Kapitel 3: LAN-Komponenten

3 LAN Komponenten

- 3.1 Grundlagen zum Aufbau von LANs
- 3.2 LANs nach IEEE 802.3 (Ethernet)
- 3.3 Drahtlose LANs
- 3.4 Bluetooth
- 3.5 Power over Ethernet (PoE)
- 3.6 LAN Verbundkomponenten
- 3.7 Switches
- 3.8 Router
- 3.9 Aufbau von Netzkomponenten
- 3.10 Management von LAN-Komponenten

3.1 Grundlagen zum Aufbau von LANs

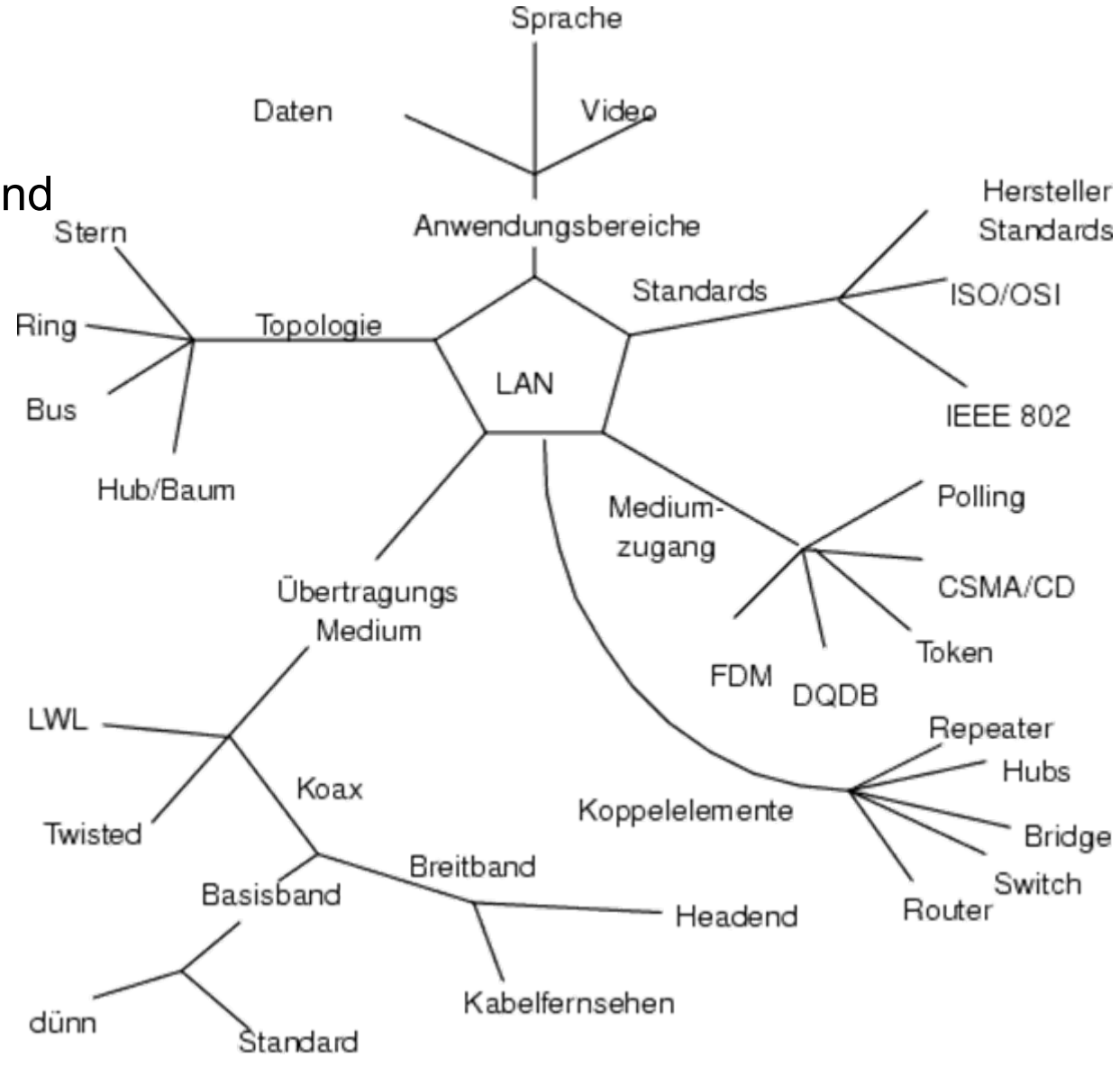
- 3.1.1 Installationskriterien
- 3.1.2 Kategorien
- 3.1.3 Topologien
- 3.1.4 LAN-Referenzmodell
- 3.1.5 LAN-Implementierungsmodell
- 3.1.6 IEEE-Standards im Überblick

3.1.1 Installationskriterien

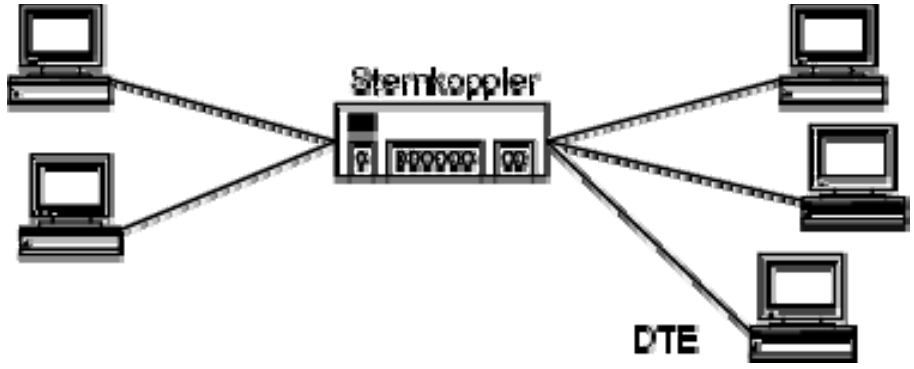
- **Aspekte, die bei der Installation von LAN‘s zu berücksichtigen sind:**
  - bevorzugt unterstützter Anwendungsbereich
  - bevorzugt unterstützte Informationstypen
  - erwartete Verkehrscharakteristik
  - Verbindungsart
  - Topologie
  - Übertragungsmedien
  - Art des Zugangs zum Übertragungsmedium
  - unterstützte Protokollhierarchie
- **Bit-Übertragungsschicht ist abhängig vom benutzten Medium; Medium-Zugang (Teil der Sicherungsschicht; Schicht 2a; "mac = medium access control") ist abhängig von Zugriffsstrategie und Netztopologie**

3.1.2 Kategorisierung von LANs

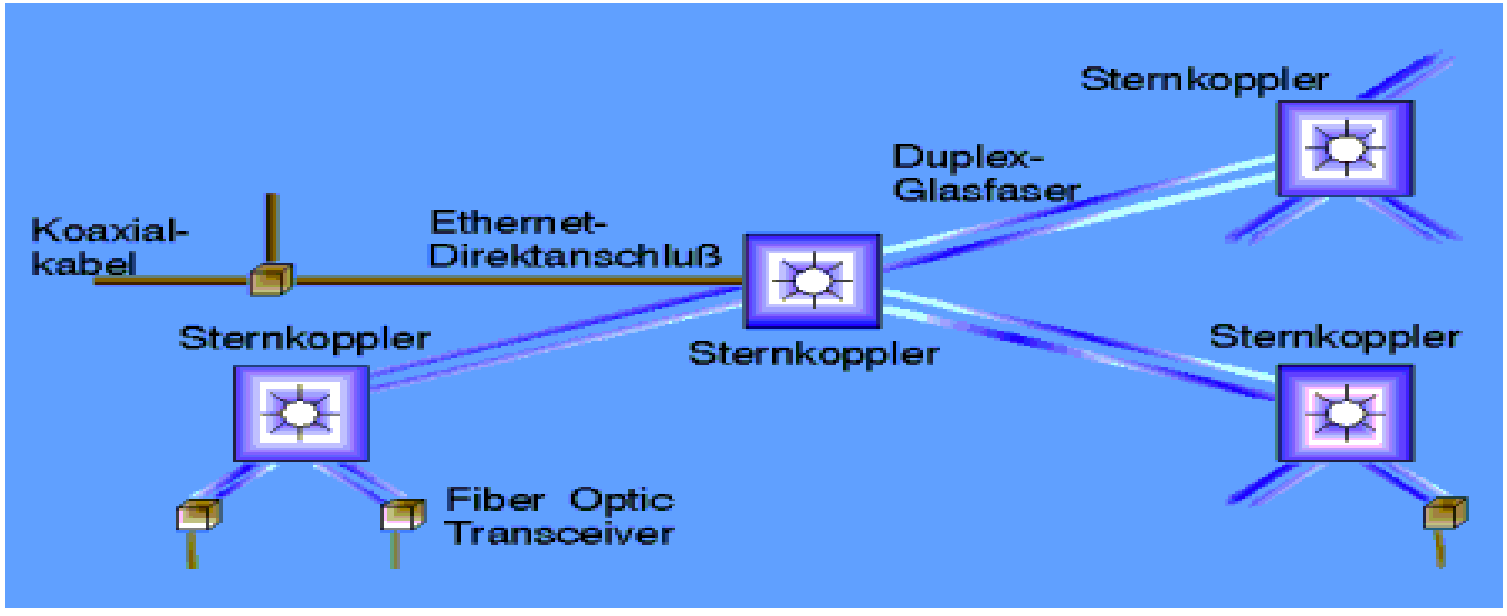
- **Einteilung der LANs**
  - Taxonomie von LANs entsprechend verschiedener Aspekte



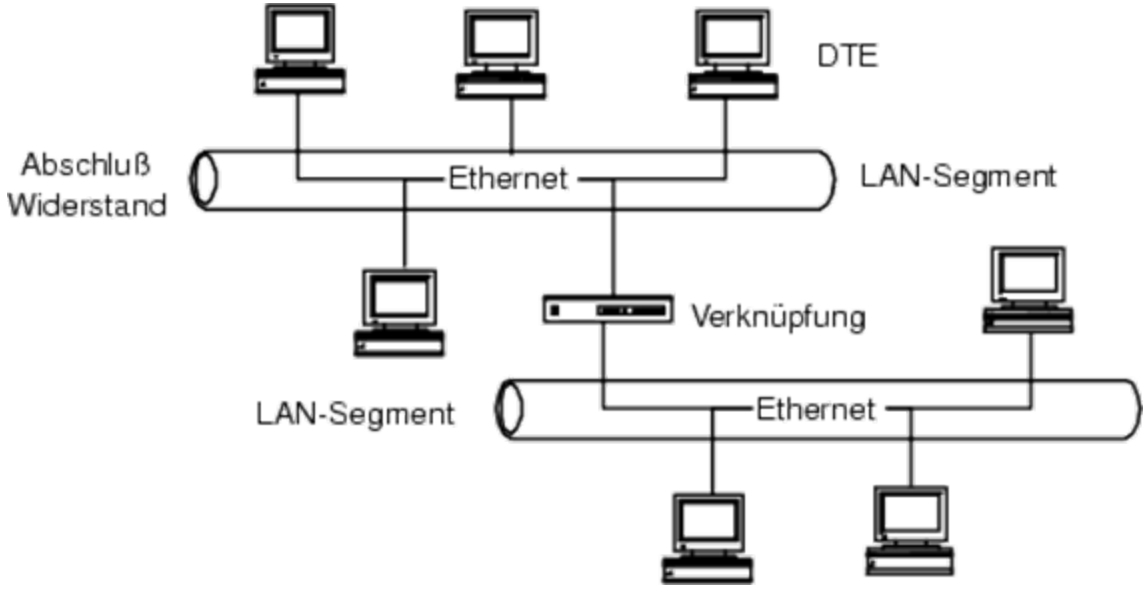
3.1.3 Topologien (1): Sterntopologie



- Ein typisches Beispiel für Sterntopologien sind die privaten Telefonanlagen; Sternkoppler kann als Vermittlung angesehen werden

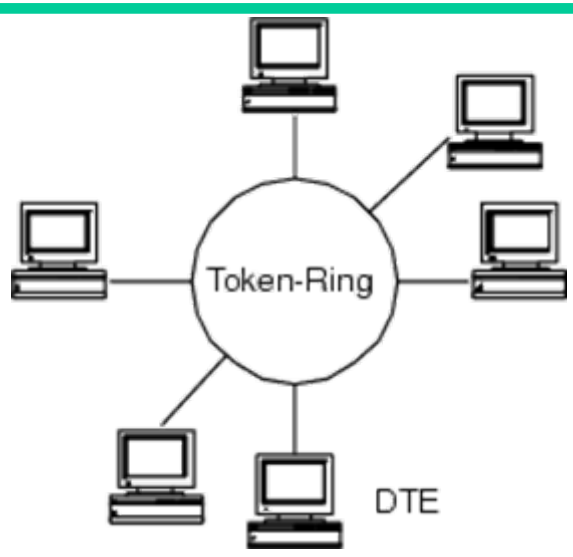


3.1.3 Topologien (2): Bustopologie



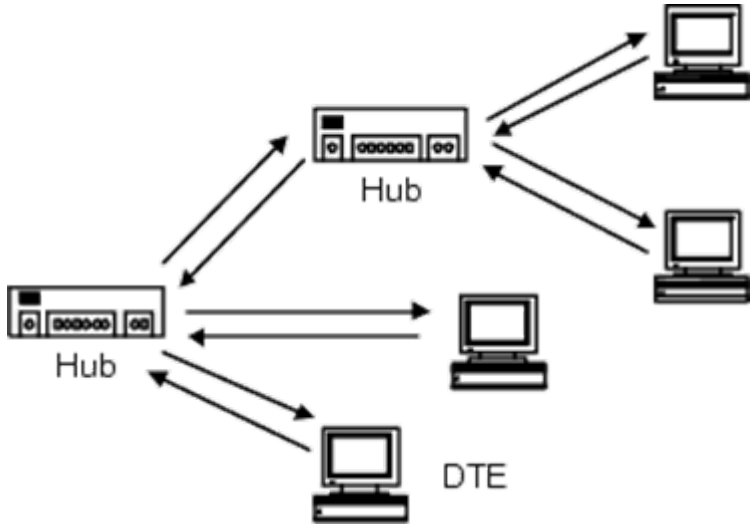
- **Alle Teilnehmerstationen an ein gemeinsames Übertragungsmedium angeschlossen**
- **Stationen können beliebig hinzugefügt oder weggenommen werden**
- **Vorteile der Bustopologie:**
  - Leichte Erweiterbarkeit, in der Modularität, der einfachen Implementierung und der dezentralen Kontrolle.
- **Nachteilig:**
  - Anfälligkeit gegenüber Ausfall des Mediums, die fehlende Abhörsicherheit und eventuelle (von der MAC-Schicht abhängige) unvorhersehbare Wartezeiten.

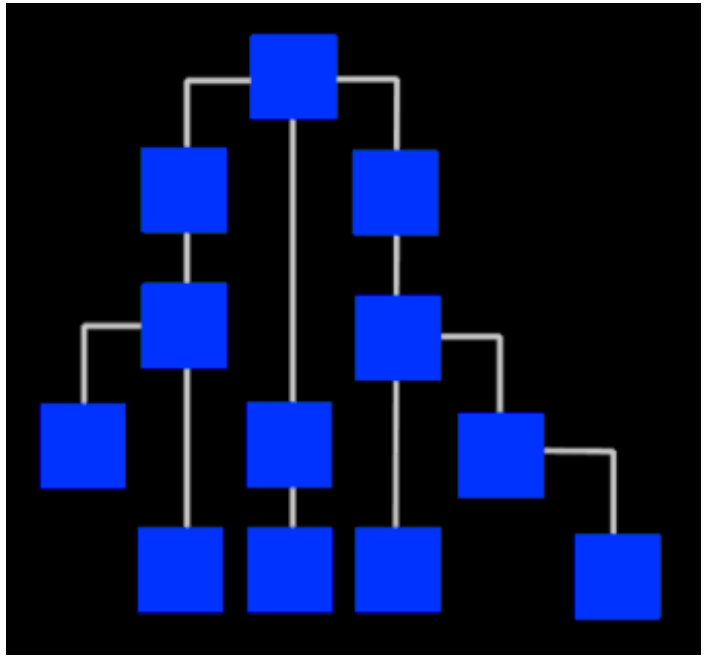
3.1.3 Topologien (3): Ringtopologie



- Die Informationsübertragung erfolgt in einer vorgegebenen Übertragungsrichtung
- Der Zugriff auf das Übertragungsmedium sequentiell von Station zu Station mittels Abrufsystem von der Zentralstation oder durch ein Token
- Ringtopologien sind leicht erweiterbar, haben eine geringere Leitungsanzahl als Sterntopologien und eine dezentralisierbare Protokollstruktur
- Nachteile entstehen bei Leitungs- oder Stationsausfall sowie bei der Dauer der Nachrichtenübertragung, die proportional zur Anzahl der angeschlossenen Stationen ansteigt

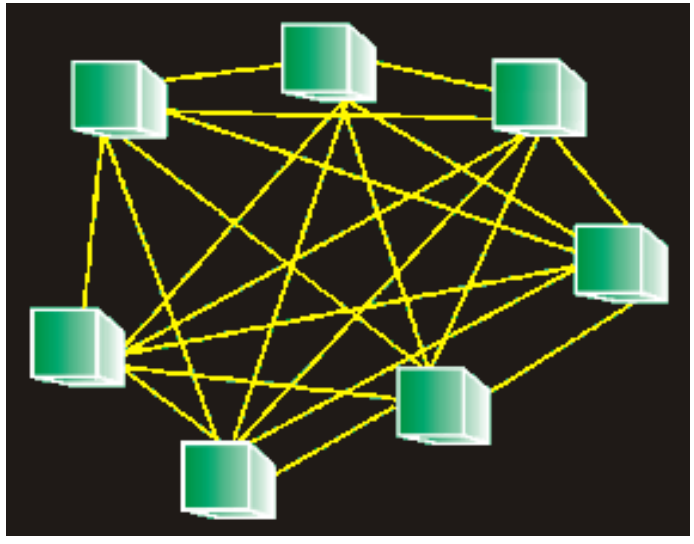
3.1.3 Topologien (4): Baumtopologie

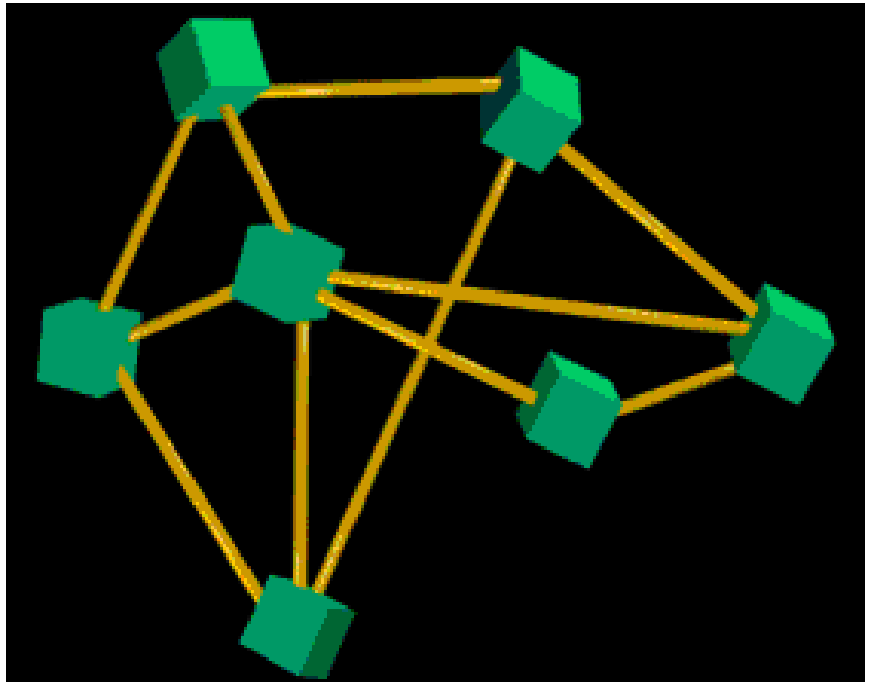




- Besonders beliebt, z.B. für die Organisation von größeren Mengen von Teilnehmerstationen oder Knoten
- In der Kommunikationstechnik gibt es sowohl logische Baumstrukturen nach dem Spanning Tree Algorithmus, als auch physische
- Eignet sich gut für flächendeckende Verkabelung oder für Netze in mehrstöckigen Gebäuden
- Baumtopologien werden bei Breitbandnetzen (IEEE 802.4) und bei Metropolitan Area Networks (MAN IEEE 802.6) verwendet

3.1.3 Topologien (5): Vermaschung





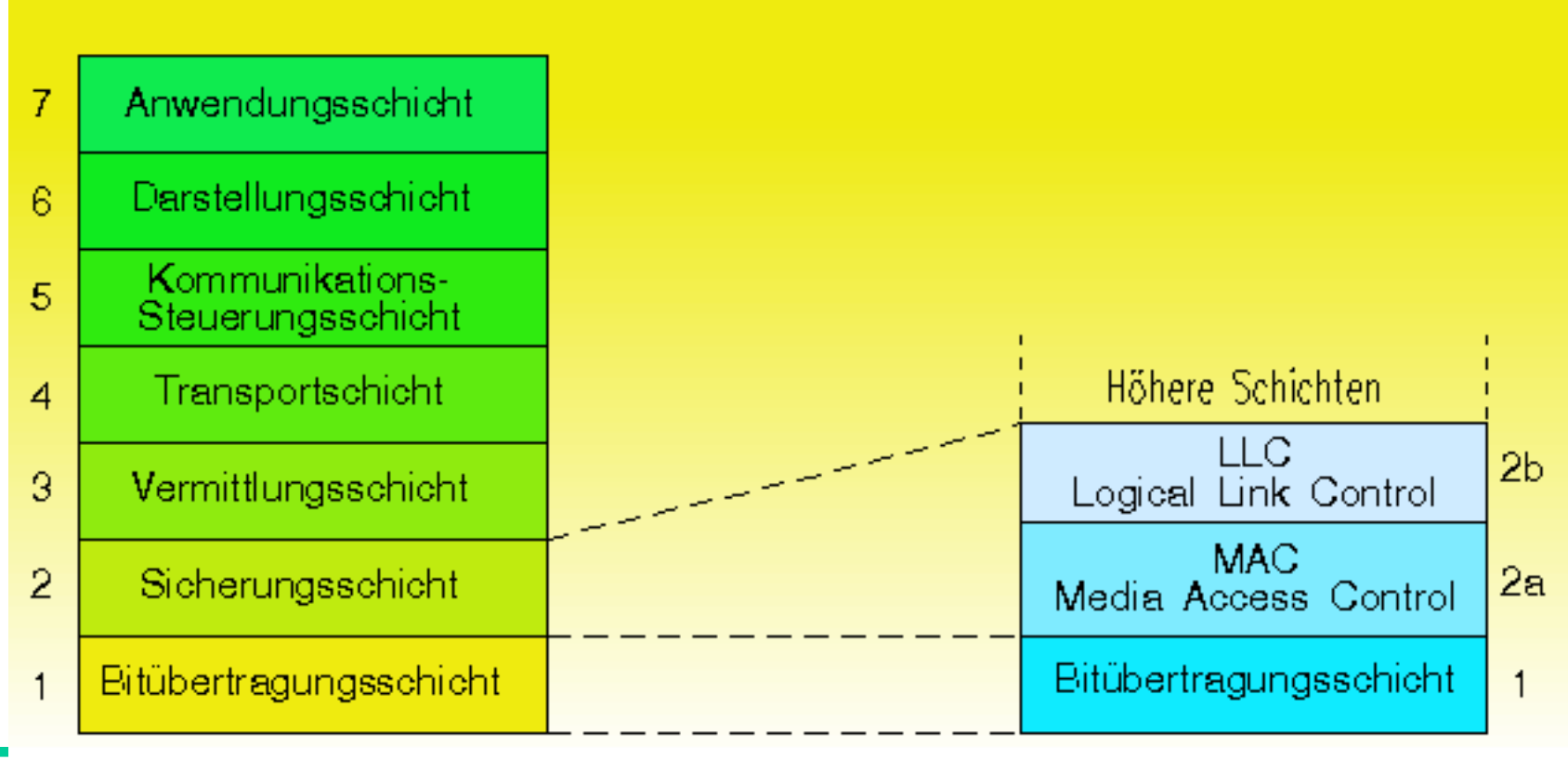
- Die Knoten sind auf mehreren Wegen miteinander verbunden, jedoch nicht notwendigerweise jeder mit jedem (außer bei Vollvermaschung)
- Diese Struktur, vorwiegend bei Weitverkehrsnetzen anzutreffen, hat den Vorteil, dass bei Staus oder Leitungsunterbrechungen zwischen einzelnen Knoten alternative Wege benutzt werden können
- Die Vermittlungsintelligenz ist in den Netzknoten angeordnet

3.1.4 LAN-Referenzmodell (1)

- **Insgesamt existieren unterschiedliche LAN-Techniken, je nach Wahl nachfolgender Aspekte:**
  - Netzstruktur
    - Physikalisches Medium (Material, Bandbreite, Störempfindlichkeit, Installation)
    - Konfiguration (Topologie, Ausdehnung, Stationsanzahl)
    - Signalstruktur (Basisband/Breitband, Codierung, Datenrate)
  - Zugriffsverfahren
    - Selektionsverfahren (Polling, Token Passing)
    - Reservierungsmethoden (FDM, fixed TDM)
    - Stochastische Verfahren (Aloha, CSMA/CD)
- **Netzdienste (Transportdienste, Managementdienste)**
- **Protokollhierarchien (XNS, IPX-Novell, TCP/IP, ISO)**

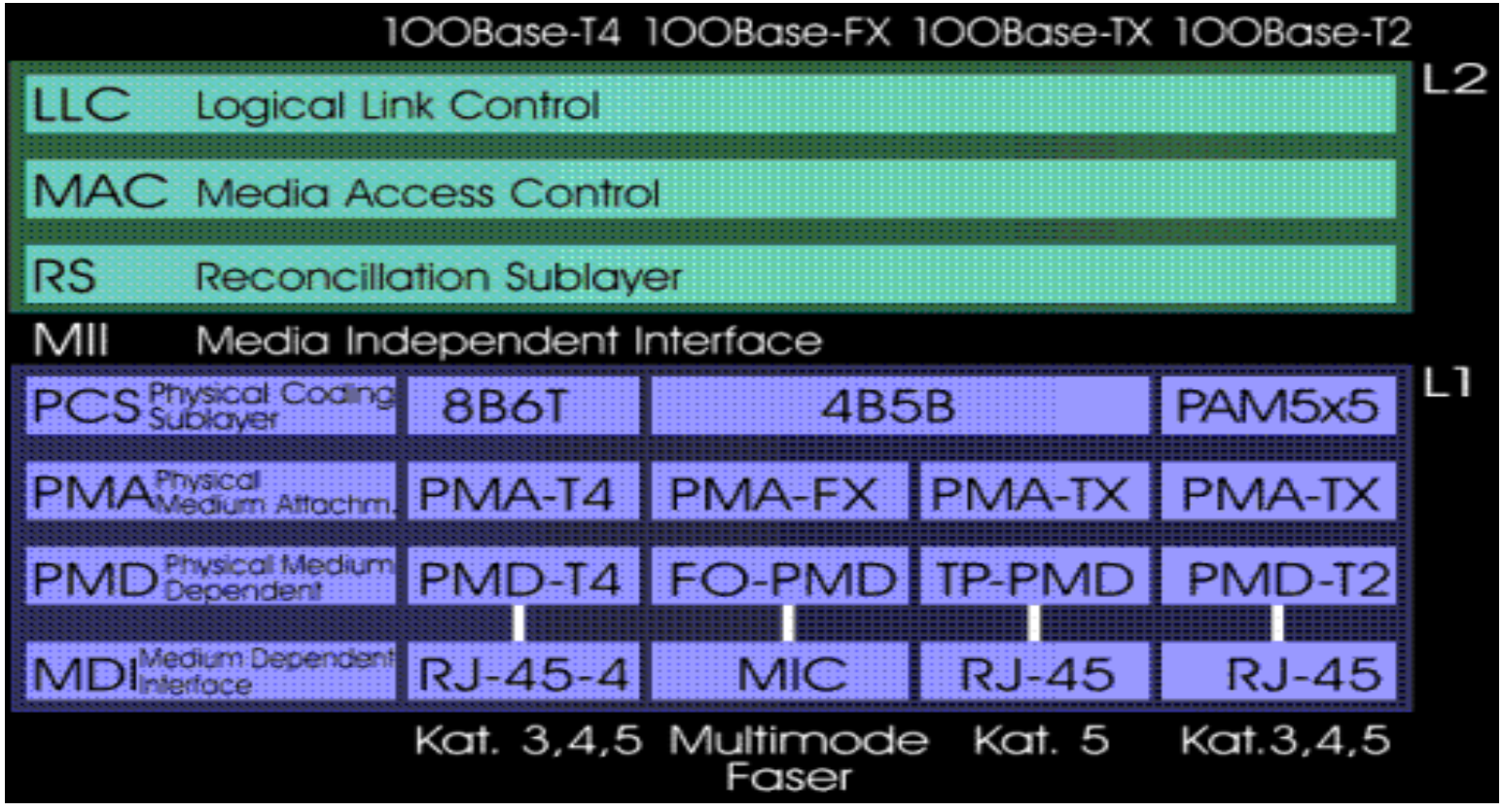
3.1.4 LAN-Referenzmodell (2)

