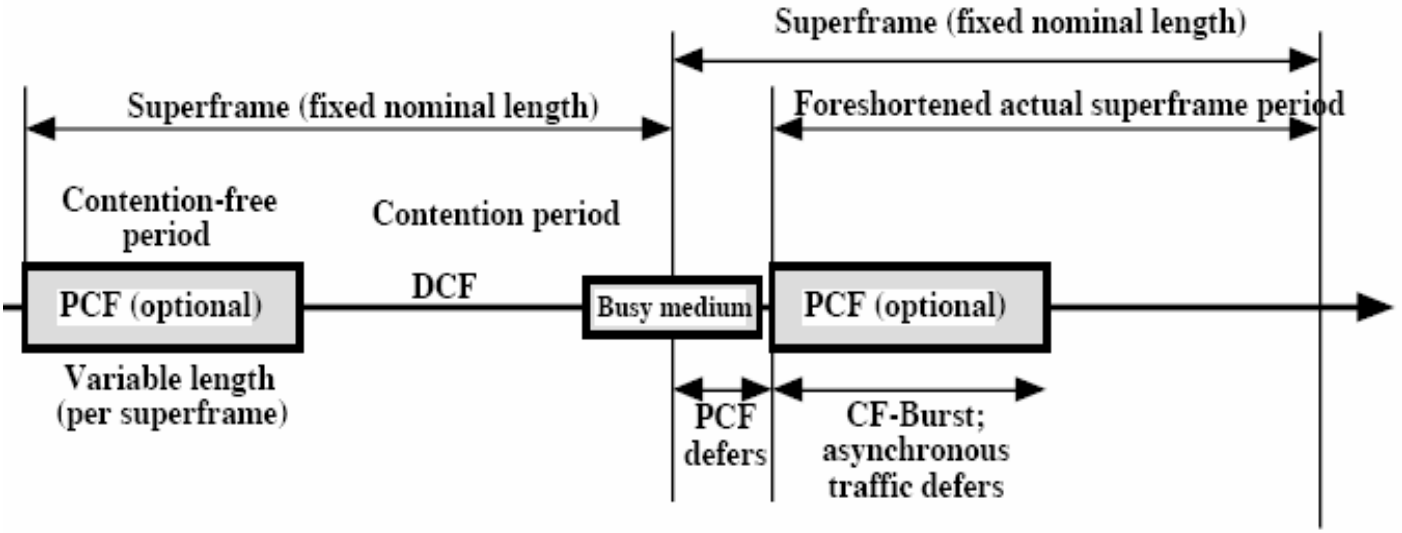
  dann berechnet die Station eine zufällige ***„Back-Off-Zeit"*** und wartet dieses Zeitintervall

  Diese Methode trägt zur Vermeidung der Kollisionen bei.

802.11 MAC-Timing



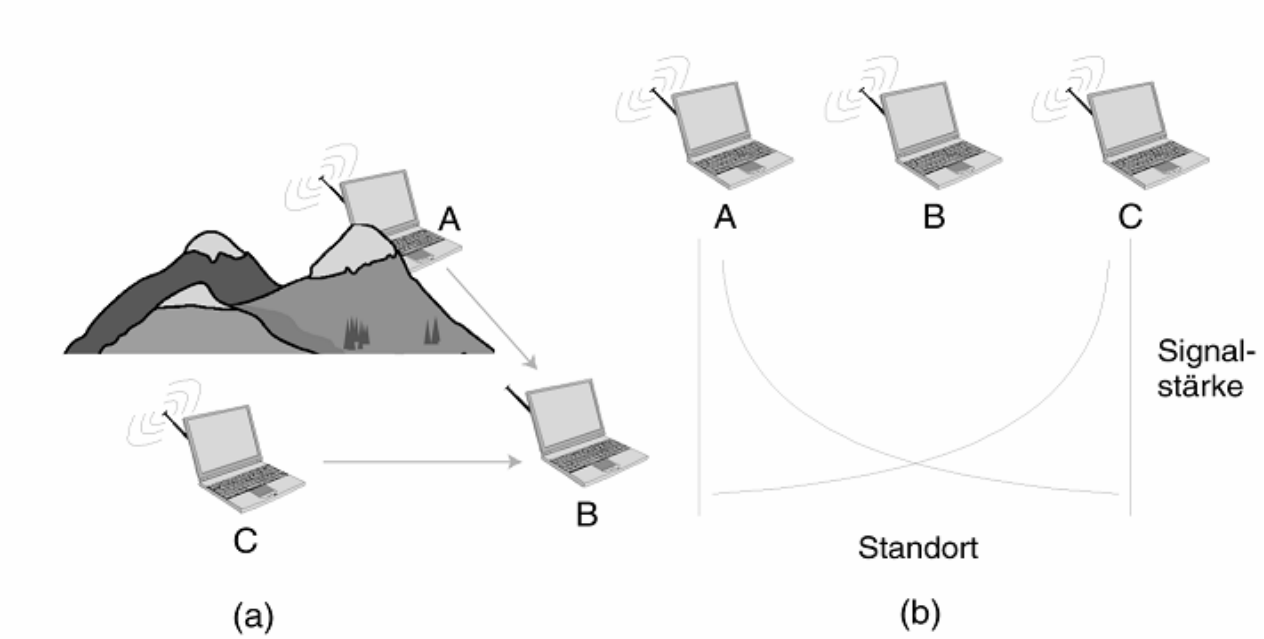
(a) Basic Access Method



(b) PCF Superframe Construction

Hidden-Terminal Problem

Teilbild a) Hidden-Terminal Problem **Teilbild b) Fading Problem**



- Wegen physischer Hindernisse (z. B. Berg) und sog. ***Fading*** können trotzdem Kollisionen entstehen.

  Lösung: Verwendung von Verfahren, die Kollisionen vermeiden.

  - Mechanismen: a) RTS - CTS Austausch
    b) DIFS und SIFS Zeit-Intervalle
    c) NAV – Network Allocation Vector
    d) 802.11 Rahmen enthält auch ein
    Feld „Duration“ : d.h.: sendende Station gibt an:
    : „die Dauer der Übertragung“

NAV→ Mindestzeit, auf die der Zugriff auf den Kanal nicht möglich ist.
Dieses Zeit-Intervall wird auch ***„Differ Access***“ genannt