- **Das LAN-Schichtenmodell wird von den Arbeitskreisen jeweils den Anforderungen entsprechend modifiziert; So ist beispielsweise bei den 10-Mbit/s-Varianten nach 802.3 die Sicherungsschicht in zwei Teilschichten und die Bitübertragungsschicht in drei Teilschichten unterteilt**



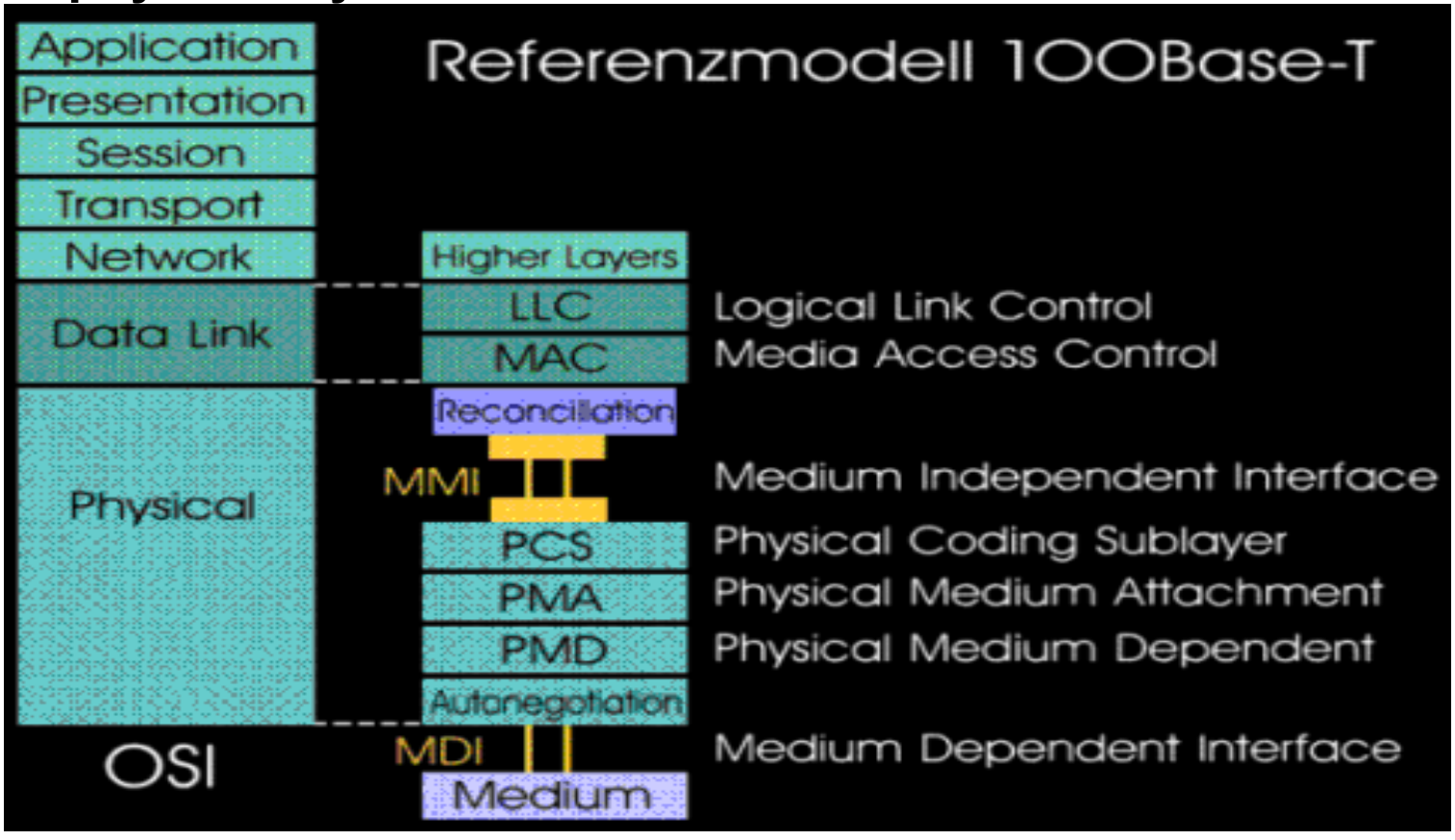
3.1.4 LAN-Referenzmodell (3)

- **Bei den Hochgeschwindigkeitsvarianten nach 802.3U mit 100Base-T und 100Base-X wird die Sicherungsschicht dreigeteilt in Logical Link Control (LLC), Media Access Control (MAC) und Reconciliation-Teilschicht (RS)**



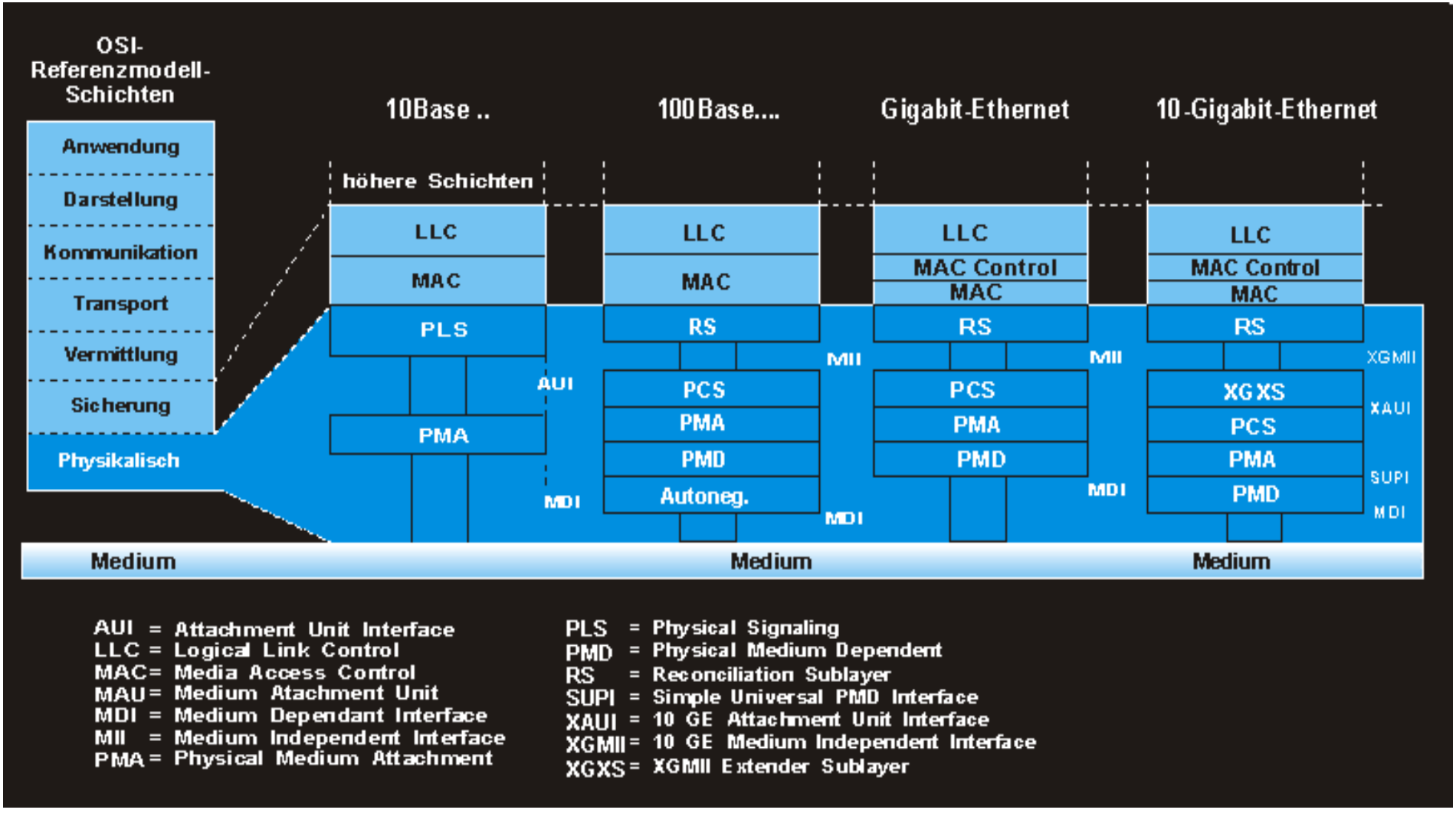
3.1.4 LAN-Referenzmodell (4)

- Der Reconciliation-Sublayer und das Media Independent Interface (MII) bilden bei den schnelleren Ethernet-Varianten - Fast-Ethernet, Gigabit-Ethernet und 10-Gigabit-Ethernet - zusammen den Zugang zum physical layer



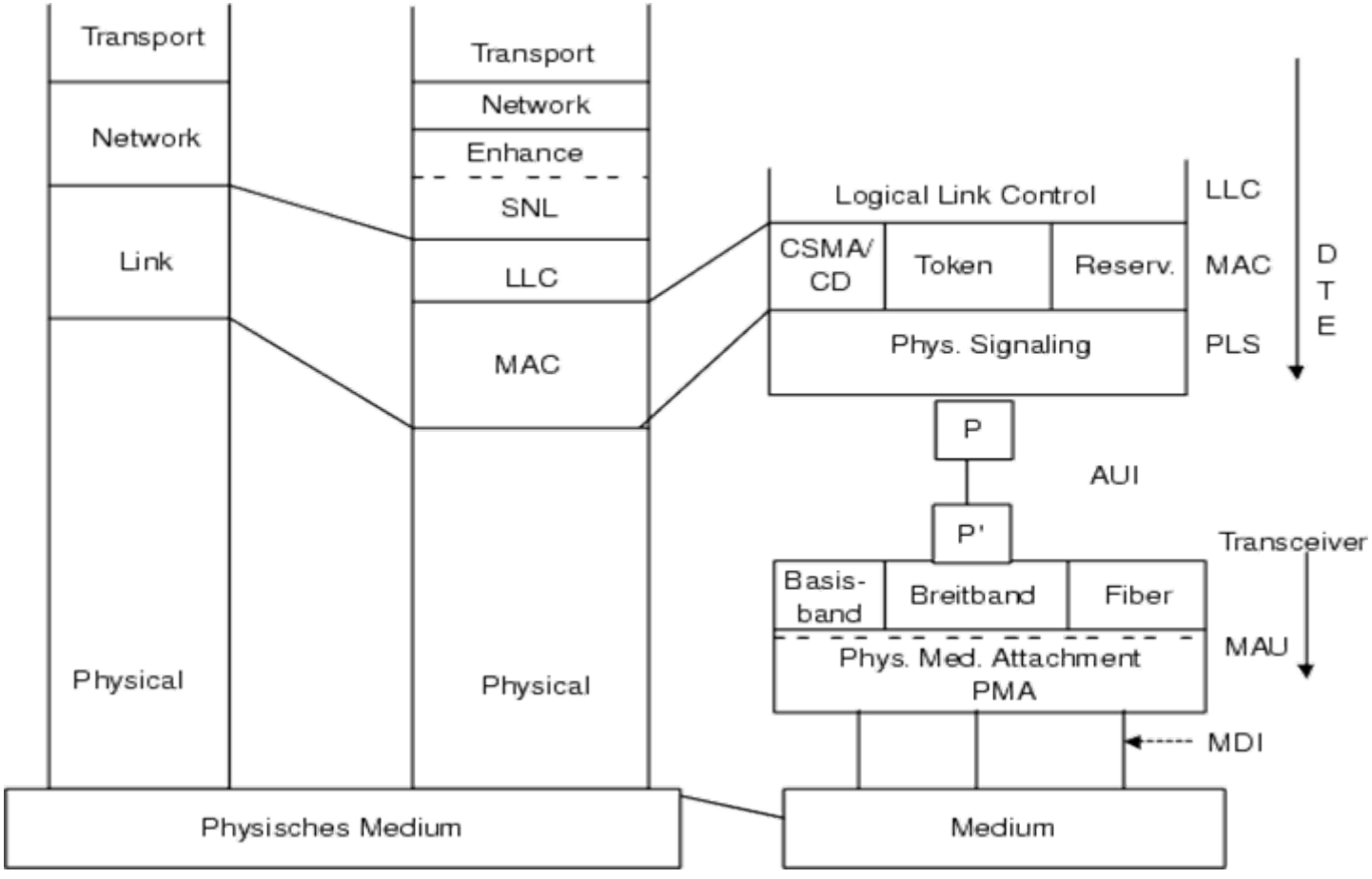
3.1.4 LAN-Referenzmodell (5)

- Schichtenmodell für die verschiedenen Ethernet-Varianten



3.1.5 LAN-Implementierungsmodell

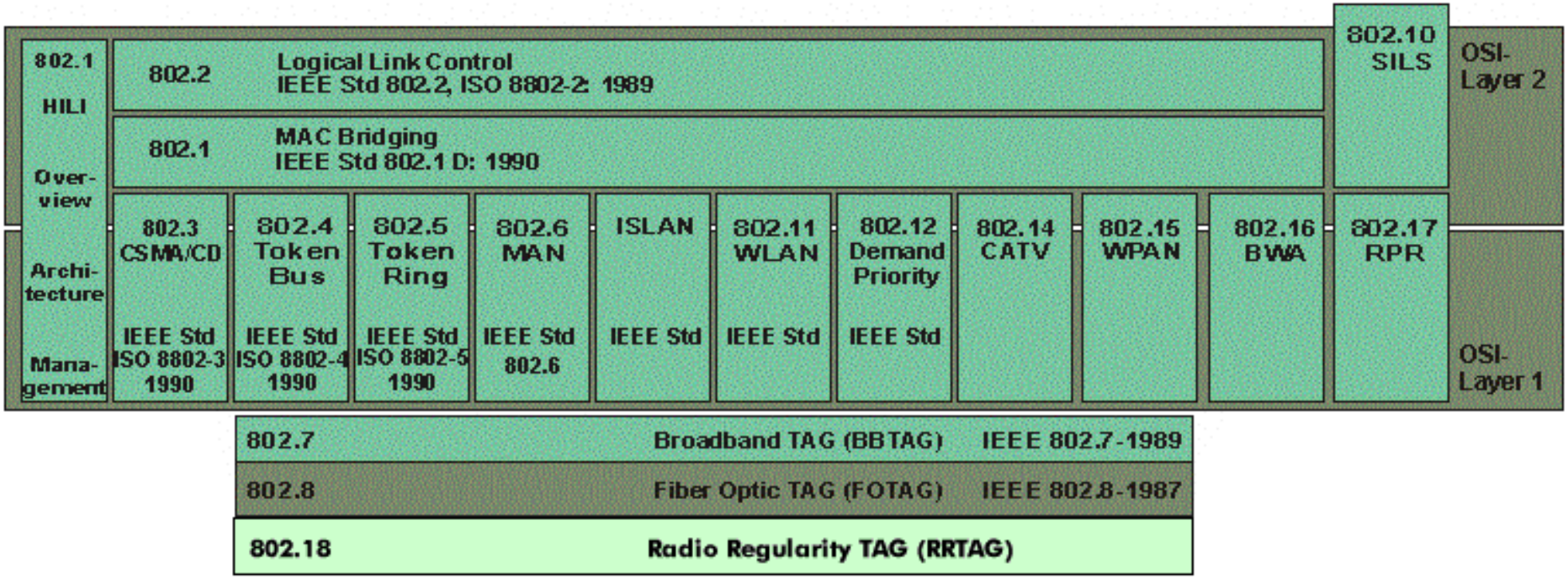
- **Trotz verschiedener Aspekte hat sich zur systematischen Beschreibung von Schnittstellen, Diensten und Protokollen *ein* LAN-Implementierungs-Referenzmodell bewährt**



SNL: Subnetwork Network Sublayer
LLC: Logical Link Control
MAC: Medium Access Control
MAU: Medium Attachment Unit
PLS: Physical Signaling
AUI: Attachment Unit Interface
MDI: Medium Dependent Interface

3.1.6 IEEE Standard 802 (1)

- IEEE hat für LANs abhängig vom gewählten Übertragungsmedium, der Netztopologie und dem Medium-Zugangsverfahren mehrere Standards definiert, die in der Reihe 802 zusammengefasst sind



3.1.6 IEEE Standard 802 (2)

- **Für jeden LAN-Typ ergeben sich unterschiedliche Komponenten wie z.B.:**
  - unterstützte Medien
  - Anschlusskomponenten (z.B. Transceiver)
  - Verbundkomponenten (Repeater, Bridges, Router)
- **Übertragungsmedien**
  - bei Ethernet: Koaxialkabel/Basisband bei Bus-Topologie und Twisted Pair für Hubtopologie (Fast Ethernet)
  - bei Token-Ring: Shielded Twisted Pair (STP)
  - gemäß Norm "Strukturierte Verkabelung" EN 50173, also
    - STP im Tertiärbereich (Typ 5/6), (Raten bis 155 Mbps)
    - LWL im Primär/Sekundärbereich
    - Hubstrukturen

3.1.6 IEEE 802.1

- Beschäftigt sich mit Fragen, die alle IEEE-802-Arbeitskreise und LAN-Typen betreffen; dazu gehören insbesondere allgemeine Management-Fragen und Aspekte des Internetworking
- Es wurden bereits eine ganze Reihe von Normen dieses Arbeitskreises veröffentlicht (u.A.):
  - **802.1a-1990: Overview and Architecture**
  - **802.1b-1992: LAN / MAN Management**
  - **802.1q: Virtual LANs, VLAN, Architecture and Bridging, GVRP, GARP VLAN Registration Protocol**
  - **802.1v: VLAN Classification by Protocol and Port: Die Gruppe arbeitet an der Klassifikation von virtuellen LANs nach Port und Protokoll**
  - **802.1X: Port Based Network Access Control**

3.2 LANs nach IEEE 802.3

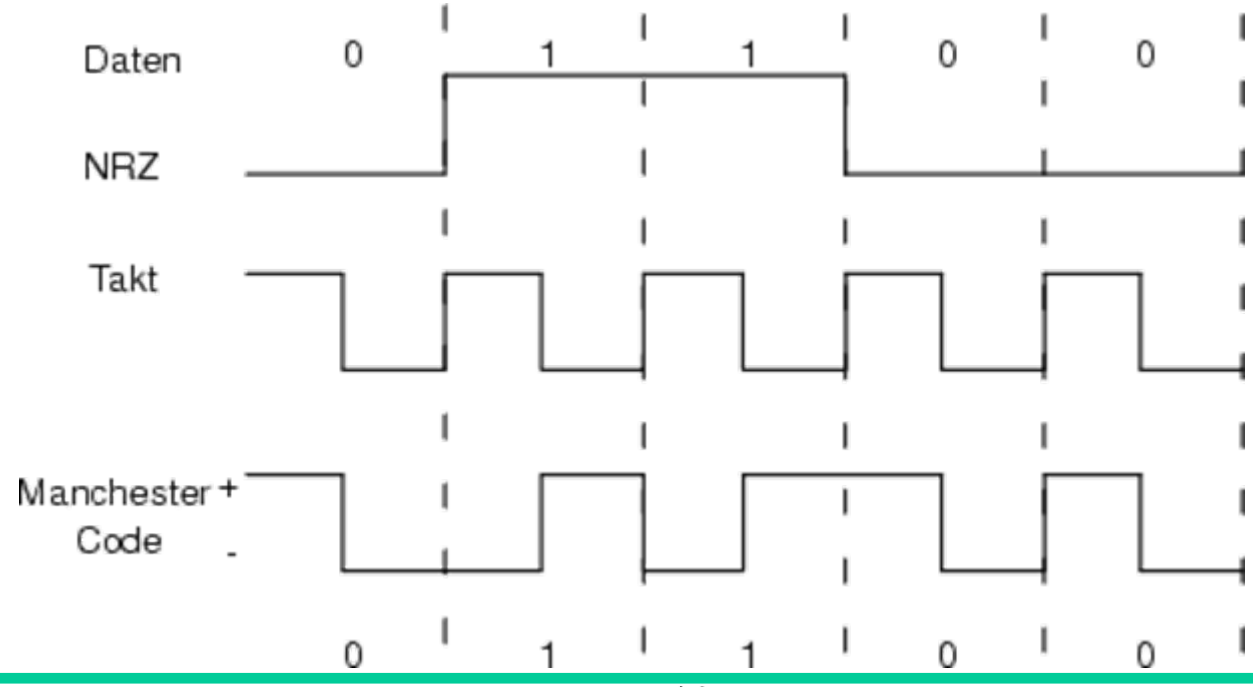
- **3.2.1 Manchester Codierung**
- **3.2.2 CSMA/CD**
- **3.2.3 Varianten**
  - 10 Mbit/s
  - 100 Mbit/s (802.3n)
  - 1 Gbit/s (802.3z)
  - 10 Gbit/s (802.3ae)

3.2 Standard-Ethernet (IEEE 802.3)

10Base5	Standard Koaxialkabel (0,5 Zoll Durchmesser); maximale Segmentlänge von 500 m, Basisband
10Base2	Dünnes Koaxialkabel (0,25 Zoll Durchmesser); maximale Segmentlänge 200 m; Basisband
10BaseT	Twisted Pair-Kabel mit Hub (Stern)-Topologie; Basisband
10BaseF	Lichtwellenleiter mit Hub (Stern)-Topologie; Basisband
10Broad36	TV-Koaxialkabel (36 MHz Bandbreite) mit Kopfstation (Head-End); Breitband
100BaseT	STP mit Hub (Stern); Basisband
1000BaseT	Twisted Pair mit Hub

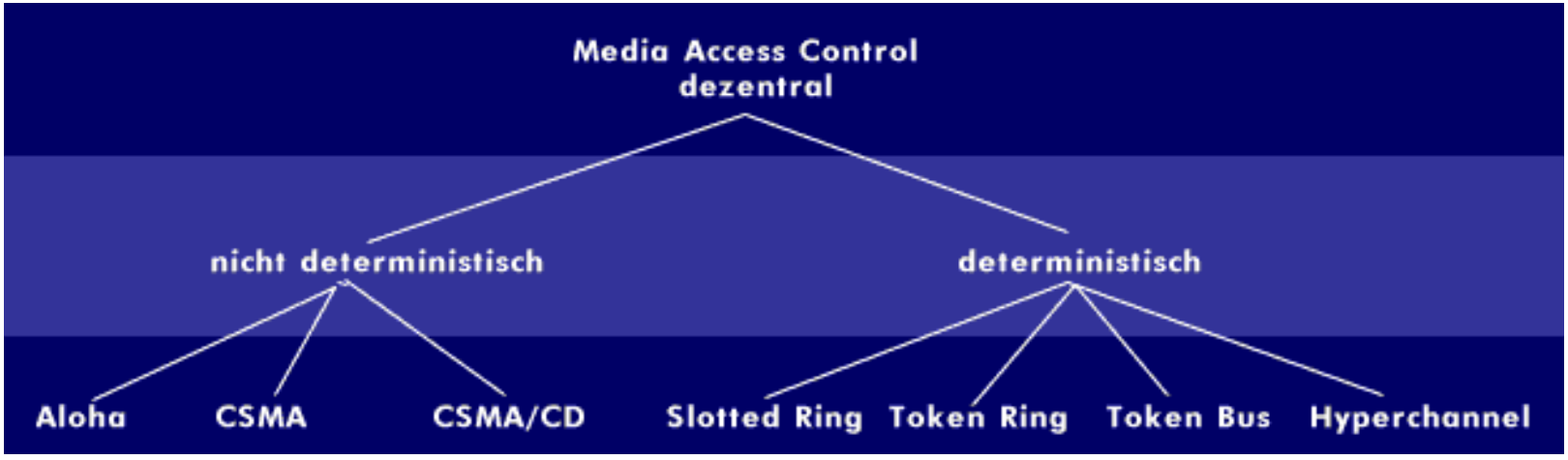
3.2.1 Manchester-Kodierung (z.B. bei 10Base5)

- **Kodierung von 0 oder 1 erfolgt durch Flankenwechsel in der Mitte der Darstellung eines Bits; Der wird zur Synchronisation verwendet**
  - 0: Wechsel von +0,85 V nach –0,85 V
  - 1: Wechsel von –0,85 V nach +0,85 V
- **Man benötigt zwei Schritte, um ein Bit zukodieren, d.h. die Baudrate ist doppelt so groß wie die Bitrate**
- **Anwendung bei Bustopologien für LANs**



3.2.2 Zugriffsverfahren des Ethernet: CSMA/CD (1)

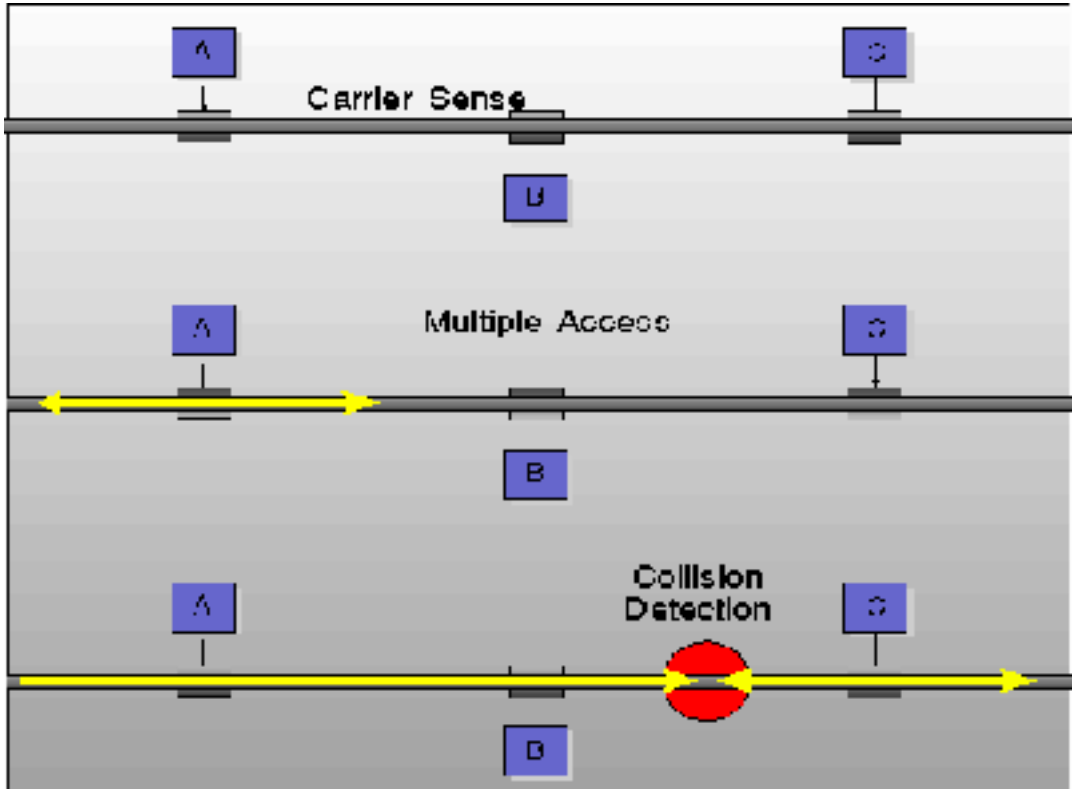
- **Zugriffsverfahren (allgemein)**



- **CSMA/CD („Carrier Sense Multiple Access with Collision Detection“) gehört zu den kollisionsbehafteten Verfahren, denen ein Konkurrenzschema zugrunde liegt; es umfasst 3 Teilaktivitäten**
  - Carrier sense: Lauschen auf der Leitung (Listen-before-Talk)

3.2.2 Zugriffsverfahren des Ethernet: CSMA/CD (2)

- Collision detection: Mithören während des Sendens, um eine Kollision zu erkennen (Listen-while-Talking) und
- Backoff-Algorithmus: Wiederaufsetzen einer Sendung nach einen Konfliktfall

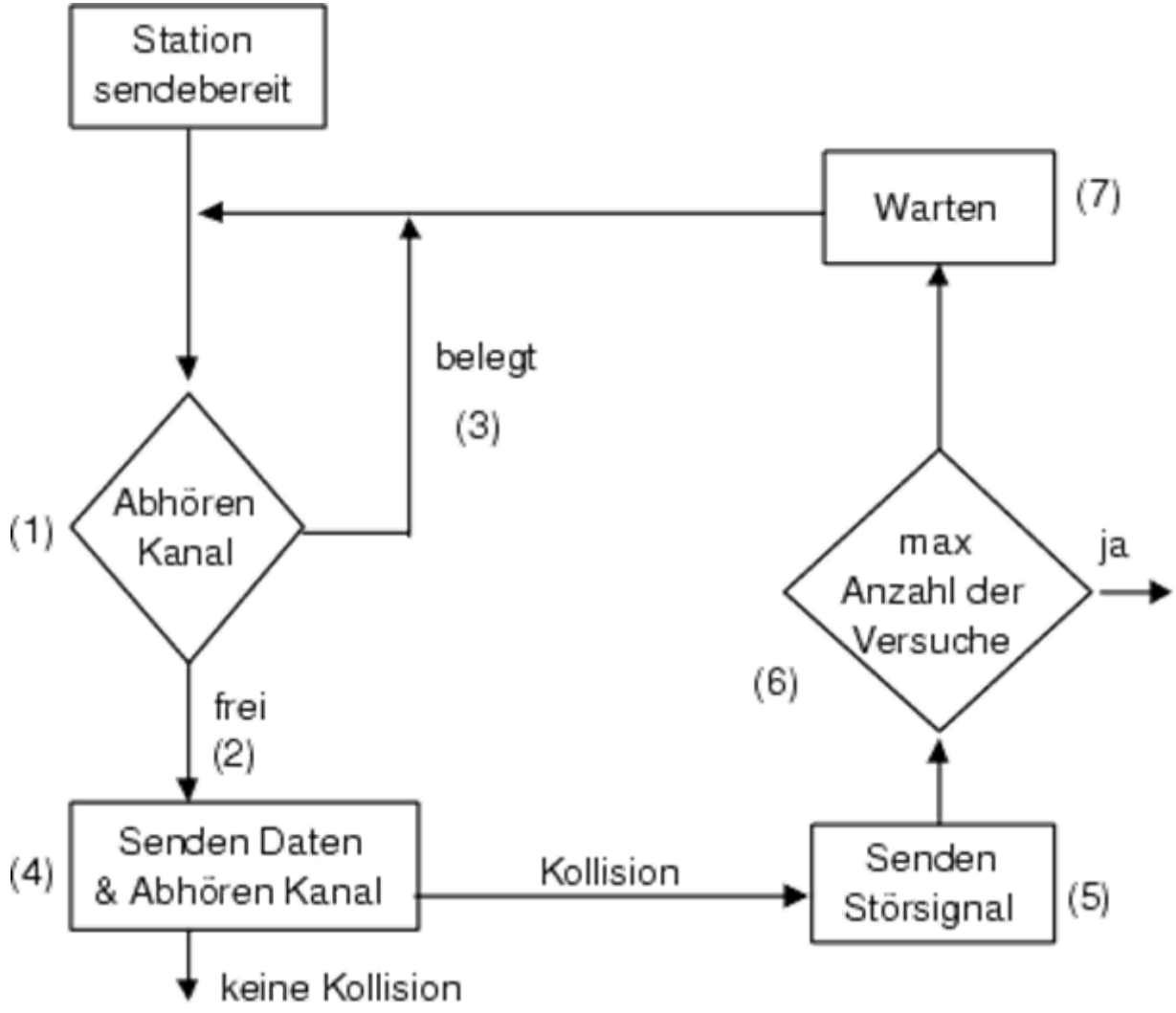


3.2.2 CSMA/CD

❑ Parameter des CSMA/CD-Standards

- Datenrate: 10 Mbps mit Manchester Codierung bei 10Base5
- Slot time: 512 Bitübertragungen
- Übertragungsfrist ("interframe gap"): 9.6 Mikrosekunden; Warten nach Entdeckung einer freien Leitung
- max. Fehlversuche: 16
- Backoff-Obergrenze: 10; definiert das Intervall für die zufällige Wartezeit
- Störsignal: 32 bits
- max. Framelänge:1518 bytes
- min. Framelänge: 64 bytes

3.2.2.1 Graphische Übersicht von CSMA/CD

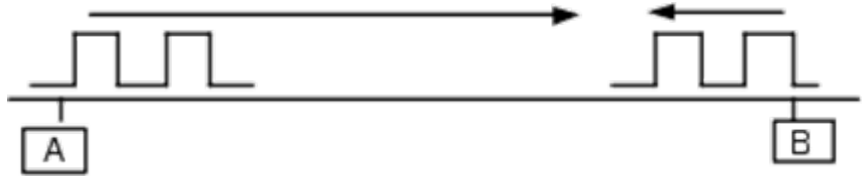


3.2.2.2 Einzelschritte von CSMA/CD (1)

1. **Sendewillige Station überwacht Übertragungsmedium**
   - Entdecken des Carrier-Signals: Medium belegt, d.h. im Zustand 0-Bit oder 1-Bit
2. **Übertragungsmedium frei -> Übertragung kann beginnen**
   - Nach Freiwerden des Mediums kurze Frist abwarten, damit alle Teilnehmer das vorherige Paket ohne Beeinträchtigung empfangen können. Wartezeit („Interframe Gap“) beträgt ca. 9,6 Mikrosekunden
3. **Übertragungsmedium nicht frei -> warten bis es frei wird, danach 2**
4. **Während der Übertragung simultane Abhörung des Kanals**
   - Unterschied zwischen gesendeter Information und Information auf Medium -> Kollision hat stattgefunden, d.h. auch eine andere Station hat angefangen zu senden; Kollisionen treten am Anfang einer Übertragung auf (wegen Medienüberwachung)

3.2.2.2 Einzelschritte von CSMA/CD (2)

- *Kollisionsfenster*: 2 * Signallaufzeit des ersten Framebit durch gesamtes Übertragungsmedium



5. **Senden eines Störsignals, Länge von 4-6 Bytes ("jam signal")**
6. **maximale Anzahl von Fehlversuchen**
7. **Warten gemäß *Backoff Strategie* ("truncated binary exponential backoff")**
   - Berechnung der Wartezeit abhängig von der Anzahl der Wiederholungen
   - i * Warteperiode ("slot-time") mit $i \in IN$ und $0 \leq i \leq 2^k$
   - k = min (Anzahl Wiederholungen, Backoff-Obergrenze)

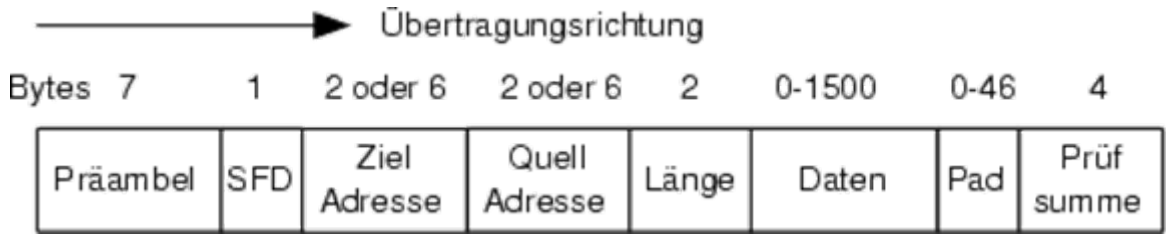
   Beispiel:

   1. Kollision: $i \in [0,2]$, d.h. i = 0,1,2

   10. Kollision: $i \in [0,1024]$

3.2.2.3 CSMA/CD: Frameaufbau (1)

- **Frameaufbau: Standard definiert eine minimale (512 bits) und maximale Framelänge (1518 bytes)**



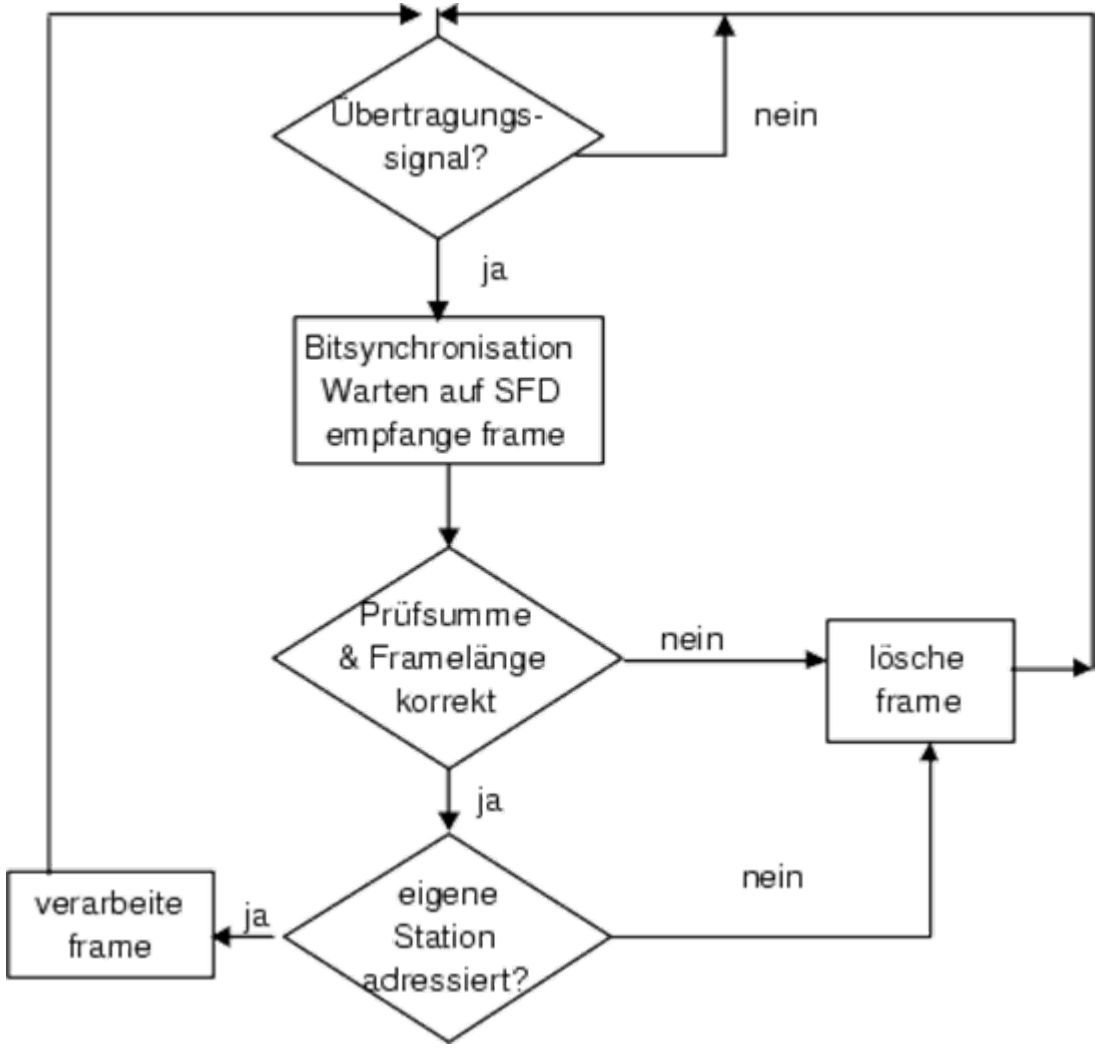
  - ***Präambel*: dient dem Empfänger zur Bitsynchronisation und zur Lokalisierung des 1. Framebits; besteht aus Bitmuster 10101010 je Byte**
- ***SFD*: "start of frame delimiter" kennzeichnet den Frame-Anfang; Bitmuster 10101011**
- ***Ziel-/Quelladresse*: spezifizieren das empfangende (möglicherweise mehrere) und sendende DTE; innerhalb eines LAN nur einheitliche Längen erlaubt (16 oder 48 Bit)**
- ***Länge*: spezifiziert die Anzahl der Bytes im Datenfeld**
- ***Pad*: da Datenlänge 0 erlaubt ist, müssen Füllbits ("pad bits") übertragen werden, damit minimale Framelänge erreicht wird**
- ***Prüfsumme*: Generatorpolynom vom Grad 32 ("CRC")**

3.2.2.3 CSMA/CD: Frameaufbau (2)

- **Frameaufbau (Fortsetzung)**
  - Frame ist ungültig, falls
    - Framelänge inkonsistent mit Inhalt des Längenfeldes
    - Frame verletzt minimale und maximale Grenzen
    - CRC-Prüfung ergibt Fehler
    - Framelänge ist kein Vielfaches von 8

3.2.2.3 CSMA/CD: Übertragung von Frames

- **Empfangen eines Frames**



3.2.3.1 Ethernet-Varianten für 10 Mbit/s (1)

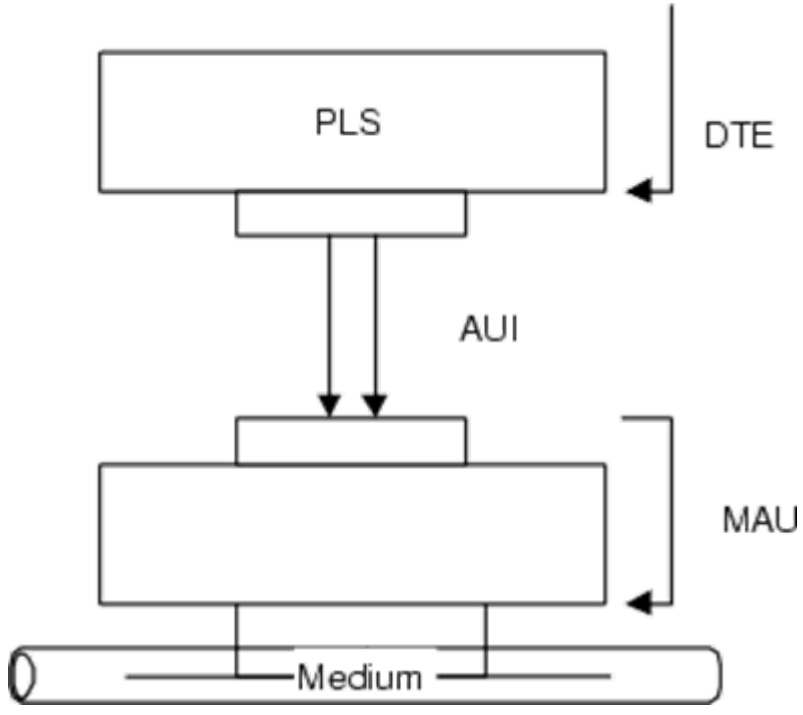
- **Ethernet-Verkabelung**
  - 10Base5; Dickes Koaxialkabel; Max Segment 500m; Knoten/Seg. 100; ursprüngliches Kabel, heute veraltet
  - 10Base2; Dünnes Koaxialkabel; Max Segment 185m; Knoten/Seg. 30;
  - 10BaseT; Twisted Pair; Max Segment 100m; Knoten/Seg. 1024; kostengünstigstes System
  - 10BaseF; Glasfaser; Max Segment 2000m; Knoten/Seg. 1024; beste Lösung zwischen Gebäuden

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (2)

- **10Base5 (Standard-Ethernet)**
  - Klassische Ausführung eines CSMA/CD-Bussystems mit Basisbandübertragung
  - Ein 10Base-5-Segment darf 500 m nicht überschreiten
  - Höchstens 100 MAUs dürfen an einem Segment angeschlossen werden, wobei ein Minimalabstand von 2,5 m nicht unterschritten werden darf; mit einer Laufzeitverzögerung von höchstens 2.165 ns
  - Ein AUI-Kabel darf maximal 50 m lang werden; eine maximale Laufzeitverzögerung von 257 ns
  - Zwischen zwei Stationen dürfen höchstens fünf LAN-Segmente und vier Repeater liegen, die "eigenen" Segmente eingeschlossen; von den Segmenten dürfen allerdings nur drei Segmente Koaxialsegmente sein („5-4-3“-Regel)

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (3)

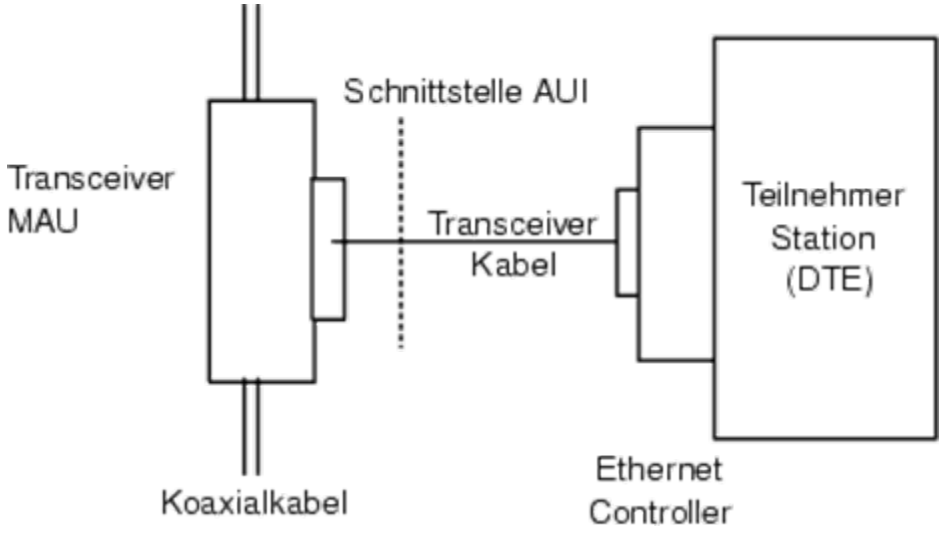
- **10Base5 (Standard-Ethernet)**
  - Transceiver
    - Unterteilung von Schicht 1

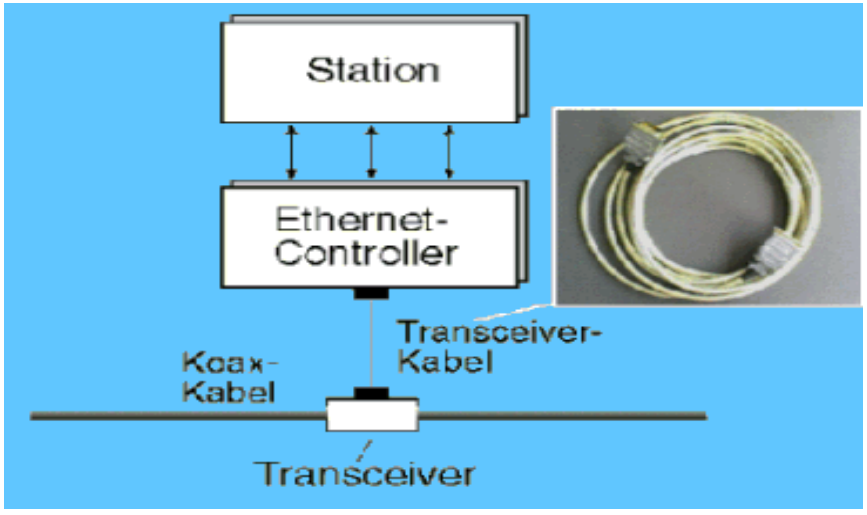


PLS ("physical signaling")
AUI ("attachment unit interface")
MAU ("medium attachment unit")

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (4)

- **10Base5 (Standard-Ethernet)**
  - Transceiver-Anschluss



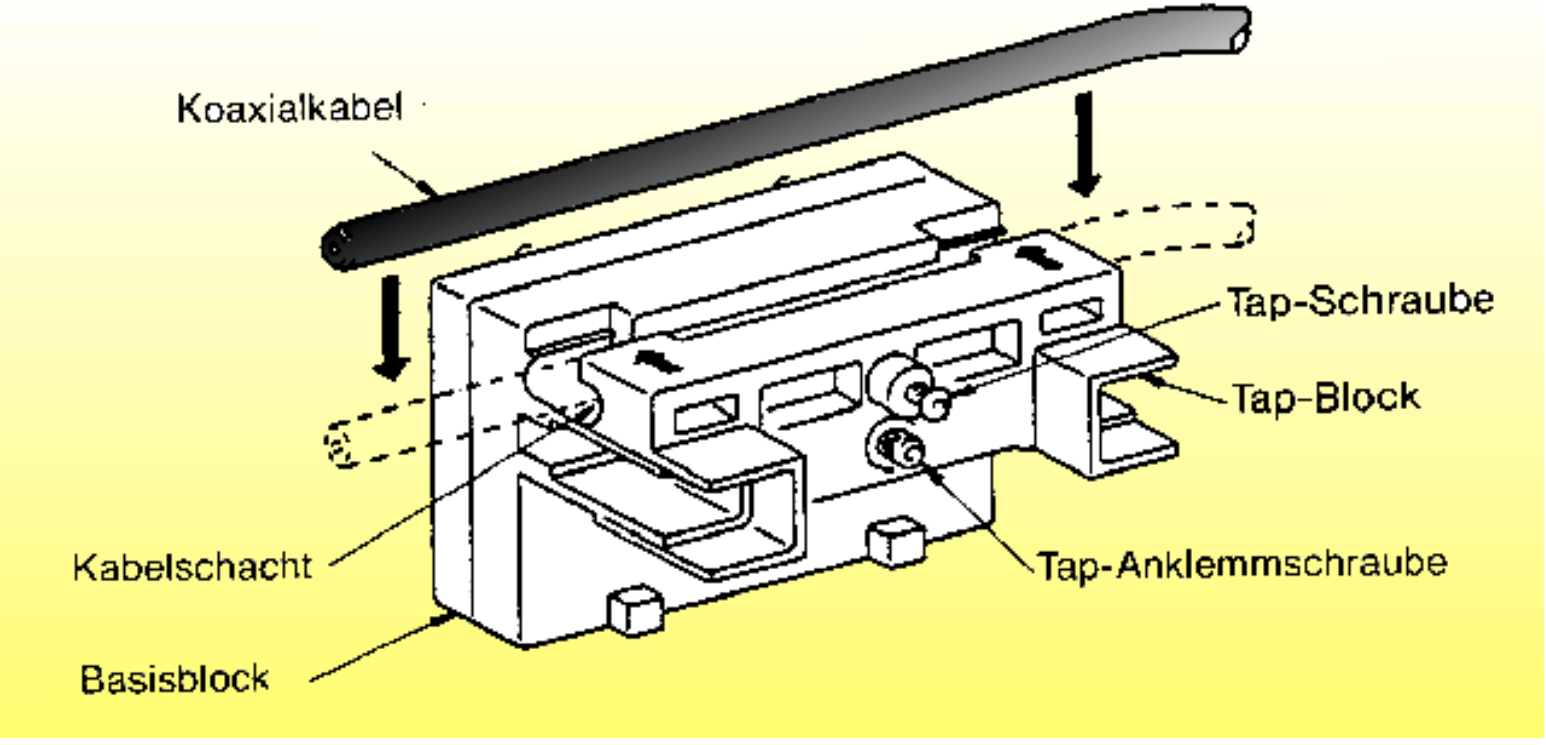


3.2.3.1 Ethernet-Varianten für 10 Mbit/s (5)

- **10Base5 (Standard-Ethernet)**
  - Transceiver
    - Transceiver ist ein Kombinationswort aus Transmitter (Sender) und Receiver (Empfänger) und bezeichnet eine Sende/Empfangseinrichtung
    - Der Transceiver realisiert den Netzzugang einer Station an das Ethernet und entspricht damit der Medium-Anschlusseinheit (MAU)
  - Aufgaben eines Transceivers
    - Senden und Empfangen von Daten
  - Entdecken von Kollisionen auf Übertragungsmedium
  - Isolierung des Kabels von der Schnittstelle zum DTE
  - Schutz des Kabels vor Fehlverhalten verursacht von Transceiver oder DTE
  - (z.B. Jabber Control, d.h. Schutz vor langen Frames)

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (6)

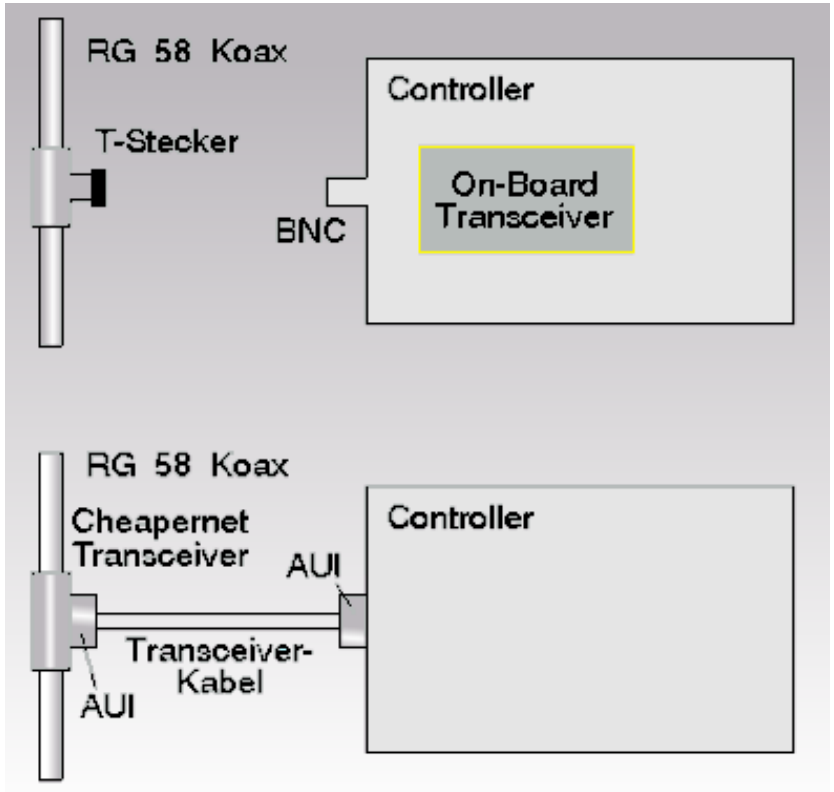
- **10Base5 (Standard-Ethernet) (Fortsetzung)**
  - Montageblock mit eingelegten Yellow-Kabel



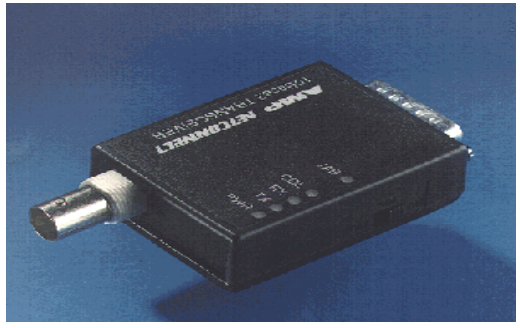
3.2.3.1 Ethernet-Varianten für 10 Mbit/s (7)

❑ 10Base5 (Standard-Ethernet) (Fortsetzung)

- Der Transceiver kann, wie im Falle des klassischen Yellow-Cable-Anschlusses, direkt am Kabel angeschlossen werden, mittels einer so genannten Vampirklemme (man bohrt,während des Betriebes, ein Loch in das Kabel, das bis zum Mittellleiter reicht), oder er befindet sich auf dem Controller-Board
- Er kann allerdings auch als externe Einheit ausgeführt sein
- Transceiver-Anschluss



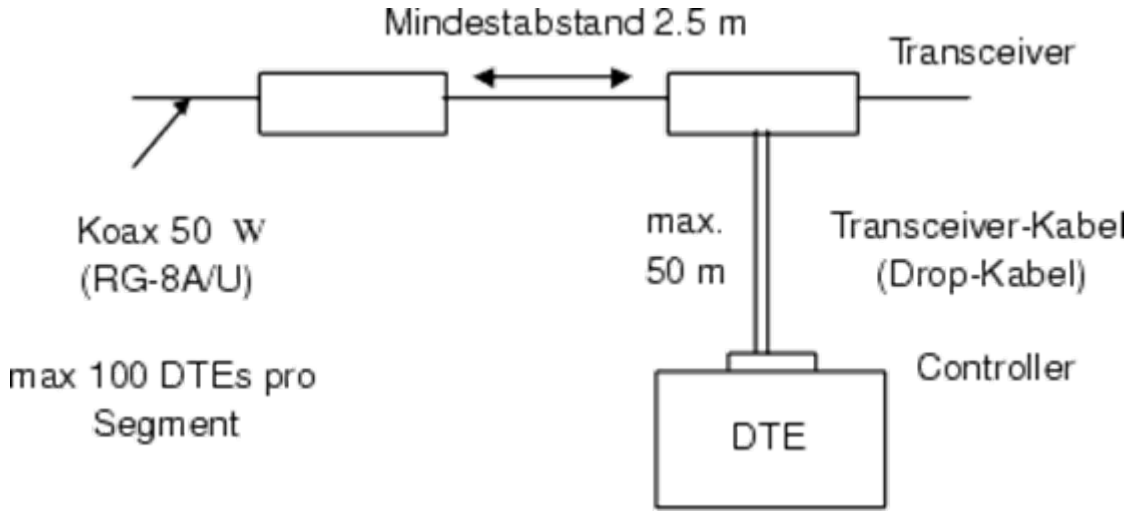
BNC-Transceiver



3.2.3.1 Ethernet-Varianten für 10 Mbit/s (8)

❑ 10Base5 (Standard-Ethernet) (Fortsetzung)

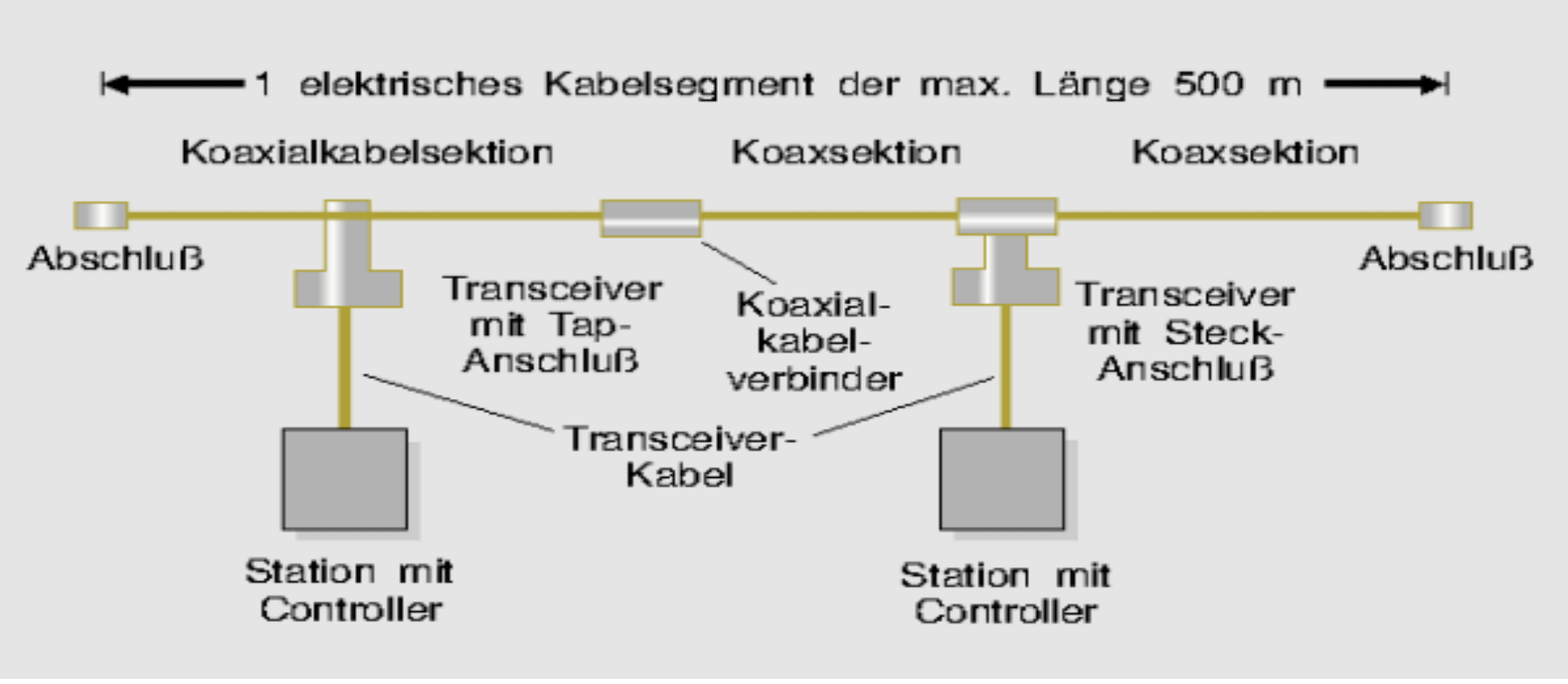
- Transceiver: Topologie



  - Zwischen je 2 Ethernet Stationen dürfen maximal 4 Repeater liegen
    ⇒ maximale Ausdehnung eines Ethernets ist beschränkt auf 2.5 km
- Anschluss des Transceivers mittels
  - T-Verbindung
  - Tap-Verbindung

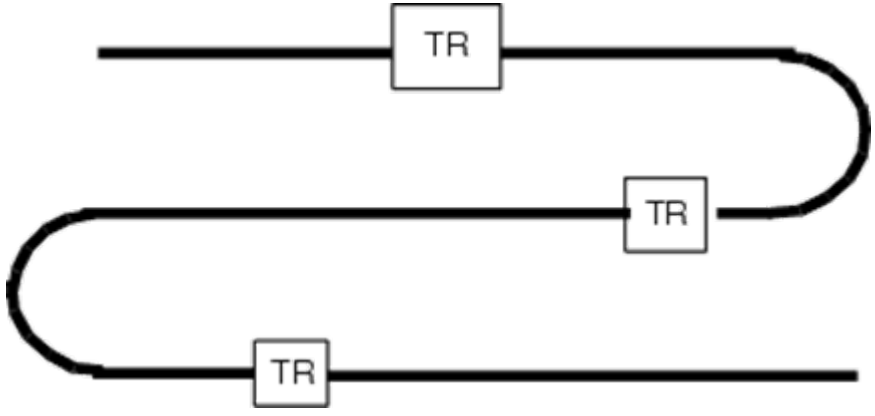
3.2.3.1 Ethernet-Varianten für 10 Mbit/s (9)

- **10Base5 (Standard-Ethernet)**
  - Ethernet-Segmente



3.2.3.1 Ethernet-Varianten für 10 Mbit/s (10)

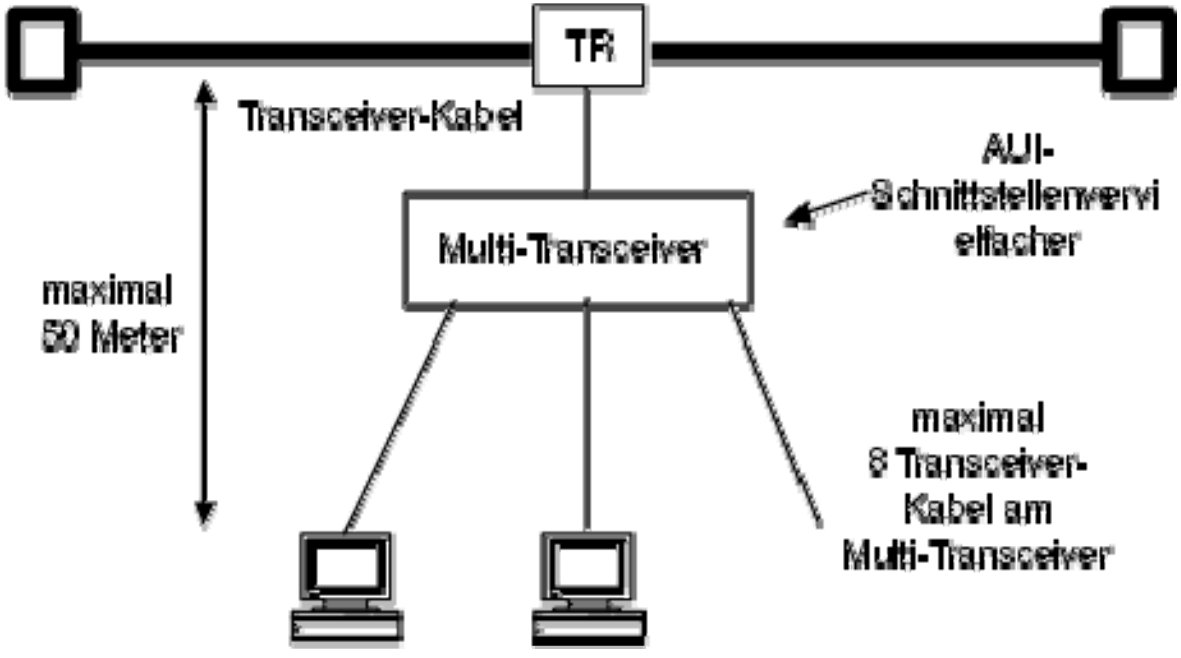
- **10Base5 (Standard-Ethernet)**
  - Schleifenbildung



  - pro Ethernet-Station ein Transceiver; zwischen 2 Transceivern sind 2.5 m Kabel notwendig
  - Lösung: Verwendung Multi-Transceiver zur Vervielfachung der AUI Schnittstelle

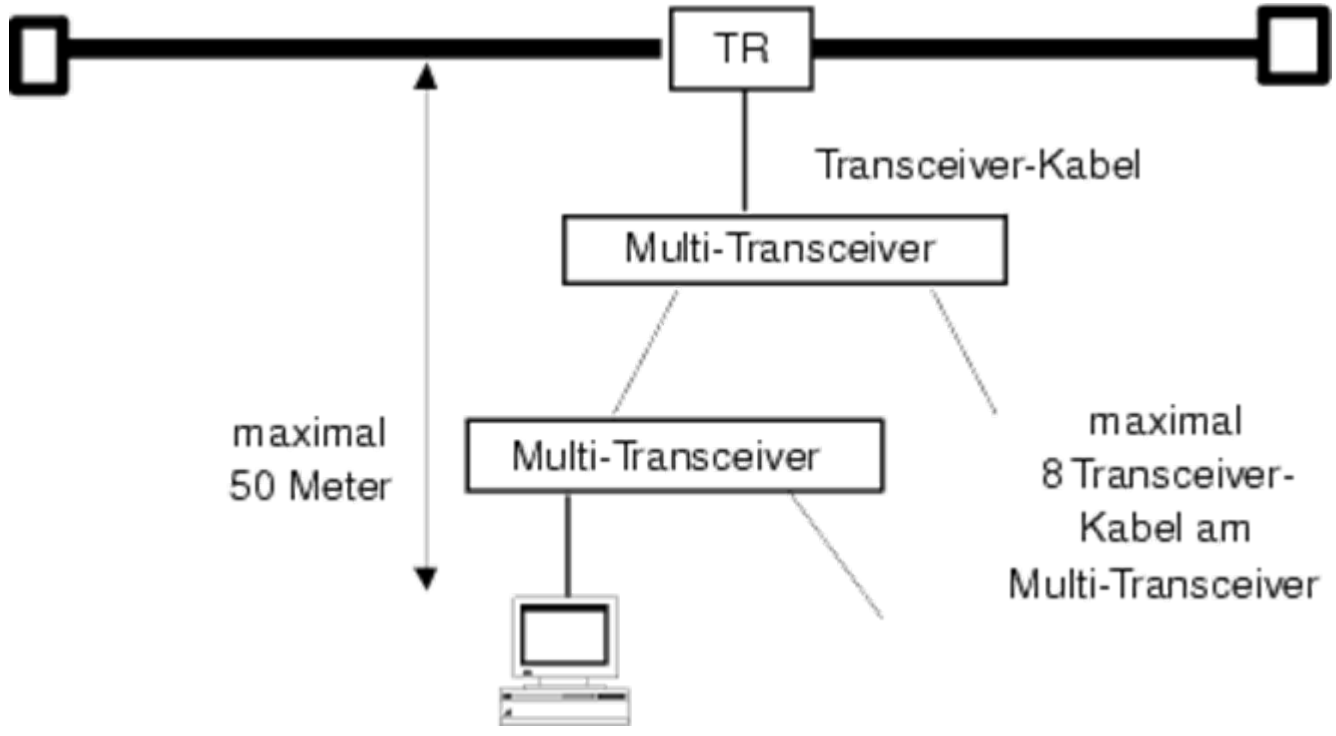
3.2.3.1 Ethernet-Varianten für 10 Mbit/s (11)

- **10Base5 (Standard-Ethernet)**
  - Multitransceiver



3.2.3.1 Ethernet-Varianten für 10 Mbit/s (12)

- **10Base5 (Standard-Ethernet)**
  - Kaskadierung von Multitransceivern

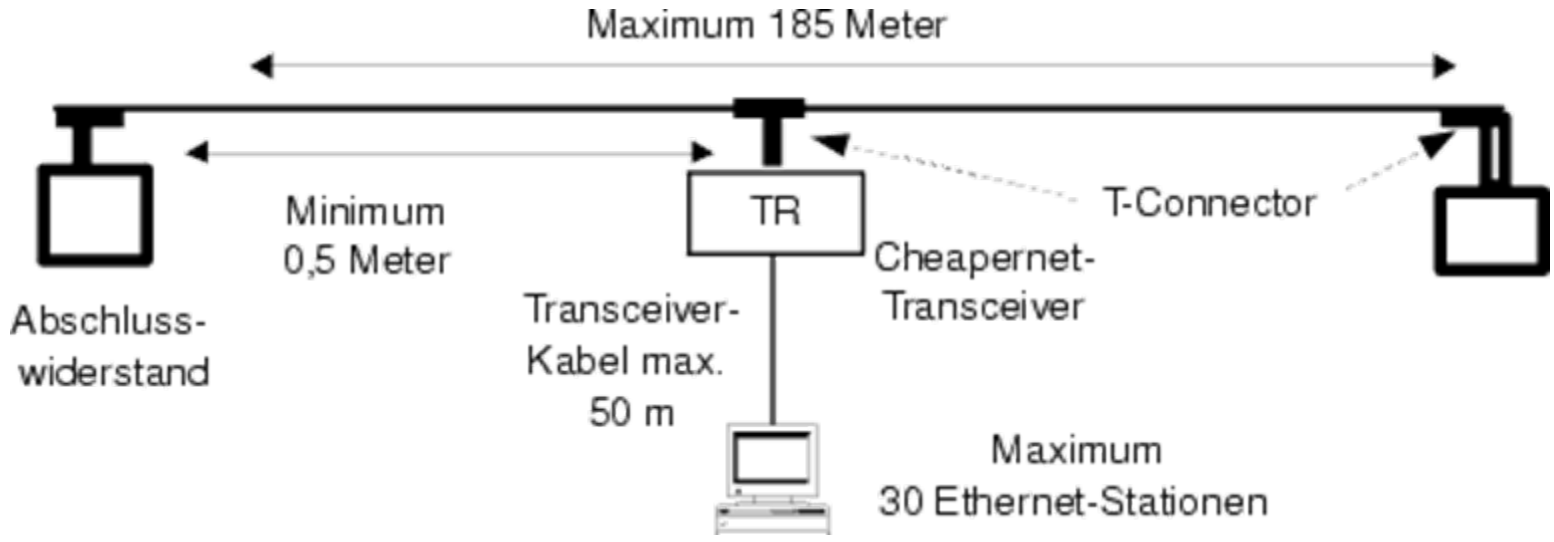


3.2.3.1 Ethernet-Varianten für 10 Mbit/s (13)

- **10Base2 (Cheapernet)**
  - Der Standard 10Base-2 beschreibt eine Ethernet-Variante mit einem dünnen Koaxialkabel
  - Die Datenrate beträgt 10 Mbit/s und die Topologie ist wie bei 10Base-5 ein Bus, allerdings nur von der max. Länge 185 m pro LAN-Segment ohne Repeater
  - An ein LAN-Segment können bis zu 30 Stationen angeschlossen werden
  - Im Gegensatz zum 10Base-5 befindet sich eine Cheapernet-MAU meistens komplett auf der Adapterkarte, die dann zum Anschluss an das LAN-Segment einen BNC-T-Konnektor bzw. eine BNC-Buchse besitzen muss
  - 10Base-2 kennt ebenfalls das Konzept der Repeater
  - Mittels geeigneter Geräte lassen sich 10Base-5- und 10Base-2-Segmente untereinander mischen, wobei ähnliche Randbedingungen gelten wie bei 10Base-5
  - Ein reines Cheapernet kann somit maximal 925 m lang werden
  - 10Base-2 wird kaum noch eingesetzt, die sternförmige Twisted-Pair-Verkabelung von 10Base-T ist eine wirtschaftliche Alternative

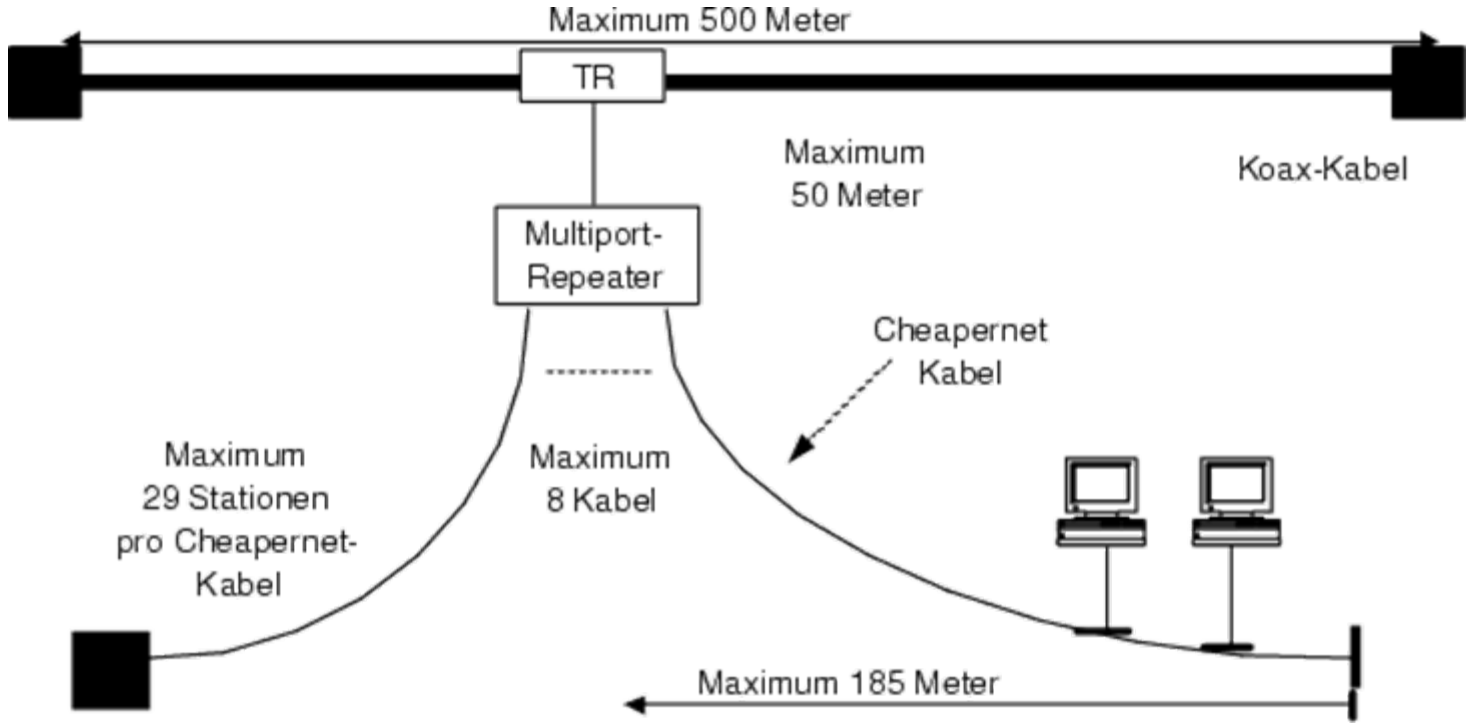
3.2.3.1 Ethernet-Varianten für 10 Mbit/s (14)

- **10Base2**
  - Eigenschaften



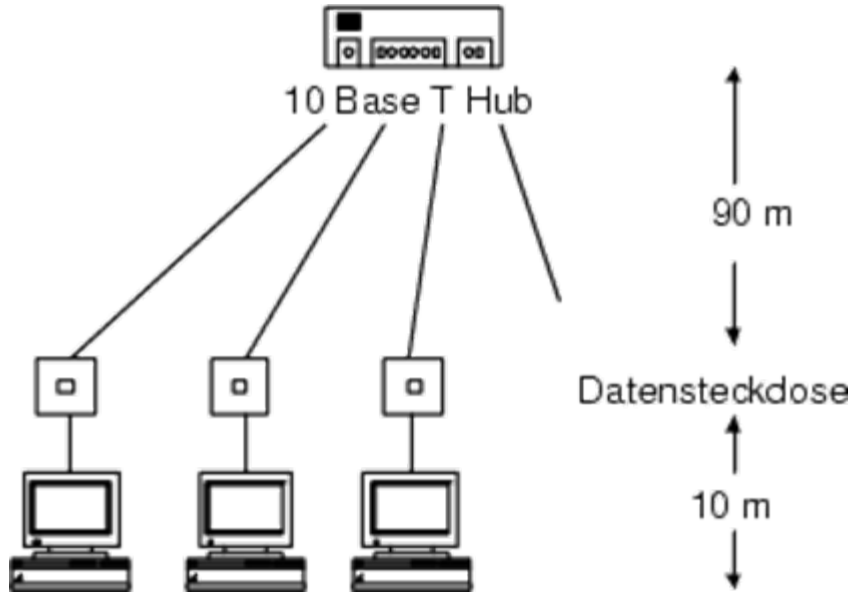
3.2.3.1 Ethernet-Varianten für 10 Mbit/s (15)

- **10Base2**
  - Eigenschaften



3.2.3.1 Ethernet-Varianten für 10 Mbit/s (16)

- **10BaseT**
  - Twisted Pair (STP und UTP)
  - Topologie: Physischer Stern/Logischer Bus



    - Hub ist Repeater (kollabierter Bus)
  - Kabel: UTP, meist STP, Dämpfung < 11,5 dB, Segmentverzögerung < 1000 ns
  - Maximale Netzlänge mit kaskadierten Hubs: 2,5 km, Stecker: RJ 45

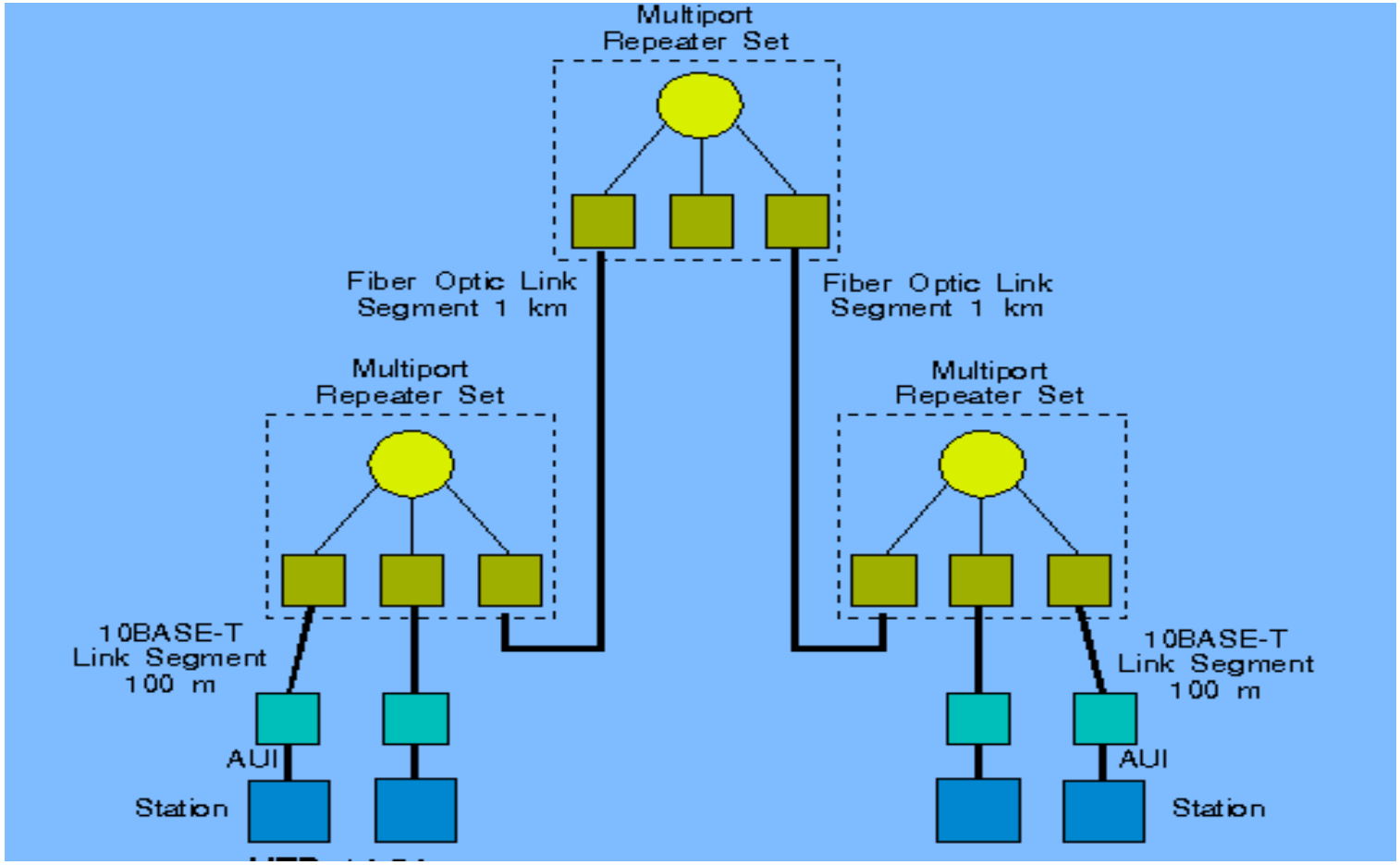
3.2.3.1 Ethernet-Varianten für 10 Mbit/s (17)

- **10BaseT**
  - Der »Bus« konzentriert sich bei dieser 802.3-Version in einem Hub
  - Alle Stationen sind mit diesem Hub sternförmig über Vierdraht-Leitungen verbunden; es werden zwei Adernpaare des TP-Kabels verwendet: Receive und Transmit
  - Die max. Entfernung zwischen zwei MAUs ohne Zwischenverstärker wurde auf 100 m festgelegt, wobei der Hub ebenfalls eine Ansammlung von MAUs darstellt, die über den internen Bus des Hubs zusammengeschaltet werden
  - In diesen 100 m sind allerdings Wandsteckdosen und Rangierverteiler sowie die Entfernungen, z.B. zwischen Endgeräten und Steckdosen, inbegriffen

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (18)

❑ 10BaseT

- Beispiel einer Konfiguration



3.2.3.1 Ethernet-Varianten für 10 Mbit/s (19)

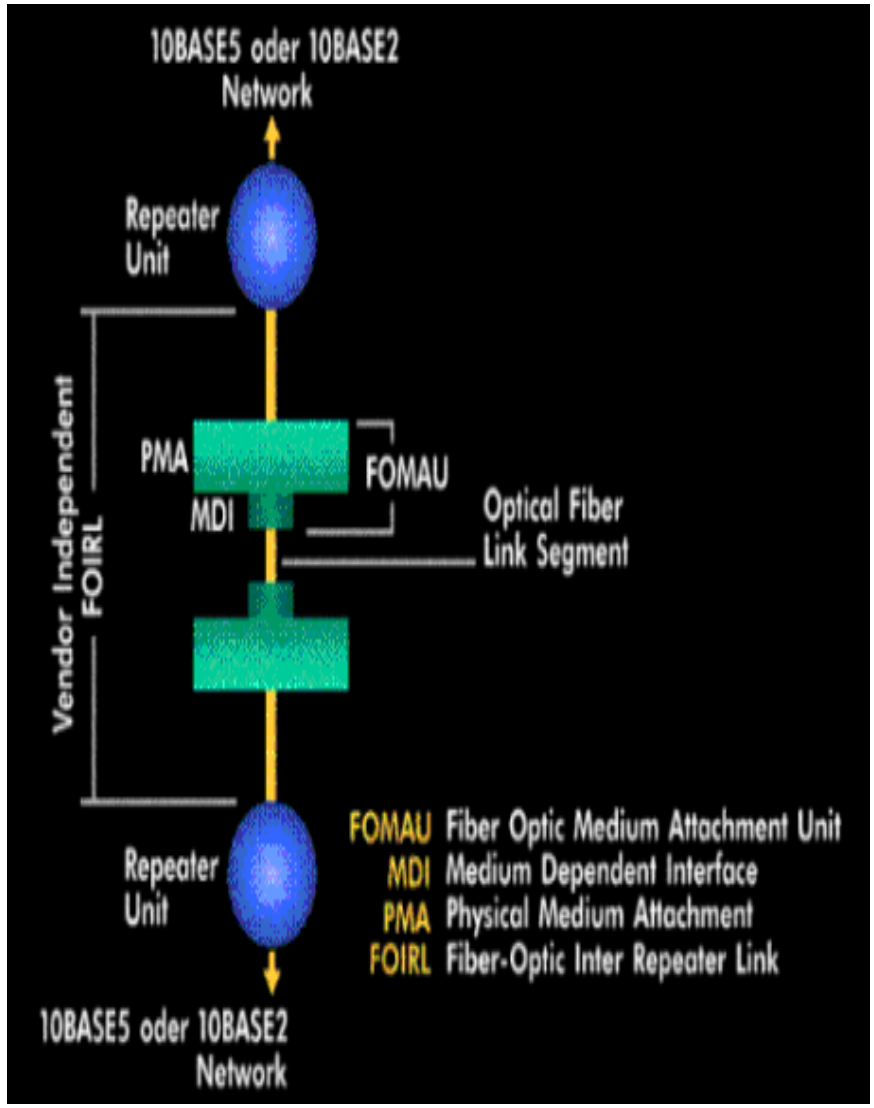
- **10BaseF**
  - IEEE hat in der Arbeitsgruppe 802.8a das Thema Fiber Optic Media standardisiert und dabei fünf Alternativen behandelt: Aktive Ringe, passive und aktive Sternkoppler mit jeweils synchroner oder asynchroner Übertragung
  - Hub ist ein optischer Sternkoppler; der passive Sternkoppler unterscheidet sich vom aktiven unter anderem dadurch, dass Übertragungsmedium und Sternkoppler vollständig passiv sind, keine Abstrahlung und keine Stromversorgung haben
  - Die Entfernung zwischen FOMAU und Sternkoppler kann bis zu 500m betragen, eine Unterstützung von 1024 Ethernet-Knoten in einem Netz ist möglich
  - 10 BaseF-LANs gestatten, 10 BaseT und 10 Base2 und 10 Base5 zu einem Gesamt-LAN zu verbinden
  - Eingesetzt werden Gradientenfasern 50/125 Mikrometer und 62,5/125 Mikrometer

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (20)

- **10BaseF (Fortsetzung)**
  - Eigenschaften
    - Bei 10Base-FB können bis zu 15 Repeater kaskadiert werden; jedes Segment kann max. 2 km lang sein; ist ausschließlich für Backbone-Anwendungen festgelegt. 10BaseF beschreibt alle Funktionen zur Datenübertragung zwischen aktiven Sternkopplern
    - Die andere Variante 10Base-FL ist eine Erweiterung des FOIRL(FiberOpticInterRepeaterLink)-Standards auf 2 km;
      Diese Variante hat maximal fünf Repeater für eine dreistufige Netzhierarchie und ist abwärtskompatibel mit FOIRL-Komponenten;
      10Base-FL beschreibt alle Funktionen zur Datenübertragung von einer MAU zu einem aktiven Sternkoppler und Verbindungen zwischen Sternkopplern

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (21)

- **10BaseF (Fortsetzung)**
  - Eigenschaften
    - Das optische Link-Segment zwischen den beiden Hälften eines Remote-Repeaters ist im **FOIRL (Fiber Optic Inter Repeater Link)** standardisiert
    - Das FOIRL-Interface arbeitet mit einer typischen Wellenlänge von 850 nm über Lichtwellenleiter in Duplex
    - Der Standard sieht Gradientenfasern mit 50/125 µm, 62,5/125 µm, 85/125 µm und 100/140 µm vor

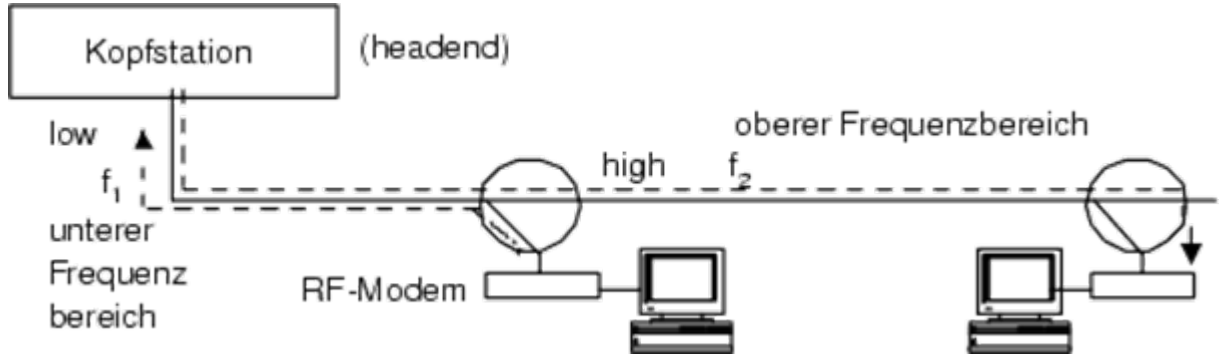


3.2.3.1 Ethernet-Varianten für 10 Mbit/s (22)

- **Breitband Koaxialkabel: 10Broad36**
  - Analoge Übertragung mit Aufteilung der Gesamtbandbreite in Frequenzbereiche
    - Zuteilung an Kanäle
    - FDM ("Frequency Division Multiplexing")
  - Kabelfernsehen: unidirektionale Verbindung
    - für Datenkommunikation jedoch bidirektionale Verbindung notwendig
  - Die Topologie ist ein unregelmäßiger Baum, dessen Wurzel die Head-End-Station ist; verwendet wird ein 75-Ohm-Breitband Koaxialkabel
  - Unterschiedliche Frequenzbereiche für Sender und Empfänger

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (23)

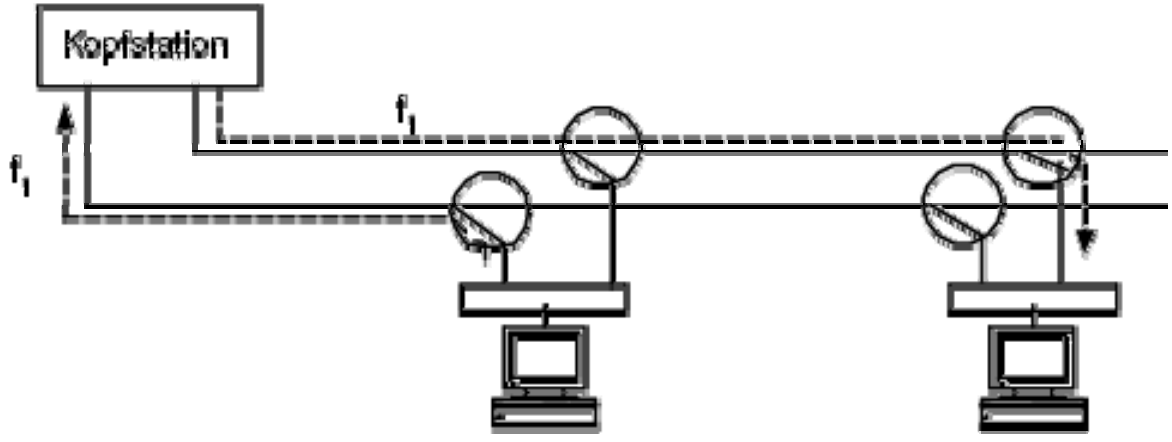
- **Breitband Koaxialkabel: 10Broad36**
  - Einkabel-Systeme



  - Headend dient sowohl als Verstärker als auch Umsetzter der Sende- und Empfangssignale; Unterscheidung zwischen Rückwärtskanälen (Sendern) und Vorwärtskanälen (Empfängern)
  - Vorwärtskanäle im unteren Frequenzbereich; Vorwärtskanäle im oberen Frequenzbereich

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (24)

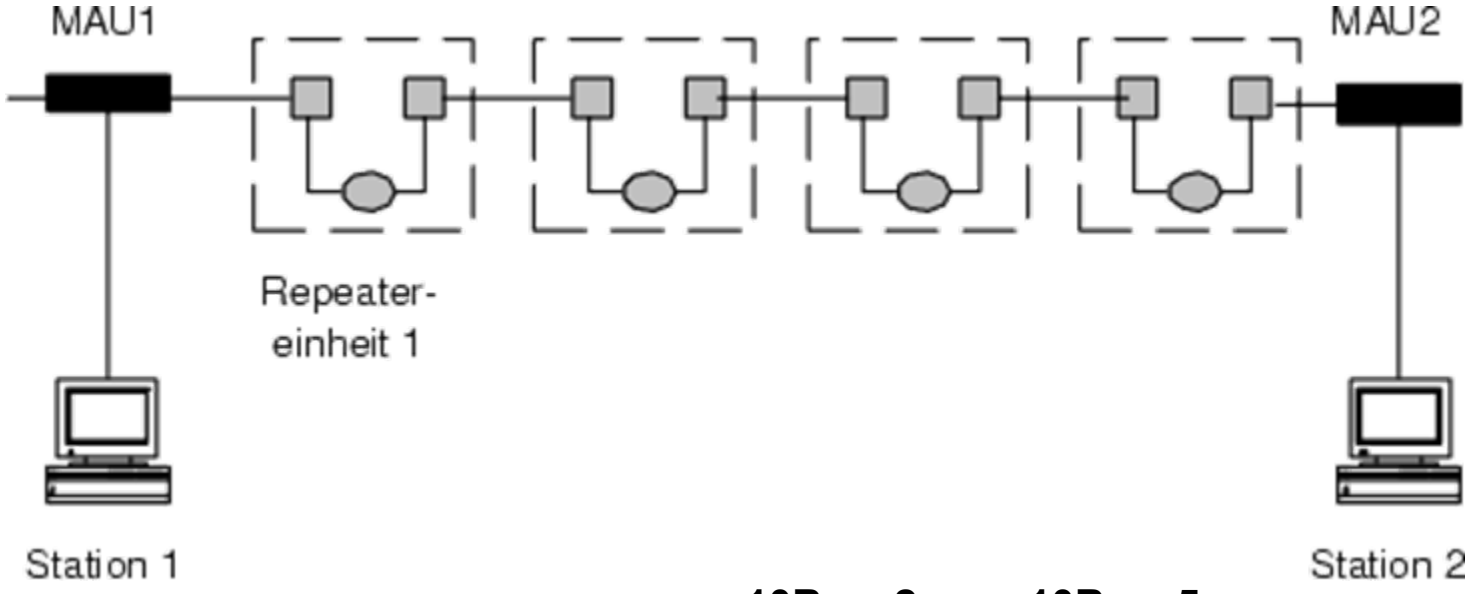
- **Breitband Koaxialkabel: 10Broad36**
  - Duales Kabel
    - getrennte Kabel für Senden und Empfangen



- Einsatz von Breitband im Produktionsbereich; leichte Integration von verschiedenen Diensten zur Realisierung einer Duplex-Verbindung zwischen 2 DTE; auf der Datenebene sind 2 getrennte Kanäle notwendig

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (25)

❑ Designregeln für 10Base2 und 10Base5



	10Base2	10Base5
Maximale Stationenzahl pro Segment	30	100
Maximale Repeaterzahl	4	4
Minimale Segmentlänge (minimaler Stationsabstand)	0,5 m	2,5 m
Maximale Segmentlänge	185 m	500 m
Minimaler Biegeradius	5 cm	25 cm
Maximale Dämpfung pro Segment	8,5 dB	8,5 dB
Maximale Übertragungsverzögerung pro Segment	950 ns	2165 ns

3.2.3.1 Ethernet-Varianten für 10 Mbit/s (26)

❑ Designregeln für 10BaseT/FB/FL und FOIRL

10Base-T Parameter	Grenzwerte
Maximale Segmentlänge	100 m
Maximale Dämpfung (10 MHz)	< 11,5 dB
Störspannung (40 Hz – 150 Hz)	< 50 mV
Störspannung (150 Hz – 16 MHz)	< 50 mV
Störspannung (16 MHz – 100 MHz)	< 300 mV
Maximale Übertragungsverzögerung pro Segment	1000 ns

	Maximale Segmentlänge	Maximale Dämpfung	Ausbreitungs-geschwind.	Maximale Übertragungsver.
FOIRL	1 km	9 dB	0,66 c	5000 ns
10Base-FB	2 km	12,5 dB	0,66 c	1000 ns
10Base-FL	2 km	12,5 dB	0,66 c	1000 ns

Max.-Konfiguration:

max. Weg zwischen 2 Stationen ⇒ 5 Segmente mit 4 Repeater

Von den 5 Segmenten können maximal 3 Koax-Segmente sein, die anderen sind dann Linksegmente (auf Basis von FOIRL) ⇒ max Weg 2500 m, min. Weg 2,5 m

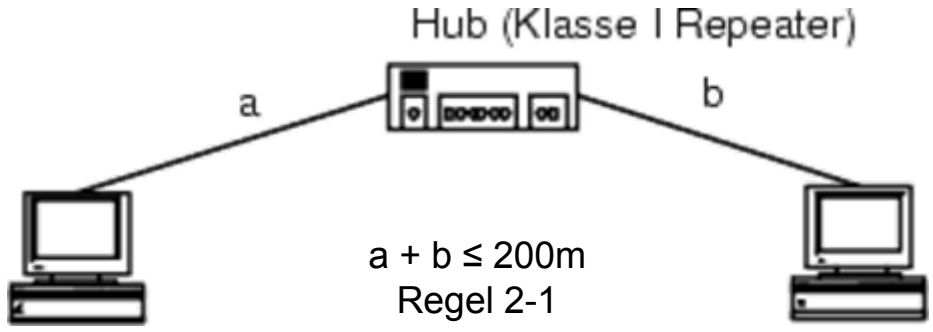
Konfliktparameter K ist gleich 0.21

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (1)

- **Ausbreitungsgeschwindigkeit in 10BaseT und 100BaseT gleich**
  - Weil höhere Rate, folgt aus Kollisionsparameter kleinere Entfernung
  - Entscheidung: CSMA/CD unverändert, Frame unverändert
- **Übertragungsmedien**
  - 4 Paar UTP, 100BaseT,
  - 2 Paar UTP/STP: 100Base TX,
  - Glasfaser: 100BaseFX
- **100BaseT-LANs: Topologie nur Stern**
  - 100BaseT4: 4 Adernpaare UTP mindestens der Kategorie 3 mit 8B/6T-Codierung
  - 100BaseTX: 2 Adernpaare UTP bzw. STP der Kategorie 5; zur Übertragung werden 2 Adernpaare benötigt, 4B/5B-Codierung
  - 100BaseFX: Gradientenfaser 62.5/125 Mikrometer
- **Klasse I-Repeater (Hub): unterstützen unterschiedliche Übertragungsmedien**
- **Klasse II-Repeater: unterstützen nur das gleiche Übertragungsmedium**

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (2)

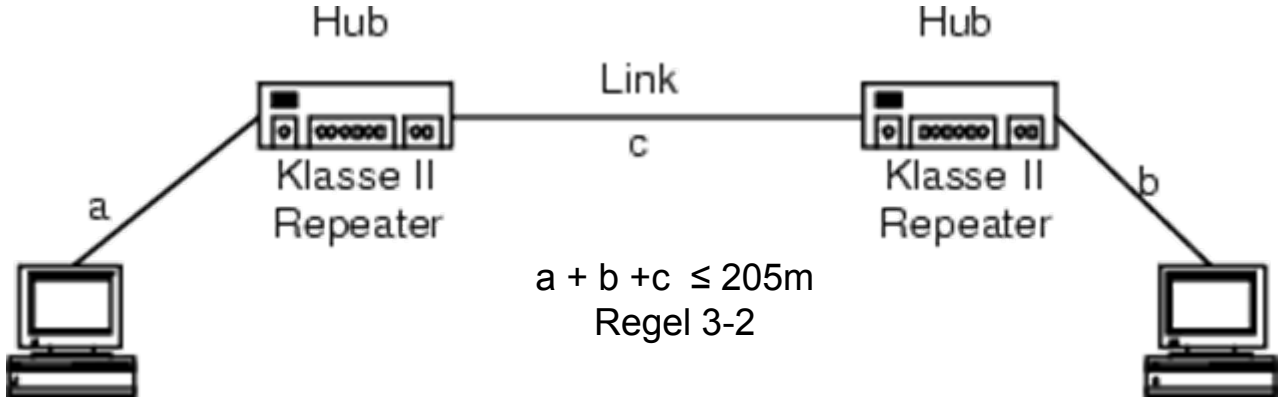
- **Repeater-Regeln**
  - Klasse-I Repeater (Hub)



  - Regel 2-1
    - Ein Pfad zwischen 2 DTEs darf sich maximal aus 2 Linksegmenten und einem Klasse-I Repeater zusammensetzen. Kollisionsdomäne besteht hier aus einem Hub

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (3)

- **Repeater-Regeln**
  - Regel 3-2:
    - Ein Pfad darf maximal aus 3 Linksegmenten und 2 Klasse-II-Repeatern bestehen
    - Kollisionsdomäne darf maximal aus 2 Klasse-II-Repeatern beziehen



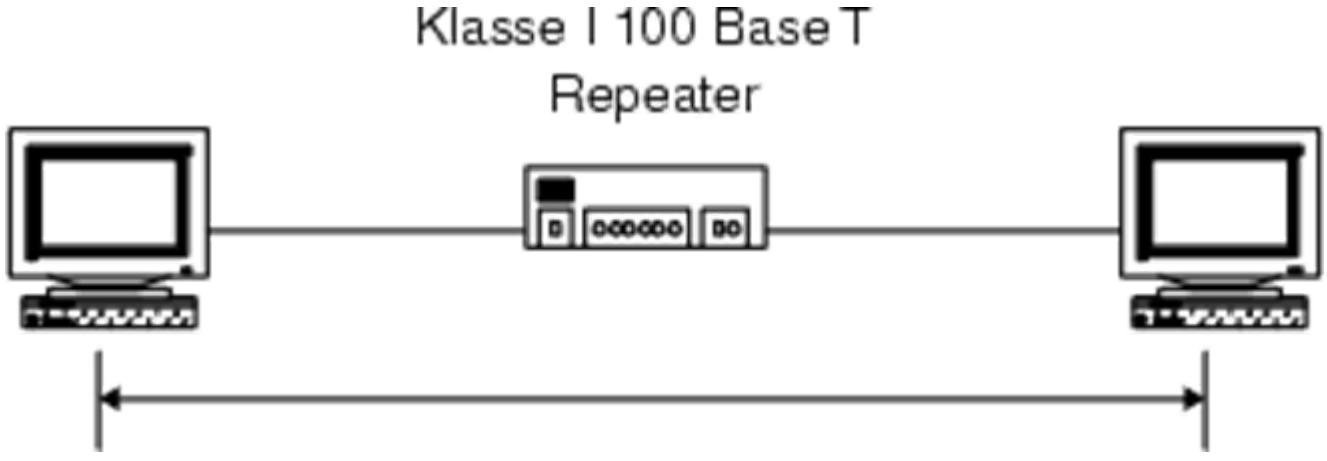
    - Mehrere Kollisionsdomänen können über Fast Ethernet Switches zu einem größeren Fast Ethernet LAN verbunden werden
    - Viele Inteface-Karten verfügen heute über Autonegotiation 10/100 Mbps, dadurch leichte Migration

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (4)

- **Kopplung von 100BaseT-Stationen**
  - Direkte Kopplung von 100BaseT-Stationen
    - Stationen arbeiten im Full-Duplex-Betrieb
    - Maximale Entfernung zwischen zwei Stationen:
      - Twisted Pair: 100 m
      - Glasfaser: 400 m

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (5)

- **Kopplung mit Klasse-I Repeater**
  - Verwendung unterschiedlicher Medien zwischen Hub und Stationen
  - Maximale Entfernung zwischen zwei Stationen:
    - Twisted Pair: 200 m
    - Glasfaser: 240 m



- Ein Repeater ist eine aktive Komponente, die Regenerierungsfunktionen in Ethernet-LANs übernimmt und auf der Bitübertragungsschicht arbeitet
- Repeater regeneriert den Signalverlauf sowie Pegel und Takt

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (6)

- **Kopplung mit Klasse-II Repeater**
  - Maximale Entfernung zwischen zwei Stationen mit einem Klasse II Repeater:
    - Twisted Pair: 200 m
    - Glasfaser: 318 m
  - Maximale Entfernung zwischen zwei Stationen mit zwei Klasse II Repeater:
    - Twisted Pair: 205 m
    - Glasfaser: 226 m

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (7)

❑ Verzögerungskomponenten in 100BaseT

Netztopologie	Verzögerung in Bit-Zeiten/Meter	Max Verzögerungszeit in Bit-Zeiten
Zwei Netzknoten	-	100
UTP Cat 3	0,57	114
UTP Cat 4	0,57	114
UTP Cat 5	0,556	111,2
STP	0,556	111,2
Glasfaser	0,501	408
Klasse-1-Repeater	-	168
Klasse-2-Repeater	-	92

3.2.3.2 Ethernet-Varianten für 100 Mbit/s (IEEE 802.3n) (8)

❑ Autonegotiation-Protokoll

- Die 100BaseT-Komponenten sind in der Lage, vor der ersten Übertragung die Übertragungsmethode zu vereinbaren
  - Mit dem Autonegotiation-Verfahren, früher als NWay bezeichnet, können Repeater oder Endgeräte feststellen, über welche Funktionalität die Gegenseite verfügt, so dass ein automatisches Konfigurieren unterschiedlicher Geräte möglich ist
  - Varianten: 10/100 Mbps, vollduplex / halbduplex
- Hierarchie für die Aushandlung
  - 100BaseTX Fullduplex
  - 100BaseT4
  - 100BaseTX
  - 100Base T Fullduplex
  - 10BaseT Halfduplex

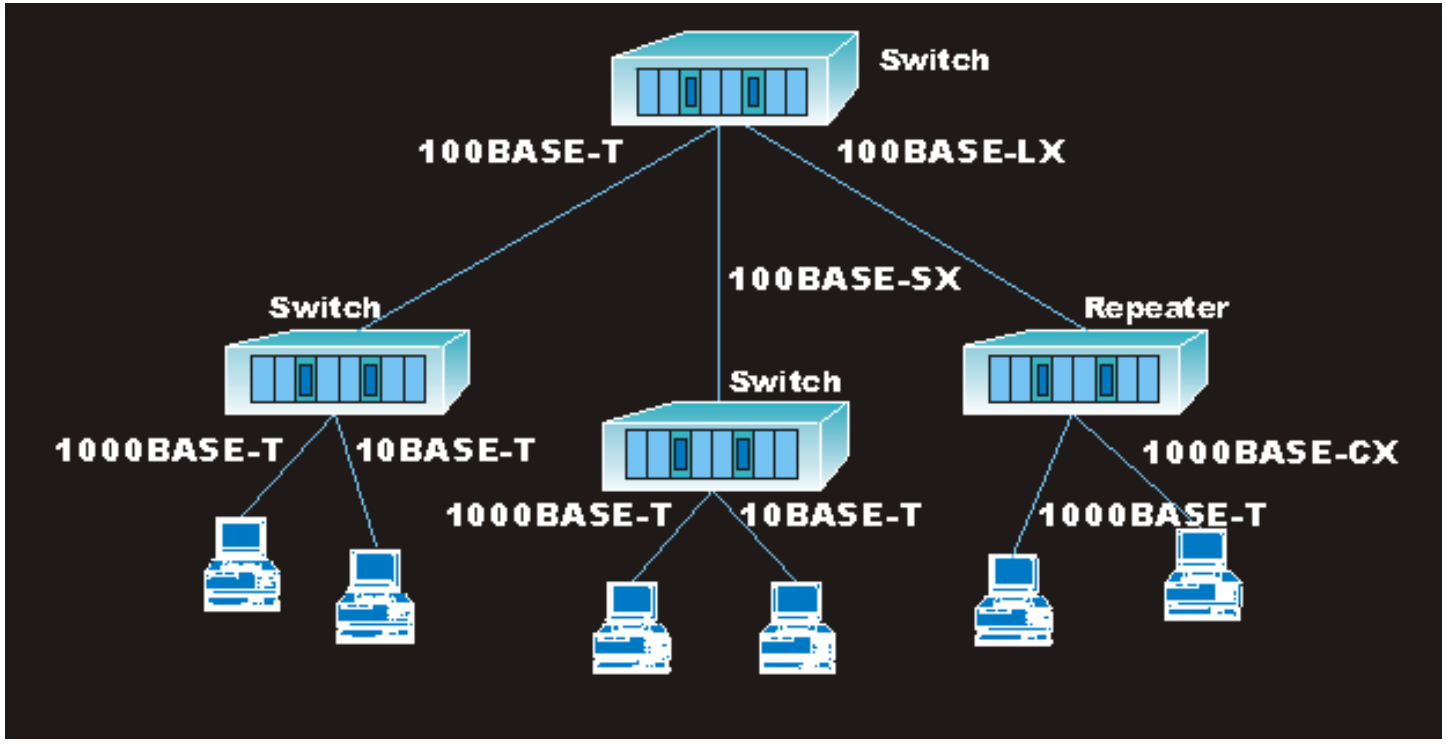
  T, TX und T4 unterscheiden sich in der Codierung; T verwendet Manchester Codierung, während T4 den Code 8B/6T und TX den Code 4B/5B verwendet

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (1)

- Standard für Ethernet Verfahren mit 1000 Mb/s; verabschiedet im Jahre 1998
  - Evolution von Standard Ethernet mit 10 Mb/s zu einem Hochgeschwindigkeitsnetz
  - Migration von Standard-Ethernet mit Übergang
    - Vom gemeinsamen Koaxialkabel zum dedizierten Übertragungsmedium (optisch oder Twisted Pair)
    - Von gemeinsamer Bandbreite zur dedizierten Übertragungs-Bandbreite
    - Von Halbduplex zu Vollduplex
- Übertragungsrate von 1 Gbit/s u.a. interessant für LAN-Backbones

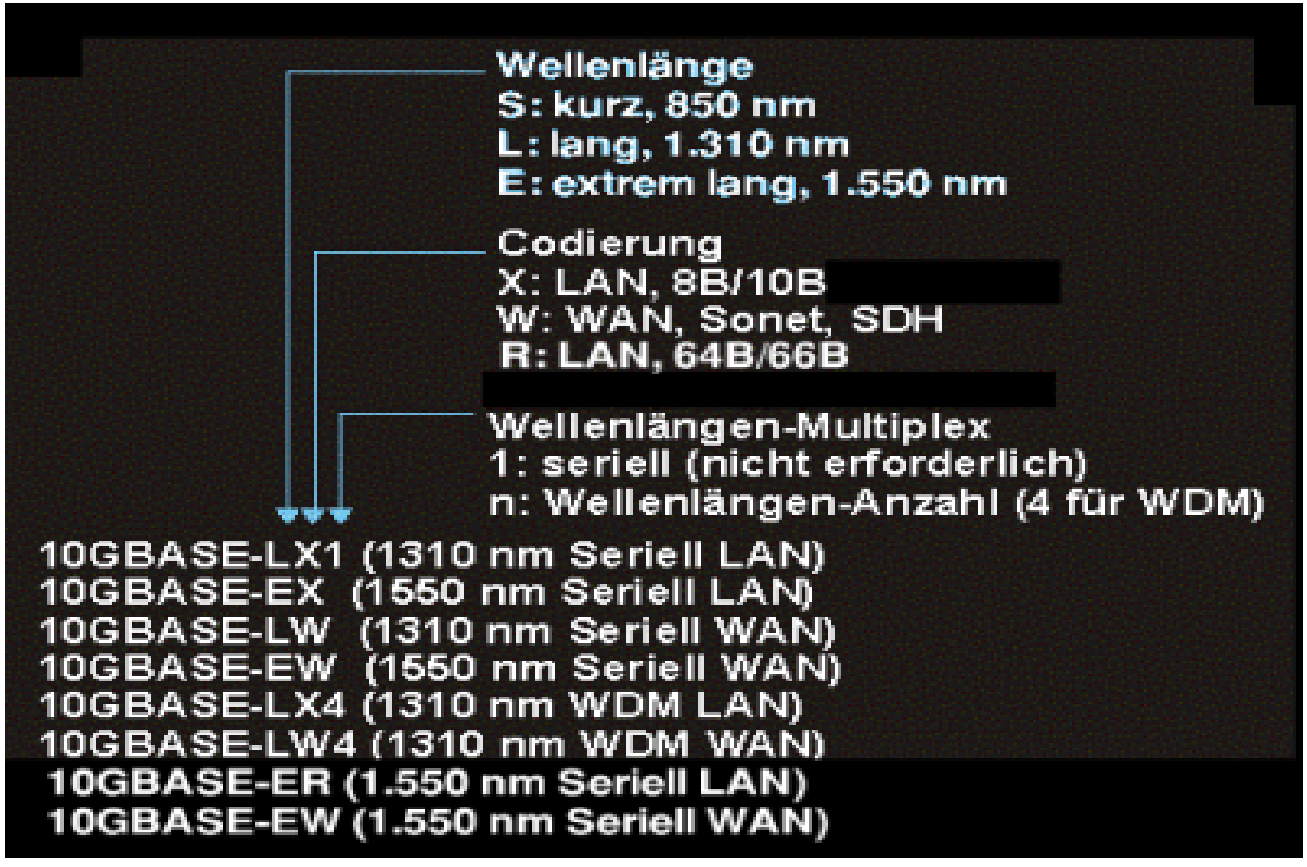
3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (2)

- Konfiguration



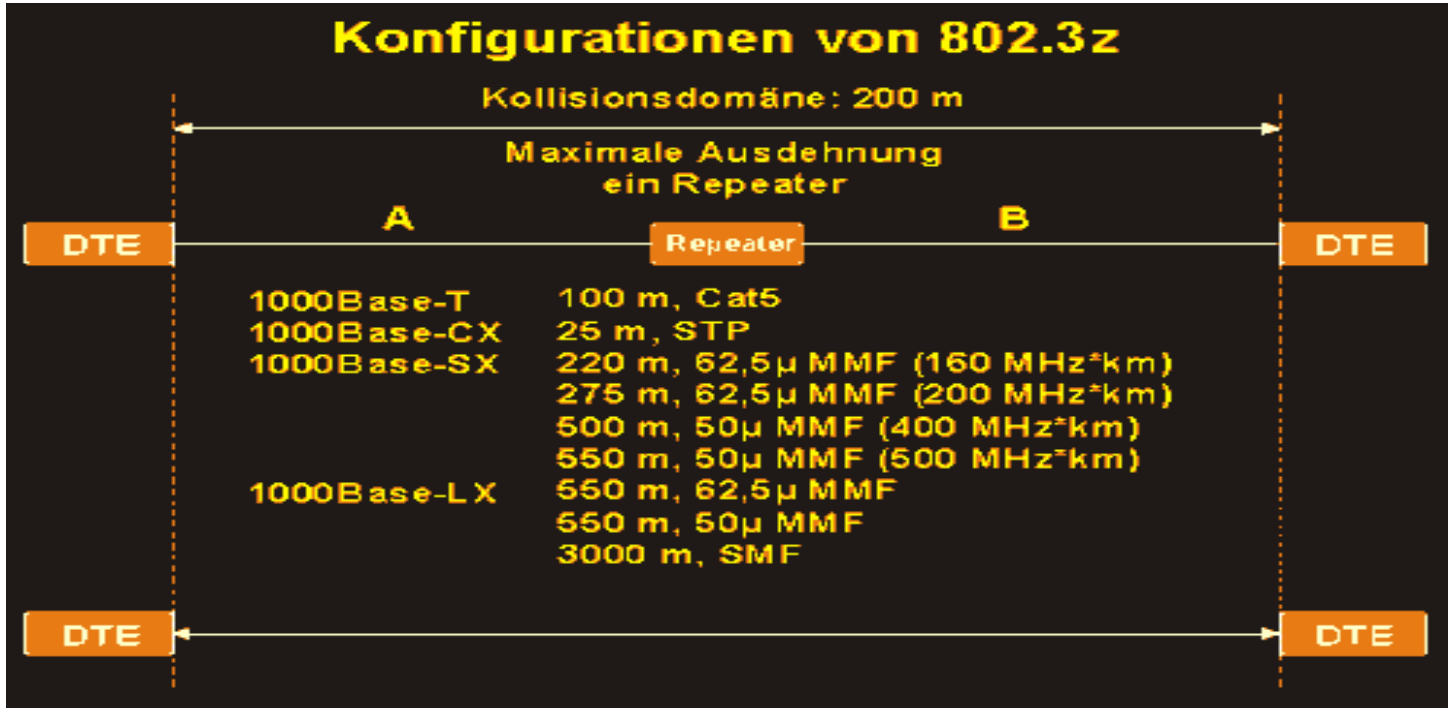
3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (3)

- **Der Normentwurf für die Gigabit-Ethernet-Architektur definiert einerseits Änderungen am existierenden CSMA/CD-Verfahren, andererseits umfasst der Basisstandard neben dem MAC-Layer vier unterschiedliche physikalische Technologien:**
  - 1000Base-LX
  - 1000Base-SX
  - 1000Base-CX
  - 1000Base-T



3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (4)

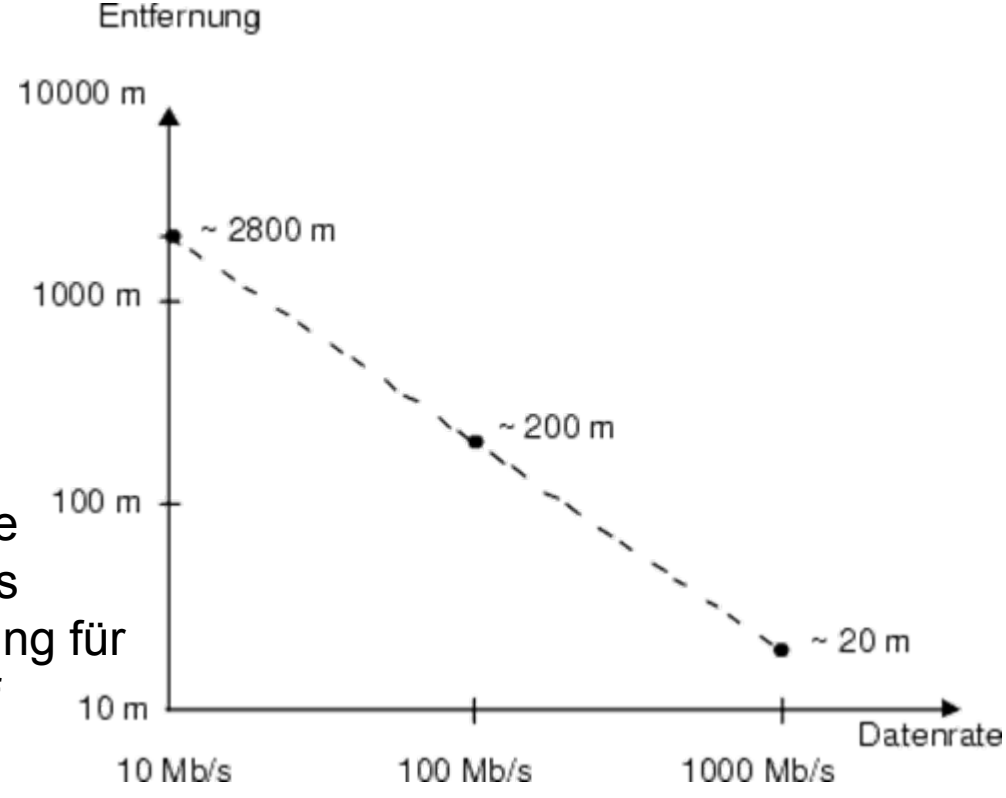
- Gigabit-Ethernet bietet sowohl einen Vollduplexmodus für Punkt-zu-Punkt-Verbindungen als auch einen Halbduplexmodus
- Der Vollduplexmodus wird mittels Monomodefasern oder Fiber-Channel mit Multimodefasern realisiert, wobei Entfernungen von 200 m bis 2 km überbrückt werden können
- Bei Halbduplex-Betrieb wird als Basistechnologie mit Fiber-Channel gearbeitet



3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (5)

❑ Halbduplex MAC-Verfahren

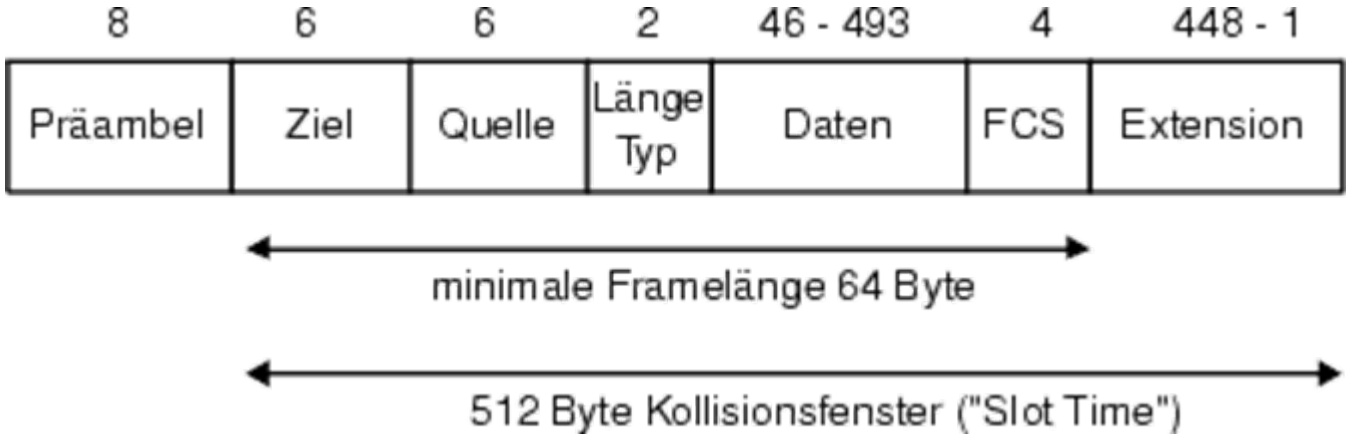
- Bei Halbduplex steht Empfangsleitung während des Sendens für Kollisionserkennung zur Verfügung.
  - CSMA/CD erfordert eine minimale Framelänge (512 bits), damit Kollisionen auch bei maximaler LAN-Ausdehnung erkannt werden können
- Netzausdehnung
  - Erhöhung der Datenrate führt zu einer Reduzierung der Netzausdehnung, falls minimale Framelänge beibehalten werden soll
  - unveränderte Übernahme des CSMA/CD-Standards würde die Netzausdehnung für Datenrate 1000 Mb/s auf ca. 20 m reduzieren



3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (6)

❑ Halbduplex MAC-Verfahren

- Carrier-Extension
  - Modifikation des CSMA/CD-Verfahrens durch Erhöhung der Minimallänge bei der *Übertragung* ; die Maximallänge der Frames bleibt unverändert
  - Falls Frame zwischen 64-511 Bytes lang, werden am Ende zusätzlich 448-1 Byte angehängt



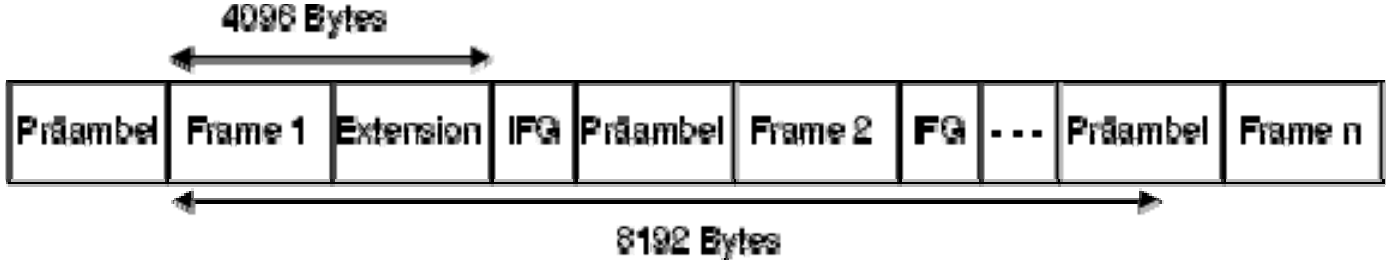
3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (7)

- **Halbduplex MAC-Verfahren**
  - Carrier-Extension
    - Extension beinhaltet Symbole, die von der Bitübertragungsschicht festgelegt werden; sie werden von empfangender Station nicht interpretiert
  - Falls Frame ≥ 512 Byte, keine Änderung
  - Damit wird Kollisionsfenster auf 4096 bits erweitert; Ausdehnung des Netzes um das 8-fache
  - Das Extension-Feld wird vom FCS nicht berücksichtigt

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (8)

❑ Halbduplex MAC-Verfahren

- Frame Bursting
  - Eine Station kann mehrere Frames zusammenfassen und in einem Schwung senden



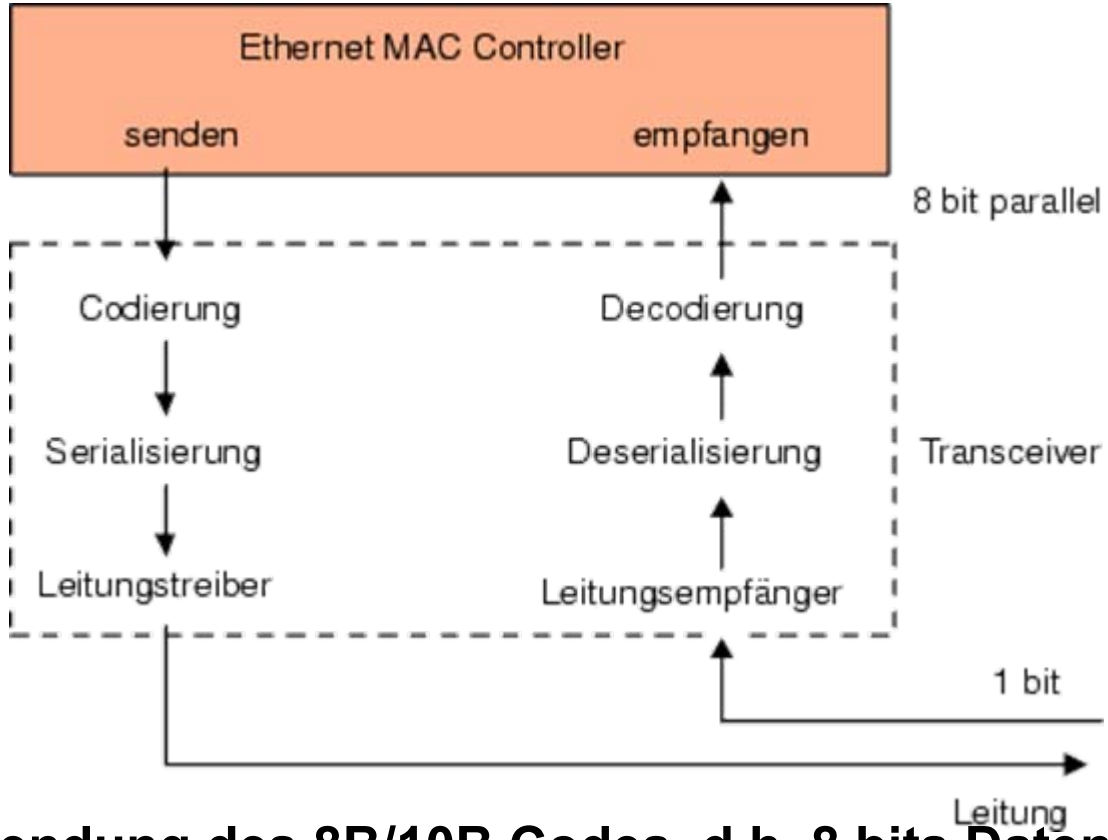
  - Bis zum Start des letzten zu übertragenden Frames sind maximal 8192 Bytes vergangen (einschließlich InterFrame Gap IFG)

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (9)

- **Vollduplex-MAC-Verfahren**
  - Weil kein MA, deshalb auch kein Konflikt möglich, also kein CS oder CD
    - Konfliktauflösung verlagert sich in Hub
    - Simultanes Senden und Empfangen von Frames
    - im Vollduplex-Betrieb gibt es kein Kollisionsfenster, Extension-Feld, Backoff-Algorithmus
    - maximale Framelänge (1518 Bytes) und IFG bleiben unverändert
  - Flusskontrolle
    - Bei Halbduplex liegt *implizite* Flusssteuerung durch Kollision und Backoff vor; bei Vollduplex, d.h. Baumstruktur, entweder Back Pressure oder explizite Flusssteuerung
      - Pufferüberlauf bei der empfangenden Station oder beim Switch
        - Senden des MAC-Kontrollframes Pause an Sender von Frames
        - Sender unterbricht Übertragung von Frames nach Beendigung des aktuellen Frames
      - Beendigung der Pufferprobleme
        - Senden eines Cancel-Pause Kontrollframes

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (10)

- **Bitübertragungsschicht**



- **Verwendung des 8B/10B Codes, d.h. 8 bits Daten werden für Übertragung auf 10 bit abgebildet; Anstelle von Manchester Codierung verwendet Gigabit Ethernet NRZ Übertragungscodierung**

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (11)

- **1000Base-SX**
  - Diese Gigabit-Ethernet-Variante arbeitet mit einem Laser mit kurzer Wellenlänge, deswegen auch der Buchstabe S, der für Short Wavelength steht
  - Mit der 850-nm-Quelle werden je nach Glasfaserdurchmesser der Multimodefasern in der Praxis Entfernungen von 270 m (62,5 µm) bzw. 550 m (50 µm) erreicht
  - Bei diesen Entfernungen ist zu berücksichtigen, dass es sich um eine Punkt-zu-Punkt-Verbindung im Full-Duplex handelt, also ohne CSMA/CD
  - Die Baudrate ist wie bei der 1000LX-Version 1,25 Gbaud
  - Dämpfungsbudget beträgt 7,0 dB
  - 1000Base-SX verwendet als Stecker den Duplex-SC-Stecker

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (12)

- **1000Base-LX**
  - 1000Base-LX ist eine Variante von Gigabit-Ethernet, die mit Glasfaser arbeitet. Dabei steht der Buchstabe L für Long Wavelength.
  - Bei dieser Variante kommt ein Laser mit einer Wellenlänge von 1300 nm, spezifiziert sind 1270 nm bis 1355 nm, zum Einsatz.
  - 1000Base-LX kann mit Multimodefasern und mit Monomodefasern arbeiten
    - Die Reichweiten unterscheiden sich dabei allerdings beträchtlich: Mit Multimodefasern von 62,5 µm und 50 µm wird eine Entfernung von 550 m überbrückt und mit einer Monomodefaser 3 km.
  - Dabei ist zu berücksichtigen, dass es sich um Punkt-zu-Punkt-Verbindungen in Full-Duplex handelt, also ohne CSMA/CD

3.2.3.3 Ethernet-Varianten für Gigabit-Ethernet (IEEE 802.3z) (13)

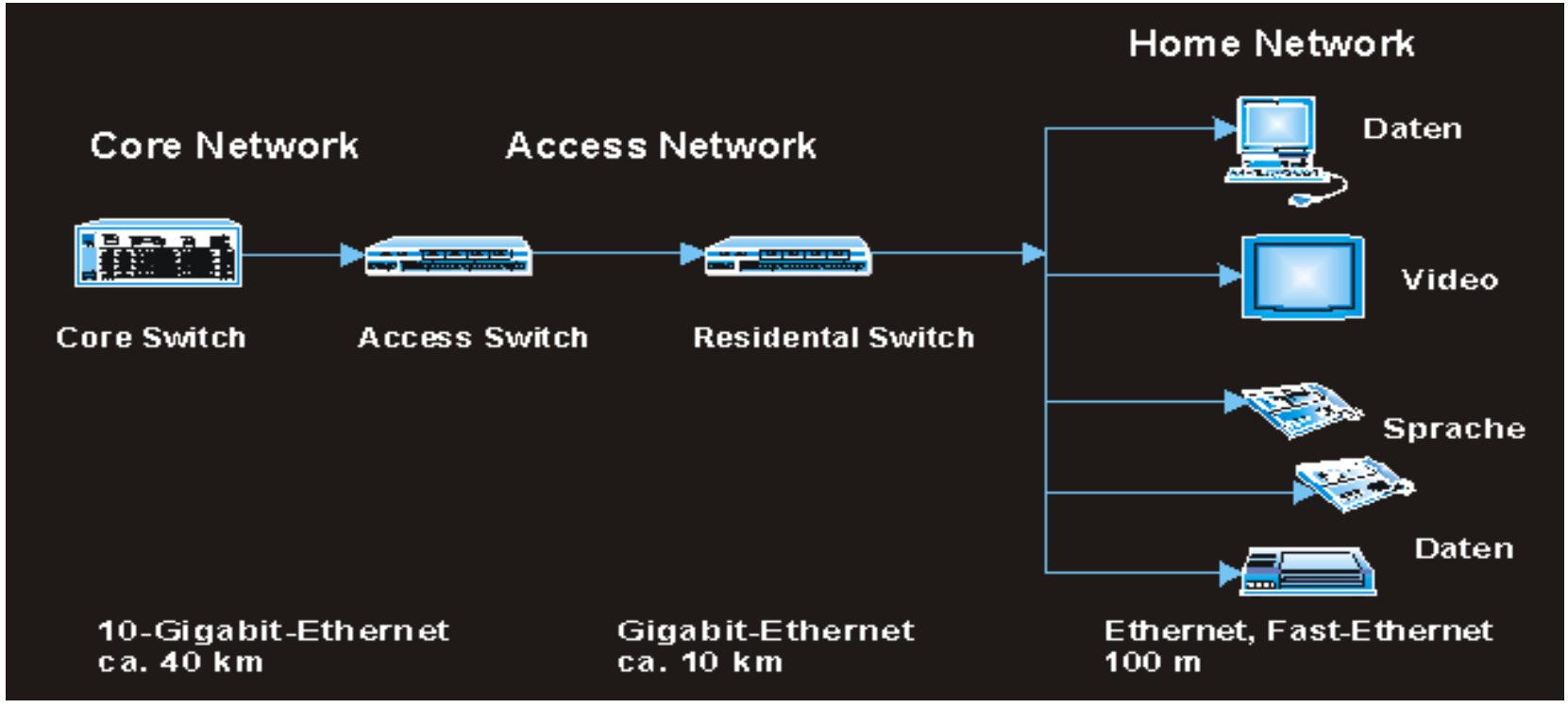
- **1000Base-CX**
  - Die CX-Variante ist für Gigabit-Ethernet über STP-Kabel mit 150 Ohm standardisiert
  - Die 1000Base-CX-Variante eignet sich für Endgeräte-Anschlüsse mit einer Entfernung von 25 Meter über STP-Kabel
- **1000Base-T**
  - Die Arbeitsgruppe IEEE 802.3ab 1000Base-T beschäftigt sich mit der Standardisierung der Gigabit-Ethernet-Technologie über Kabel der Kategorie 5 für die Arbeitsplatzverkabelung mit bis zu 100 m Länge
  - Der Basisstandard dieser Technologie umfasst den MAC-Layer, der bis auf die höhere Geschwindigkeit gegenüber dem klassischen 10-Mbit/s-Ethernet und dem Fast-Ethernet unverändert bleibt
  - Die Basisprinzipien von 1000Base-T wurden der 100Base-T2-Technik entnommen; das bedeutet, dass man mit vier Adernpaaren arbeitet. Um 1 Gbit/s vollduplex übertragen zu können, muss jedes Adernpaar in jede Richtung 250 Mbit/s übertragen
  - Die Übertragung auf den Leiterpaaren erfolgt mittels einer fünfstufigen Pulsamplitudenmodulation (PAM5).

3.2.3.4 Ethernet-Varianten für 10-Gigabit-Ethernet (IEEE 802.3ae)

- **Eigenschaften**
  - Beibehaltung des 802.3- und Ethernet-Frame-Formats und der bestehenden minimalen und maximalen Frame-Länge
  - Die Einhaltung der IEEE 802 Functional Requirements mit Ausnahme des Hamming-Abstandes
  - Die Unterstützung von Sternstrukturen mit Punkt-zu-Punkt-Verbindungen und lediglich ein Vollduplex-Modus nach IEEE 802.3x
  - Der im 10-Gigabit-Ethernet benutzte Vollduplex-Modus bedeutet den Abschied vom CSMA/CD-Zugangsverfahren und damit vom klassischen Ethernet
  - Gigabit-Ethernet war also die letzte Ethernet-Technologie, auch wenn 10-Gigabit-Ethernet noch diesen Namen trägt

3.2.3.4 Ethernet-Varianten für 10-Gigabit-Ethernet (IEEE 802.3ae)

- **Punkt-zu-Punkt-Verbindung mit 10-Gigabit-Ethernet**

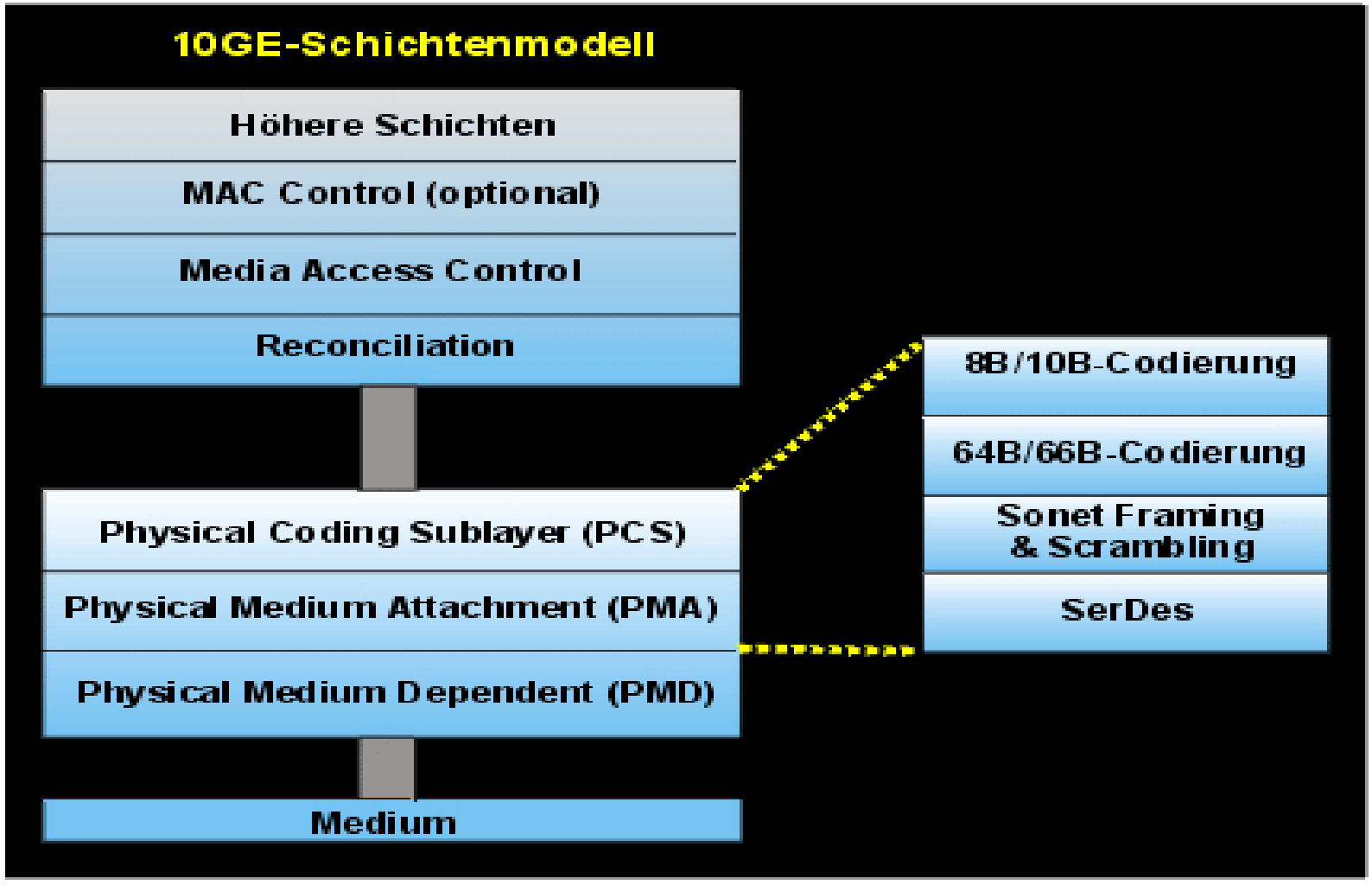


3.2.3.4 Ethernet-Varianten für 10-Gigabit-Ethernet (IEEE 802.3ae)

- **10-Gigabit Medium Independent Interface (XGMII)**
  - XGMII ist das Interface zwischen dem MAC-Layer und dem Physical Layer bei 10-Gigabit-Ethernet
  - XGMII kann eine maximale physische Länge von nur 7 cm überbrücken. Eine Verlängerung erfolgt über das XAUI (10 Gigabit attachment unit interface)
- **10-Gigabit Schichtenmodell**
  - Für das Schichtenmodell von 10GE wurden im Unterschied zu Gigabit-Ethernet einige neue Schichten und Schnittstellen definiert

3.2.3.4 Ethernet-Varianten für 10-Gigabit-Ethernet (IEEE 802.3ae)

- 10-GE-Schichtenmodell



3.2.3.4 Ethernet-Varianten für 10-Gigabit-Ethernet (IEEE 802.3ae)

- **10-GE-Schichtenmodell**
  - Als Schnittstelle zwischen dem MAC-Layer und Physical Coding Sublayer (PCS) oder XGMII Extender Sublayer (XGXS) dient XGMII
  - Für die Codierung der Daten ist die PCS-Schicht zuständig
  - Als Codierverfahren für WAN-Anwendungen wurde eine effiziente Block-Codierung ausgewählt, die 64B/66B-Codierung, die nur zwei zusätzliche Bits für einen 64-Bit-Datenblock benötigt
  - Neben dieser neuen Codiertechnik kommt bei LAN-Anwendungen die 8B/10B-Codierung zur Anwendung

3.2.3.4 Ethernet-Varianten für 10-Gigabit-Ethernet (IEEE 802.3ae)

- 10-GE-Interfaces

Version	Klasse	Fenster	Codierung	Typ
10GBASE-SR	10GBASE-R	850 nm	64b/66b	seriell
10GBASE-SW	10GBASE-W	850 nm	64b/66b	SONET/SDH
10GBASE-LX4	10GBASE-X	1310 nm	8b/10b	DWDM
10GBASE-LW4	10GBASE-W	1310 nm	64b/66b	SONET/SDH
10GBASE-LR	10GBASE-R	1310 nm	64b/66b	seriell
10GBASE-LW	10GBASE-W	1310 nm	64b/66b	SONET/SDH
10GBASE-ER	10GBASE-R	1550 nm	64b/66b	seriell
10GBASE-EW	10GBASE-W	1550 nm	64b/66b	SONET/SDH

3.3 Drahtlose LANs

- **3.3.1 IEEE-Standard 802.11**
  - Topologien
  - Schichten und Funktionen
  - Dienste
  - Roaming
  - IEEE-802.11-Standards
- **3.3.2 ETSI Hyperlan**
- **3.3.3 Komponenten**

3.3 Charakteristika drahtloser LANs

- **Vorteile**
  - räumlich flexibel innerhalb eines Empfangsbereichs
  - Ad-hoc-Netze ohne vorherige Planung machbar
  - keine Verkabelungsprobleme (z.B. historische Gebäude, Feuerschutz, Ästhetik)
  - unanfälliger gegenüber Katastrophen wie Erdbeben, Feuer - und auch unachtsamen Benutzern, die Stecker ziehen!
- **Nachteile**
  - im Allgemeinen sehr niedrige Übertragungsraten im Vergleich zu Festnetzen (1-10 Mbit/s) bei größerer Nutzerzahl
  - Proprietäre leistungsstärkere Lösungen, Standards wie IEEE 802.11 sind weniger leistungsfähig und brauchen ihre Zeit
  - müssen viele nationale Restriktionen beachten, wenn sie mit Funk arbeiten, globale Regelungen werden erst langsam geschaffen (z.B. bietet Europa mehr Kanäle als die USA)

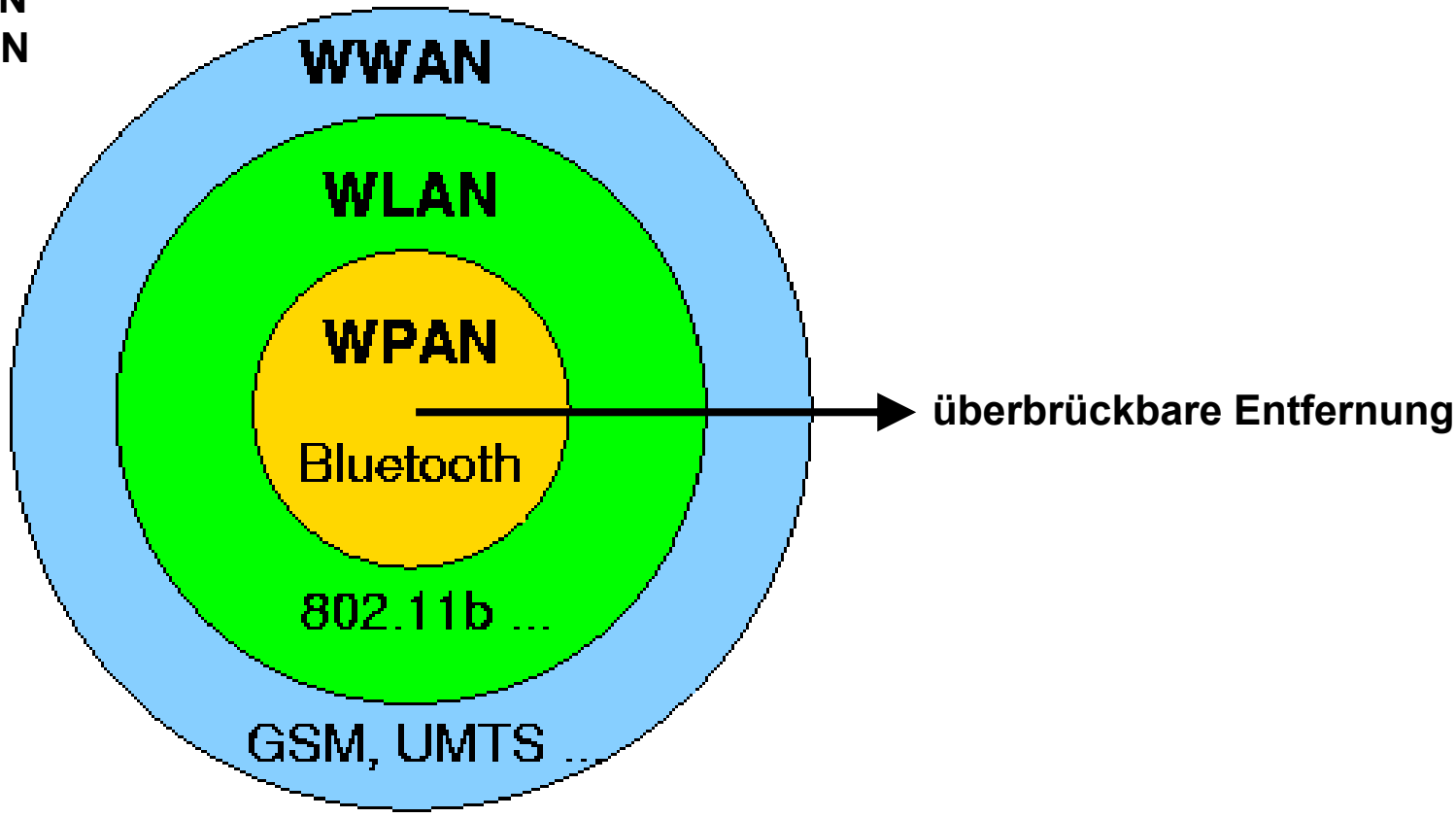
3.3 Entwurfsziele für drahtlose LANs

- Weltweite Funktion
- Möglichst geringe Leistungsaufnahme wegen Batteriebetrieb
- Betrieb ohne Sondergenehmigungen bzw. Lizenzen möglich
- Robuste Übertragungstechnik
- Vereinfachung der (spontanen) Zusammenarbeit bei Treffen
- Einfache Handhabung und Verwaltung
- Schutz bereits getätigter Investitionen im Festnetzbereich
- Sicherheit hinsichtlich Abhören vertraulicher Daten und auch hinsichtlich der Emissionen
- Transparenz hinsichtlich der Anwendungen und Protokolle höherer Schichten

3.3 Drahtlose Netze im Vergleich

WWAN: **Wireless WAN**
WLAN: **Wireless LAN**
WPAN: **Wireless PAN**

PAN: **Personal Area Network**

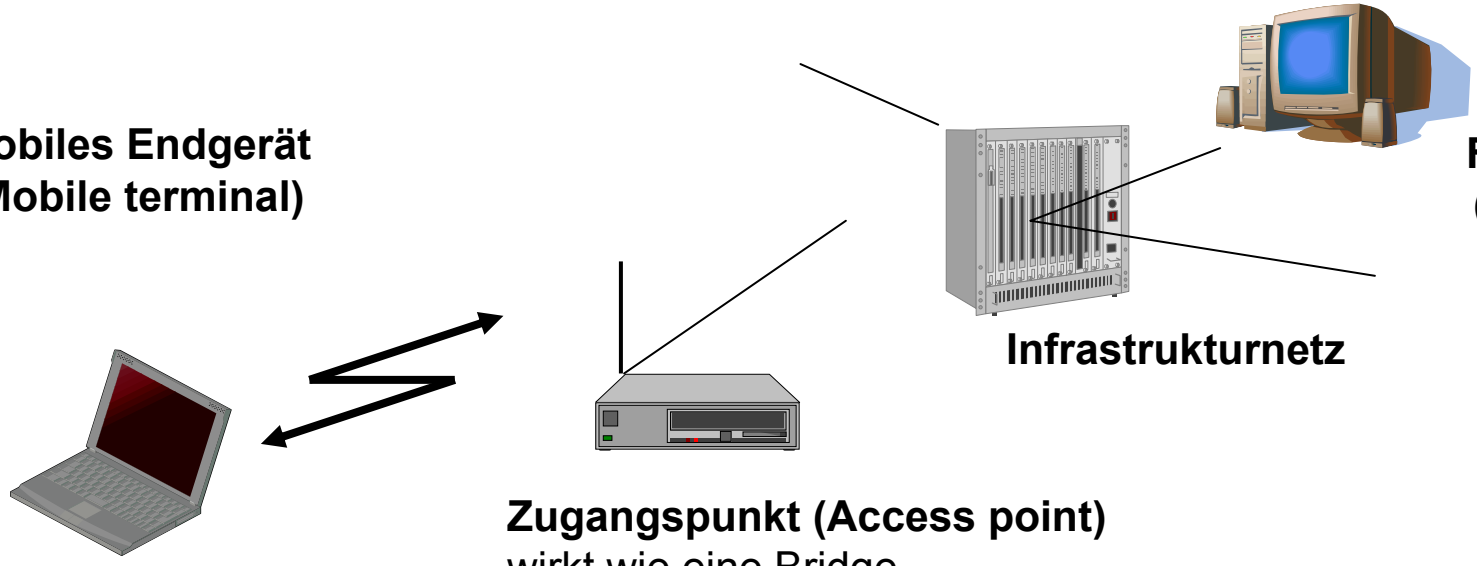


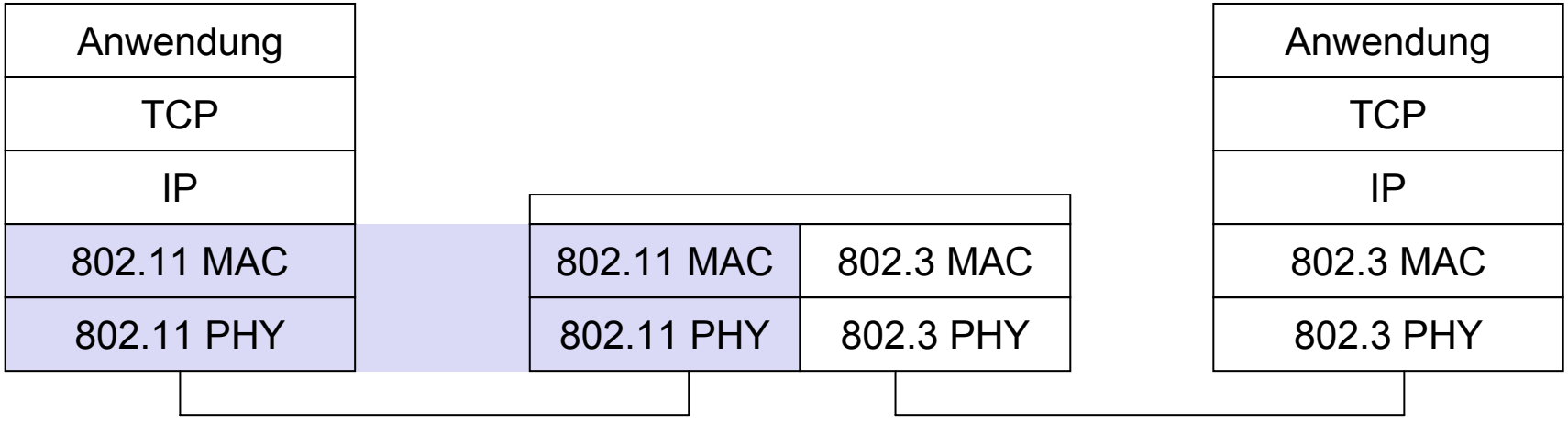
3.3 Vergleich Infrarot-/Funktechniken

- **Infrarot**
  - Einsatz von IR-Dioden, diffuses Licht, Reflektion von Wänden
- **Vorteile**
  - sehr billig und einfach
  - keine Lizenzen nötig
  - einfache Abschirmung
- **Nachteile**
  - Interferenzen durch Sonnenlicht, Wärmequellen etc.
  - wird leicht abgeschattet
  - niedrige Bandbreite
- **Einsatz**
  - als IrDA (Infrared Data Association) -Schnittstelle in fast jedem Mobilrechner verfügbar

- **Funktechnik**
  - heute meist Nutzung des 2,4 GHz lizenzfreien Bandes
- **Vorteile**
  - Erfahrungen aus dem WAN und Telefonbereich können übertragen werden
  - Abdeckung einer größeren Fläche mit Durchdringung von Wänden
- **Nachteile**
  - enger Frequenzbereich frei
  - schwierigere Abschirmung, Interferenzen mit Elektrogeräten
- **Einsatz**
  - vielfältige, separate Produkte

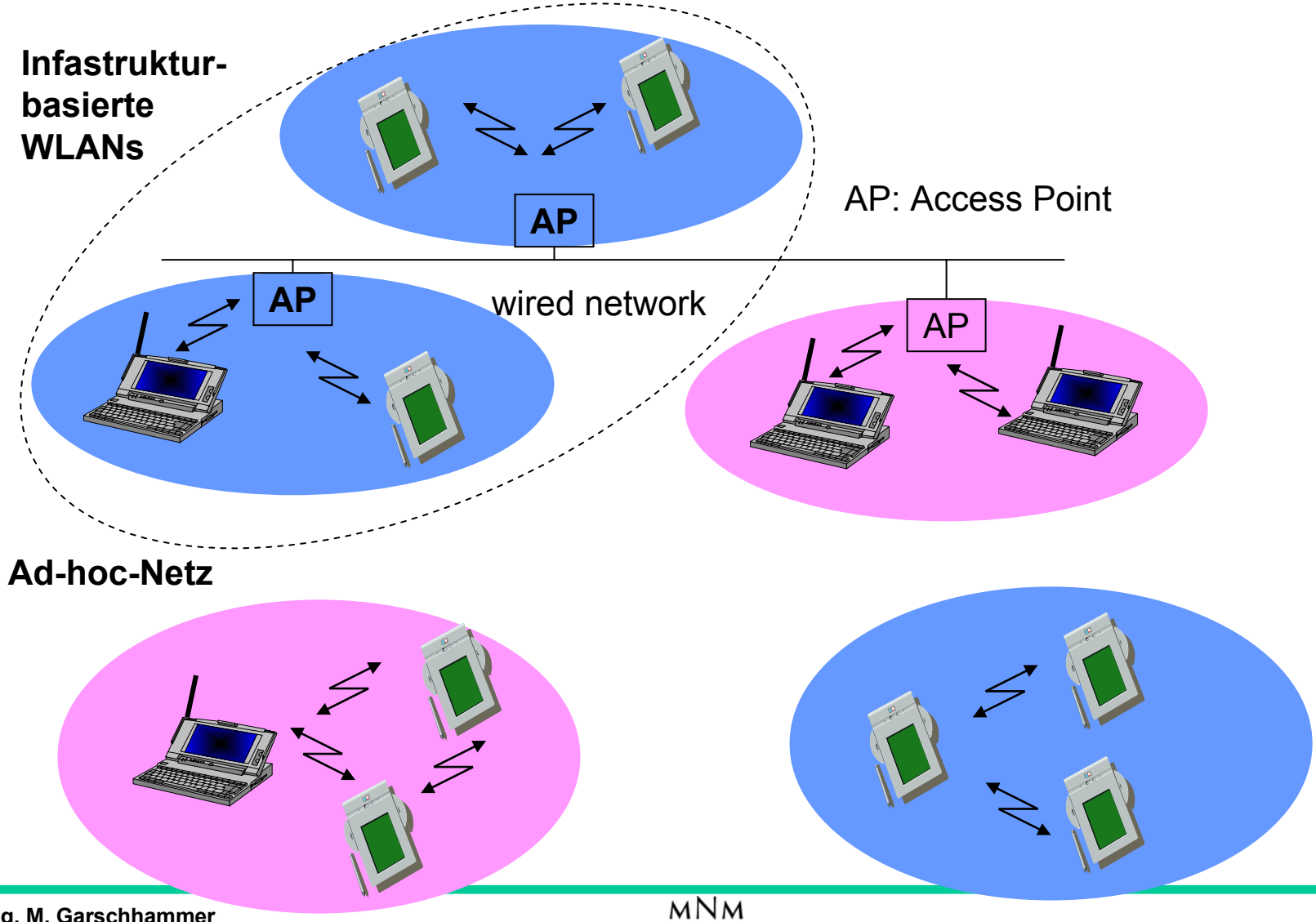
3.3.1 IEEE-Standard 802.11 (Basisversion)



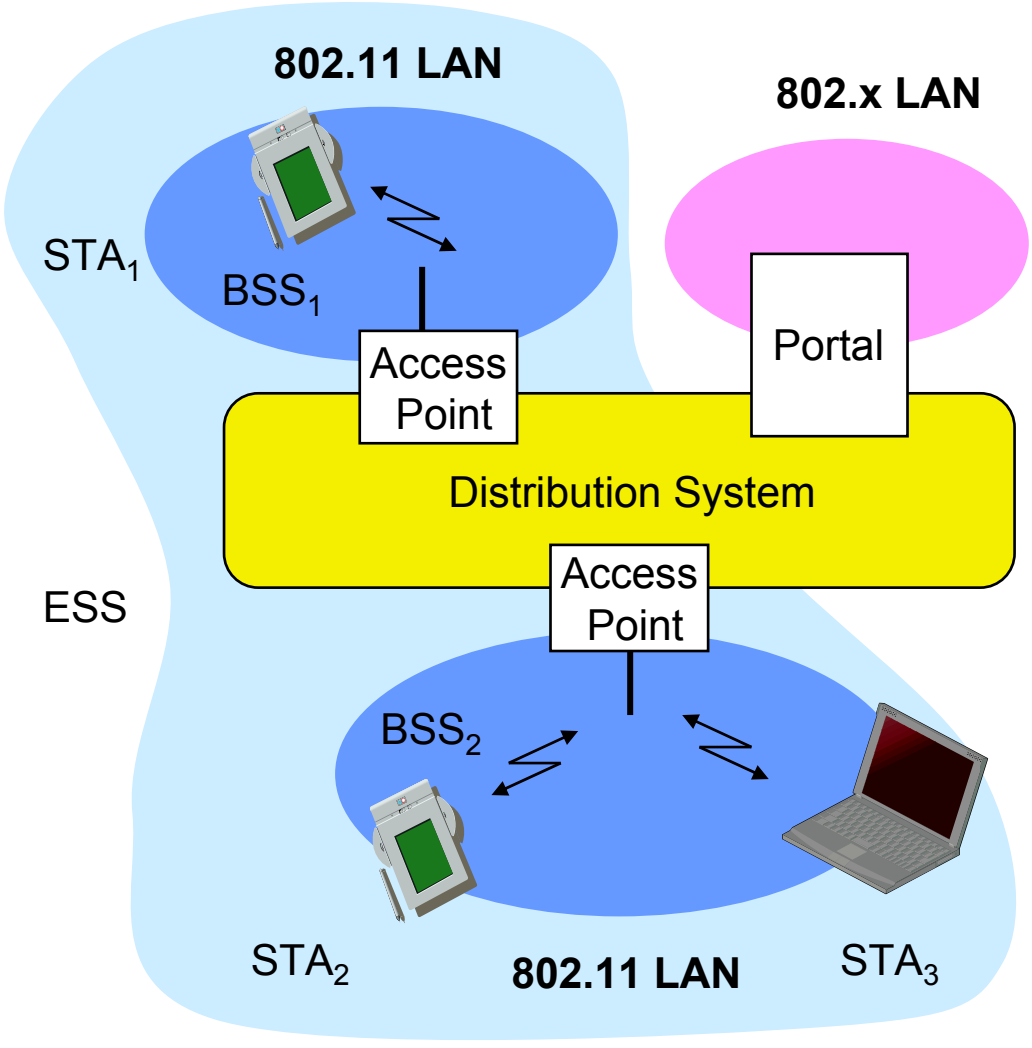


3.3.1.1 Topologien nach IEEE 802.11 (1)

- **Infrastruktur-basierte WLANs vs. Ad-Hoc-Netze**

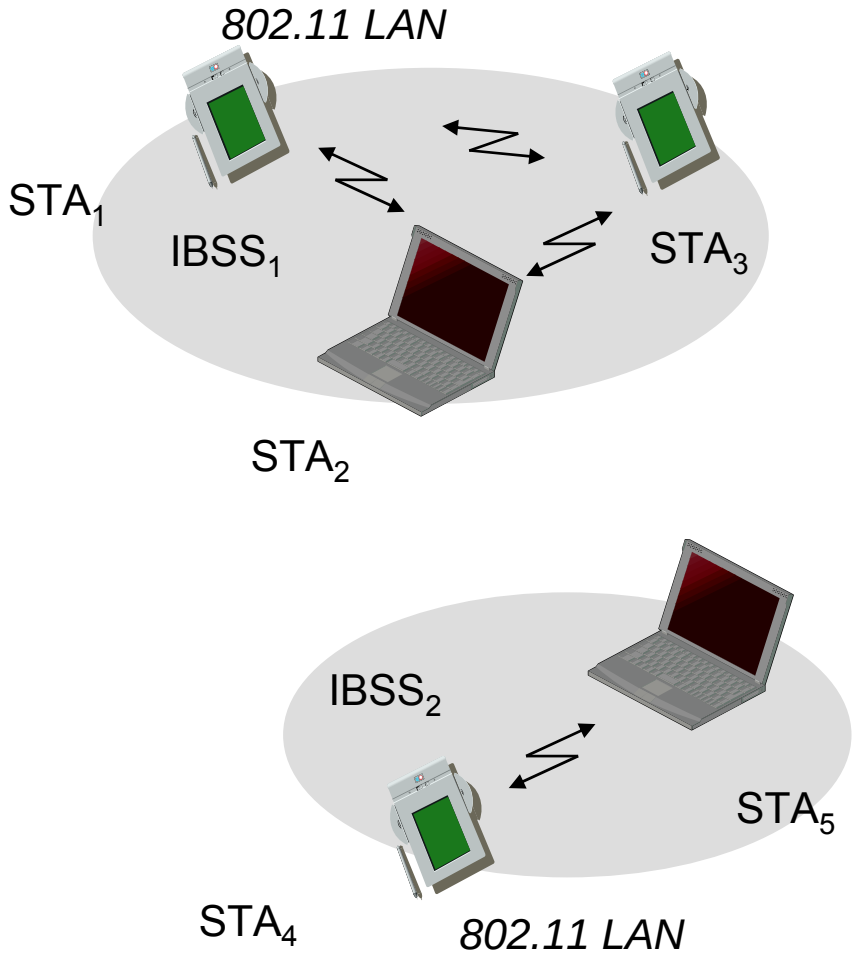


3.3.1.1 Topologien nach IEEE 802.11 (2): Infrastrukturnetz



- **Station (STA)**
  - Rechner mit Zugriffsfunktion auf das drahtlose Medium und Funkkontakt zum Access Point
- **Basic Service Set (BSS)**
  - Gruppe von Stationen, die dieselbe Funkfrequenz nutzen
- **Access Point**
  - Station, die sowohl in das Funk-LAN als auch das verbindende Festnetz (Distribution System) integriert ist
- **Portal**
  - Übergang in ein anderes Festnetz
- **Distribution System**
  - Verbindung verschiedener Zellen um ein Netz (ESS, Extended Service Set) zu bilden

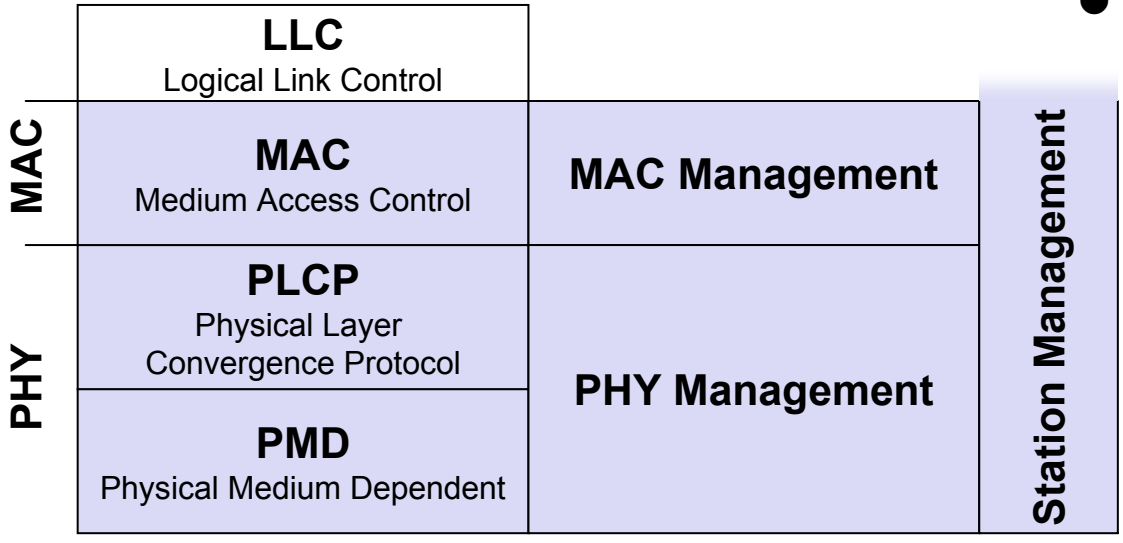
3.3.1.1 Topologien nach IEEE 802.11 (3): Ad-hoc-Netz



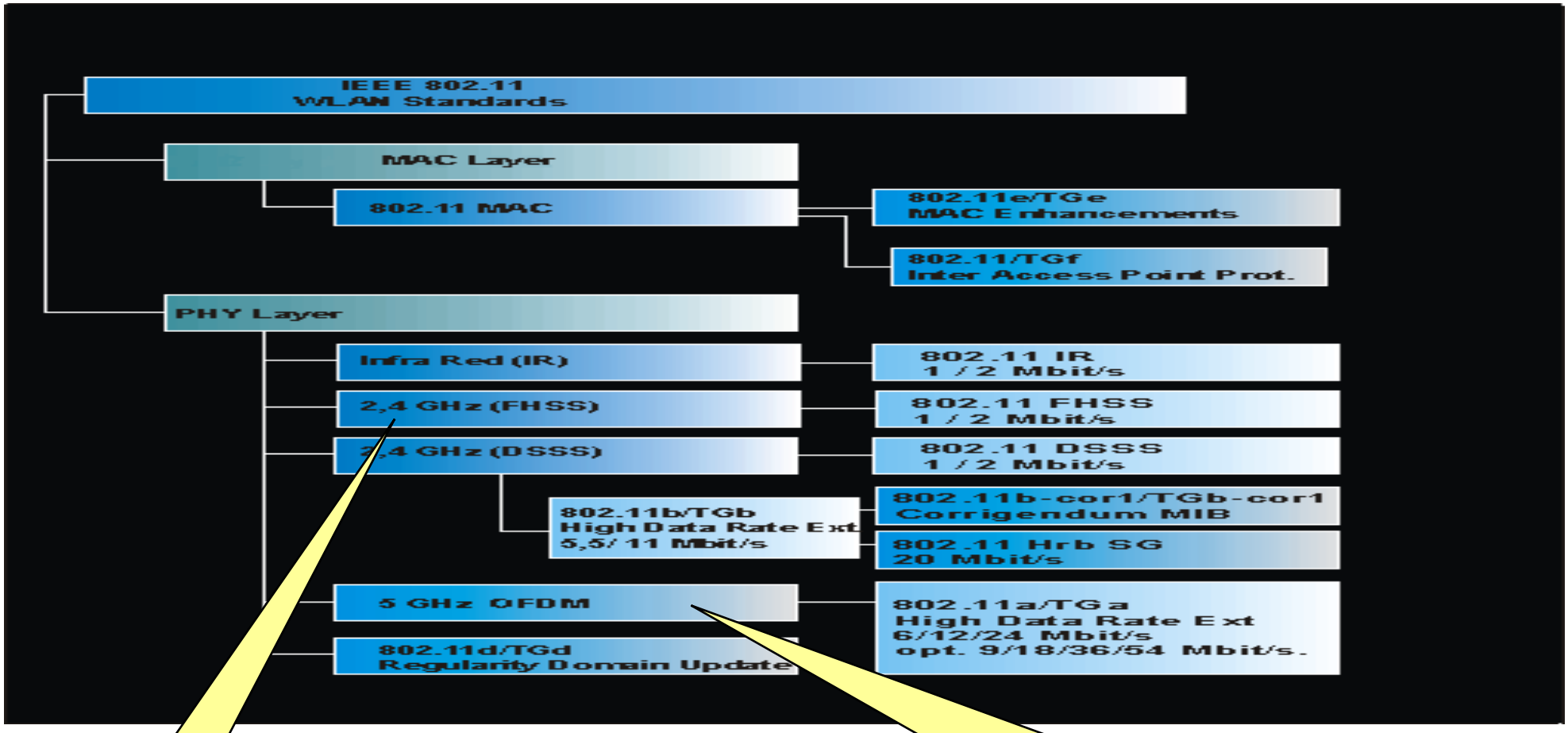
- **Direkte Kommunikation mit begrenzter Reichweite**
  - Station (STA):
    Rechner mit Zugriffsfunktion auf das drahtlose Medium
  - Independent Basic Service Set (IBSS):
    Gruppe von Stationen, die dieselbe Funkfrequenz nutzen
  - Netz besteht aus den Geräten selbst
  - Punkt-zu-Punkt Verbindungen
  - Geräte kommunizieren direkt miteinander
  - geeignet für kleine Netze oder um 2 bestehende Netze miteinander zu verbinden
  - Schwierigkeiten mit der Funknetzkarte
  - Treiberprobleme bei verschiedenen Betriebssystemen

3.3.1.2 Schichten und Funktionen

- **MAC**
  - Zugriffsmechanismus, Fragmentierung, Verschlüsselung
- **MAC Management**
  - Synchronisierung, Roaming, MIB, Power
- **PLCP**
  - Clear Channel Assessment Signal (Carrier Sense)
- **PMD**
  - Modulation, Codierung
- **PHY Management**
  - Kanalwahl, MIB
- **Station Management**
  - Koordination der Management-Funktionen



3.3.1.2 Mögliche Schichten innerhalb 802.11

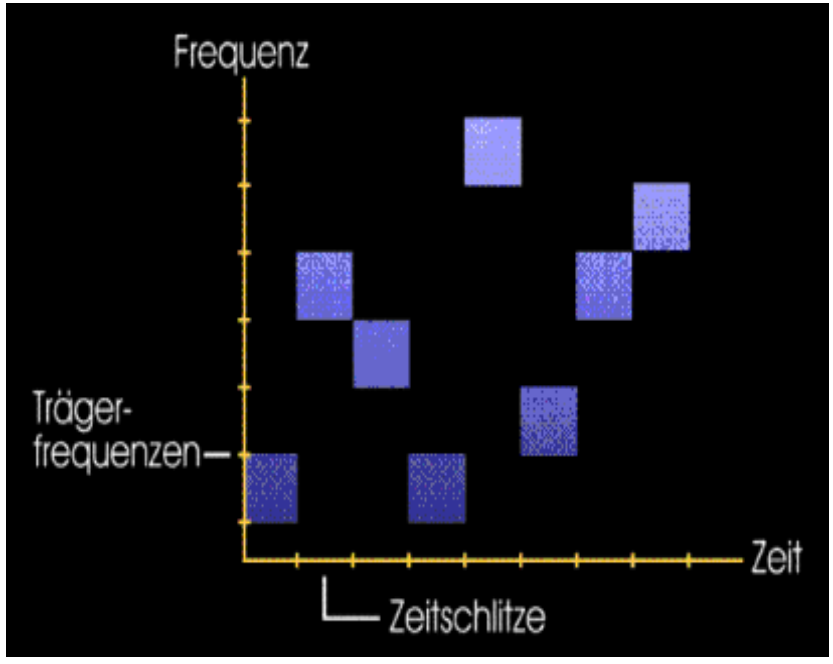


FHSS, DSSS (1997)

OFDM, HR-DSSS (1999, um höhere Bandbreiten zu erzielen)

3.3.1.2.1 Bitübertragungsschicht (1)

- **3 Varianten: 2 Funk (vornehmlich im 2,4 GHz-Band), 1 IR**
  - Datenrate 1 bzw. 2 Mbit/s
- **Funkvariante 1: FHSS (Frequency Hopping Spread Spectrum)**
  - Verwendet 79 Kanäle, jeder Kanal ist 1 MHz breit, Nutzsignal wird auf eine sich sprunghaft ändernde Trägerfrequenz aufmoduliert
  - Ein Generator für Pseudozufallszahlen erzeugt die Folge der Frequenzen, auf die gewechselt wird
  - Verweilzeit (Dwell Time): Zeitspanne, in der eine Frequenz aktiv ist (muss unter 400 ms liegen)
  - Mindestmaß an Sicherheit; unempfindlich gegenüber Funkstörungen, geringe Bandbreite

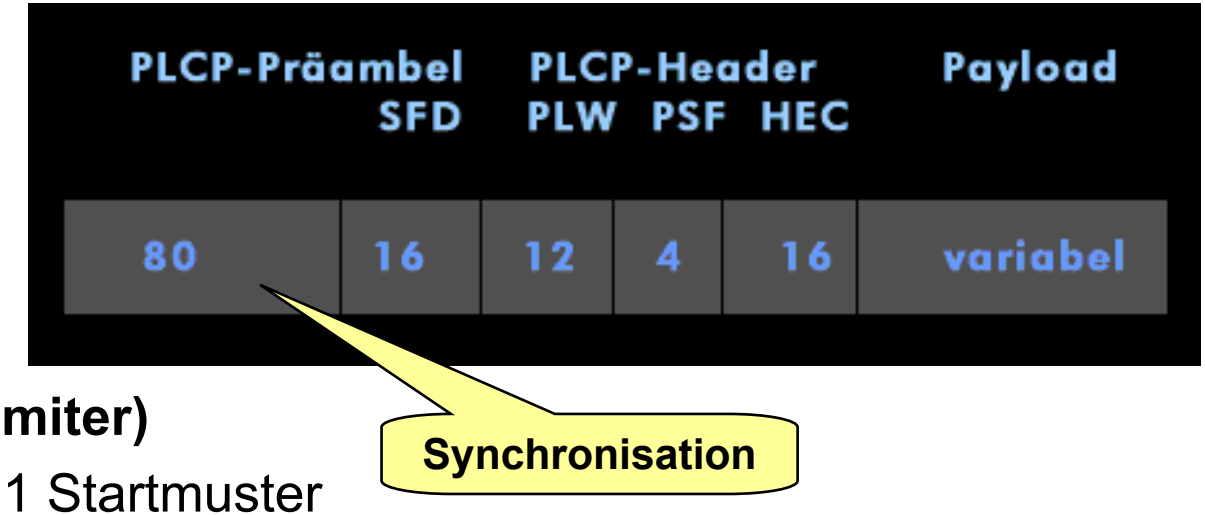


3.3.1.2.1 Bitübertragungsschicht (2)

- Die Sprungfolge wird durch einen Pseudo-Zufallsgenerator bestimmt, wobei die minimale Sprungdistanz mindestens 6 Kanäle beträgt
- Für die Frequenzsprungtechnik sind darüber hinaus mindestens 20 Frequenzsprünge pro Sekunde vorgeschrieben
- Damit das Signal vom Empfänger erkannt werden kann, muss dem Empfänger die Reihenfolge des Frequenzwechsels im Voraus bekannt sein, was durch das Aushandeln der Frequenzfolge zwischen Sender und Empfänger erfolgt

3.3.1.2.1 FHSS Paketformat

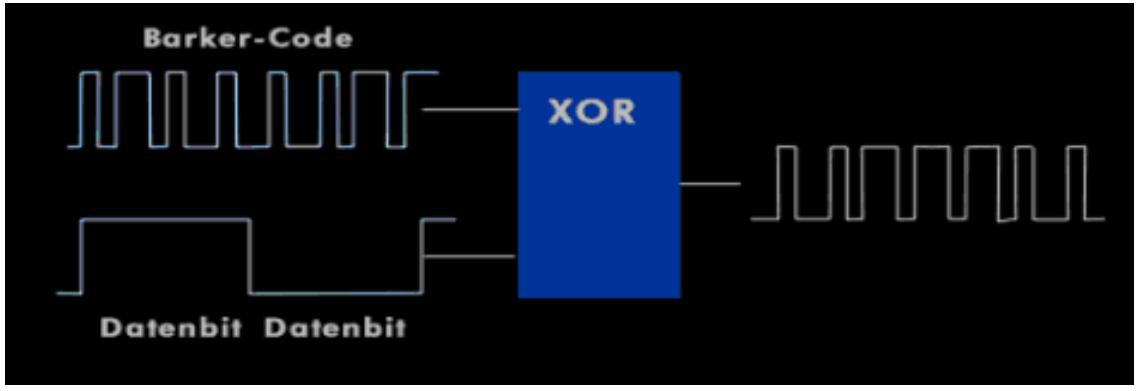
- **Synchronisation**
  - Synch. mit 010101... Muster



- **SFD (Start Frame Delimiter)**
  - 0000110010111101 Startmuster
- **PLW (PLCP_PDU Length Word)**
  - Länge der Nutzdaten inkl. 32 bit CRC der Nutzdaten, PLW < 4096
- **PSF (PLCP Signaling Field)**
  - Art der Nutzdaten (1 or 2 Mbit/s)
- **HEC (Header Error Check)**
  - CRC mit $x^{16}+x^{12}+x^{5}+1$

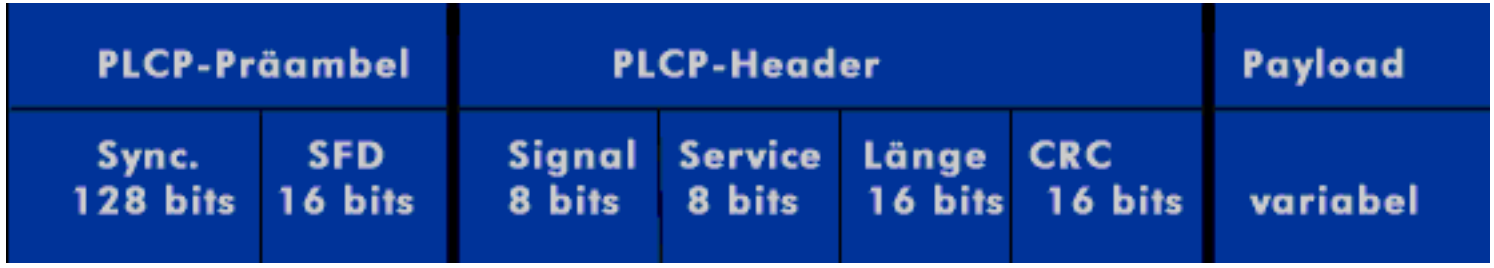
3.3.1.2.1 Bitübertragungsschicht (3)

- **Funkvariante 2: DSSS (Direct Sequence Spread Spectrum)**
  - Gewisse Ähnlichkeit mit CDMA
  - Jedes Bit wird in der Form von 11 Chips unter Verwendung der so genannten *Barker-Folge* übertragen
    - Chip-Sequenz: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (ein Barker-Code)



  - 2,4-GHz-Frequenzband in 22 MHz bis 26 MHz breite Frequenzbänder unterteilt
  - Das Verhältnis von gespreizter Bandbreite zu Übertragungsgeschwindigkeit heißt Spreizverhältnis
    - Ist dieses Verhältnis 10, sind die Übertragungs- und Sicherheitsbedingungen ideal

3.3.1.2.1 DSSS Paketformat



- **Synchronisation**
  - synch., Leistungssteuerung, Signaldetektion, Frequenzanpassung
- **SFD (Start Frame Delimiter)**
  - 1111001110100000
- **Signal**
  - Datenrate der Nutzlast (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- **Service (Dienstkennung)**
  - Ein Leistungsmerkmal von ISDN, mit dem die Verbindung unter inkompatiblen Endgeräten verhindert wird
- **Length**
  - reserviert, 00: gemäß 802.11
  - Länge der Nutzdaten
- **HEC (Header Error Check)**
  - Schutz der Felder signal, service und length, $x^{16}+x^{12}+x^{5}+1$

3.3.1.2.1 Bitübertragungsschicht (4)

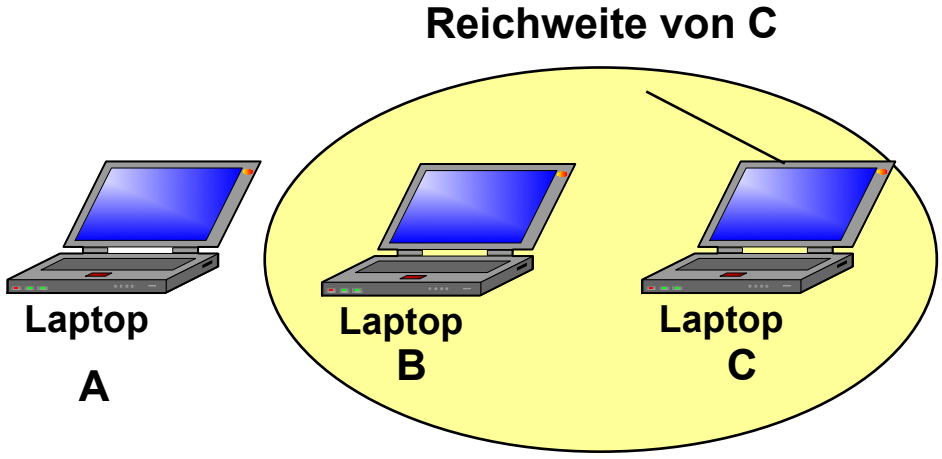
- **OFDM, Orthogonal Frequency Division Multiplex**
  - Wurde erstmals bei drahtlosen Hochgeschwindigkeits-LANs (802.11a) verwendet
    - 52 Kanäle insgesamt, 48 für Daten, 4 für Synchronisation
  - Orthogonale Frequenzmultiplex-Technik verwendet mehrere Trägerfrequenzen für die Übertragung eines Digitalsignals, diese Trägerfrequenzen werden allerdings nur mit einer verringerten Übertragungsrate moduliert
  - Zu diesem Zweck wird bei OFDM das zur Verfügung stehende Frequenzband in mehrere Trägerbänder unterteilt
  - Aufteilung des Signals in viele schmale Bänder
    - Vorteil: bessere Immunität gegen Störungen, Möglichkeit nicht benachbarte Bänder zu verwenden
    - Kompatibel mit dem europäischen HiperLAN/2-System

3.3.1.2.1 Bitübertragungsschicht (5)

- **HR-DSSS (High Rate Direct Sequence Spread Spectrum)**
  - Wird bei 802.11b eingesetzt
  - Verwendet 11 Millionen Chips/s, um 11Mbit/s auf dem 2,4-GHz-Band zu erzielen
  - Datenübertragungsrate kann dynamisch während der Übertragung angepasst werden
  - Reichweite von 802.11b etwa siebenmal größer als 802.11a, aber langsamer
- **802.11g verwendet OFDM-Modulationsverfahren von 802.11a, arbeitet aber im dem schmaleren 2.4-GHz-Band zusammen mit 802.11b**

3.3.1.2.2 MAC-Schicht

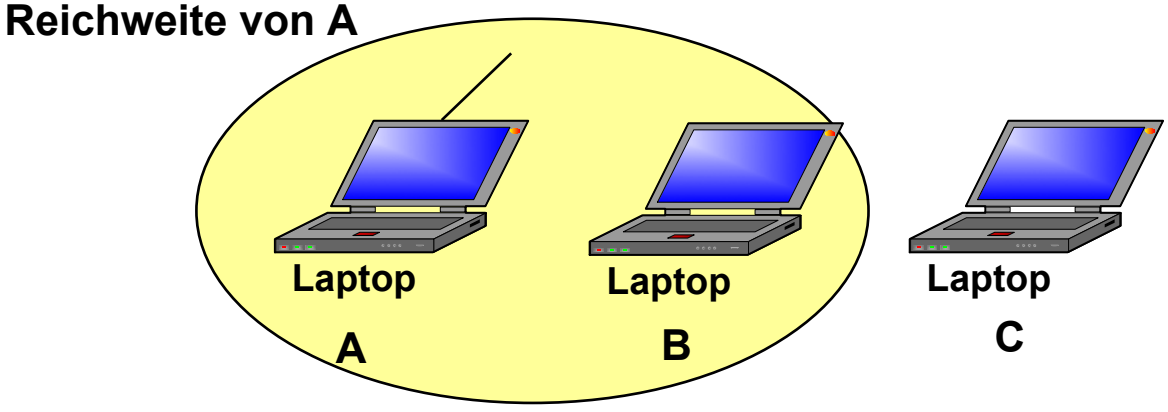
❑ Hidden-Station-Problem



A möchte an B senden,
kann aber nicht erkennen,
dass B beschäftigt ist

C überträgt Daten

❑ Exposed-Station-Problem



B möchte an C senden und
ist irrtümlich der Auffassung,
dass die Übertragung
nicht gelingt

A überträgt Daten

3.3.1.2.2 MAC-Schicht: Betriebsmodi (1)

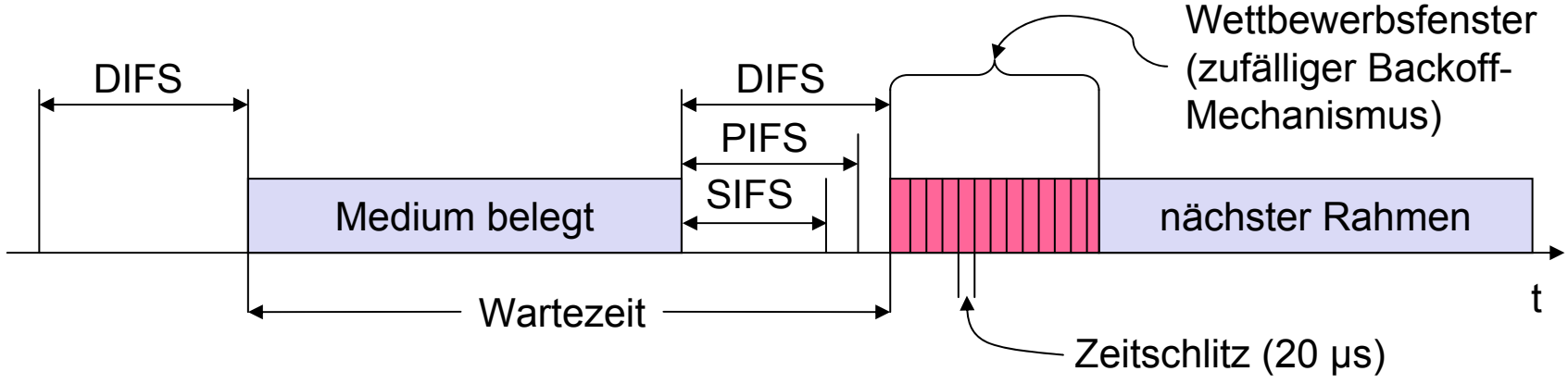
- **WLANs nach IEEE 802.11**
  - Es handelt sich hierbei übertragungstechnisch um ein Shared-Media-Verfahren mit CSMA/CA, mit dem keine Dienstgüte-Merkmale (QoS) garantiert werden können
- **Zur Lösung des Hidden-Station- und des Exposed-Station-Problems werden zwei Betriebsmodi angeboten:**
  - **Distributed Coordination Function (DCF):**
    - Verteilte Koordinierungsfunktion
    - Keine zentrale Kontrolle, daher ähnlich zu Ethernet
    - Alle Implementierungen müssen diesen Modus unterstützen
    - Protokoll **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance)
  - **Point Coordination Function (PCF):**
    - Punktbezogene Koordinierungsfunktion
    - Die Basisstation steuert die gesamte Aktivität in einer Zelle
    - Die Implementierung ist optional

3.3.1.2.2 MAC-Schicht: CSMA/CA (1)

- **Bei diesem Protokoll wird physische und virtueller Kanalprüfung verwendet**
- **Vorgehensweise**
  - Sendewillige Station hört das Medium ab (Carrier Sense basierend auf CCA, Clear Channel Assessment)
  - Ist das Medium für die Dauer eines Inter-Frame Space (IFS) frei, wird gesendet (IFS je nach Sendeart gewählt)
  - Ist das Medium belegt, wird auf einen freien IFS gewartet und dann zusätzlich um eine zufällige Backoff-Zeit verzögert (Kollisionsvermeidung, in Vielfachen einer Slot-Zeit)
  - Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, bleibt der Backoff-Timer so lange stehen

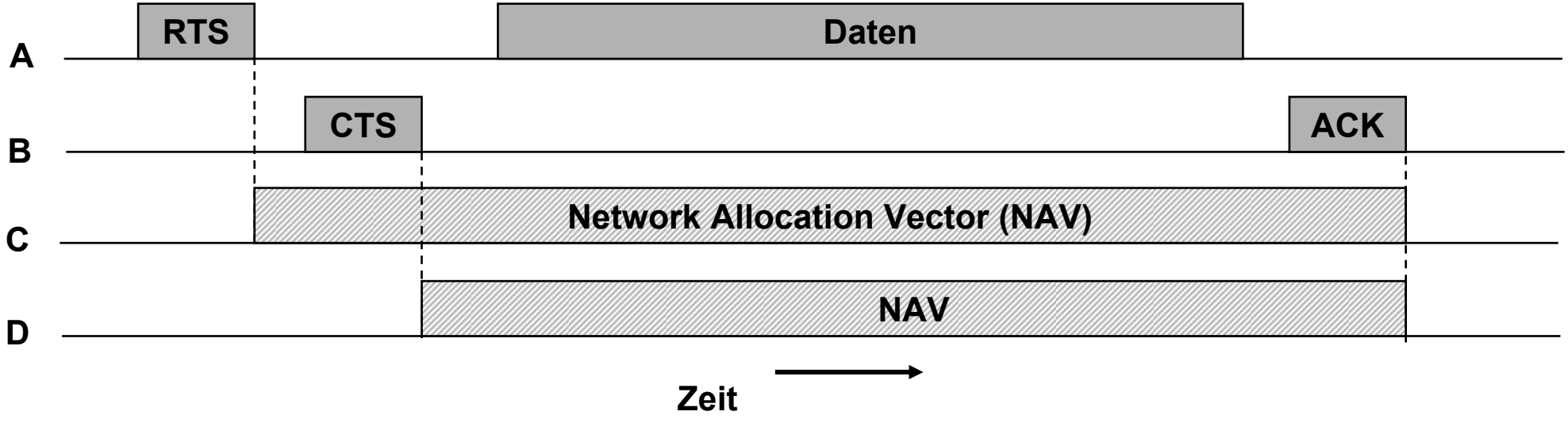
3.3.1.2.2 MAC-Schicht: Betriebsmodi (2)

- **Modus 1:**
  - werden durch Staffelung der Zugriffszeitpunkte geregelt
  - keine garantierten Prioritäten
  - **SIFS (Short Inter Frame Spacing) – 10 µs**
    - **höchste Priorität, für ACK, CTS, Antwort auf Polling**
  - **PIFS (PCF (Point Coordination Function) IFS) – 30 µs**
    - **mittlere Priorität, für zeitbegrenzte Dienste mittels PCF**
  - **DIFS (DCF, Distributed Coordination Function IFS) – 50 µs**
    - **niedrigste Priorität, für asynchrone Datendienste**
  - **EIFS (Extended InterFrame Spacing)**
    - **Wird von einer Station verwendet, die gerade einen fehlerhaften oder ungültigen Rahmen erhalten hat, um dies zu berichten**

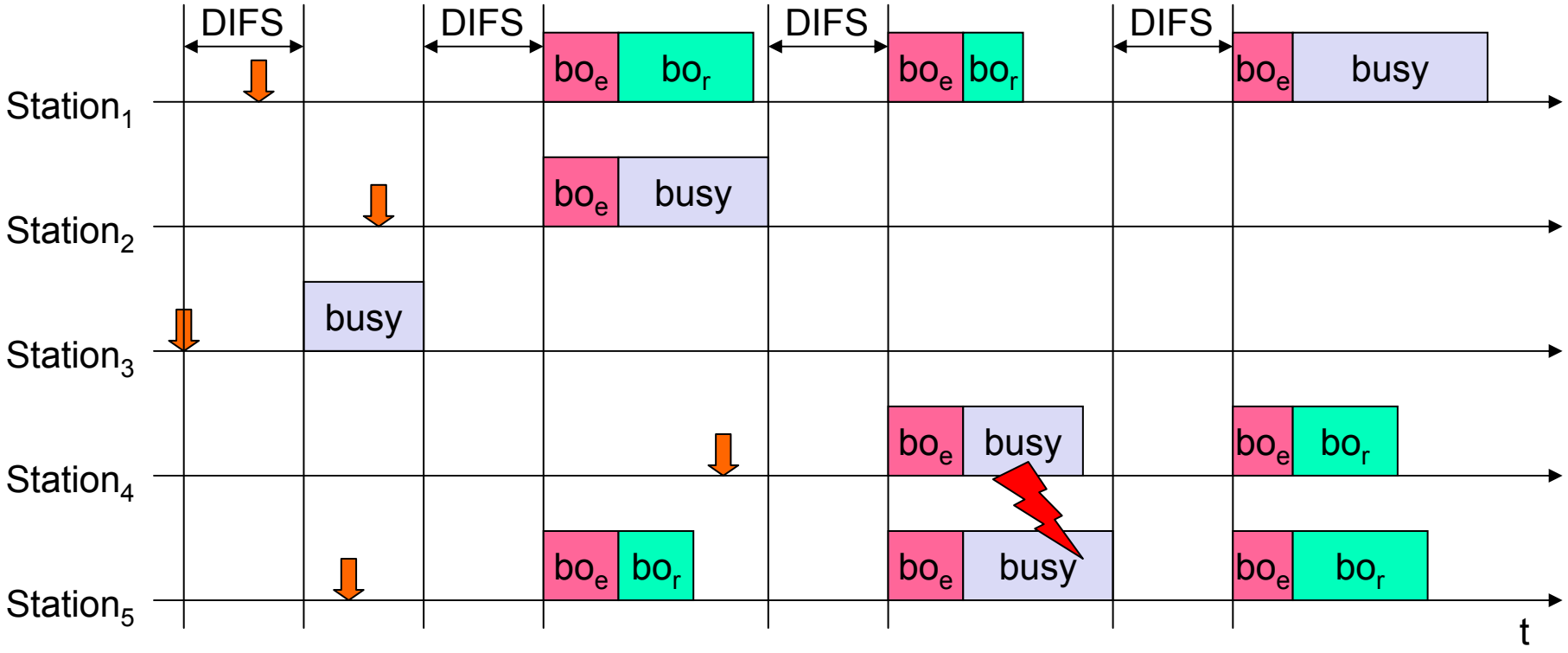


3.3.1.2.2 MAC-Schicht: CSMA/CA (2)

- **Modus 2:**
  - Basiert auf MACAW und virtueller Kanalprüfung
  - Im Beispiel (s.u.) möchte A an B Daten senden; Beginnt mit der Übertragung eines RTS-Rahmen an B, um die Erlaubnis anzufordern, einen Rahmen zu senden
  - C ist in Reichweite von A (eventuell auch von B, aber dieses ist nicht relevant)
  - D ist in Reichweite von B, aber nicht von A



3.3.1.2.2 Stationen im Wettbewerb - einfache Version



busy — Medium belegt (frame, ack etc.)

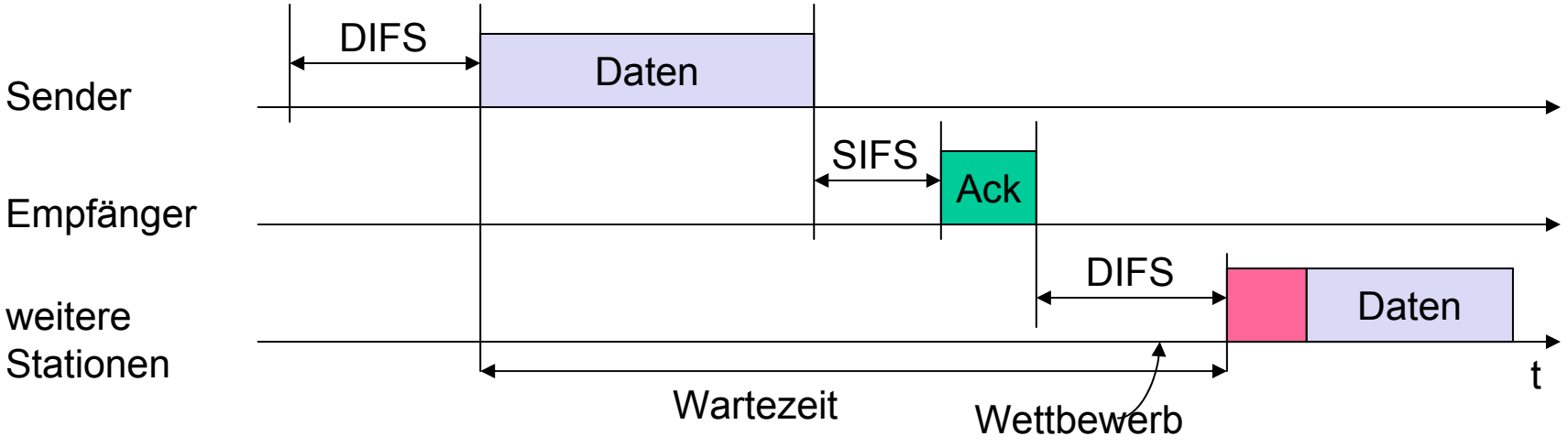
Paketankunft am MAC-SAP

bo_e verstrichene backoff Zeit

bo_r verbleibende backoff Zeit

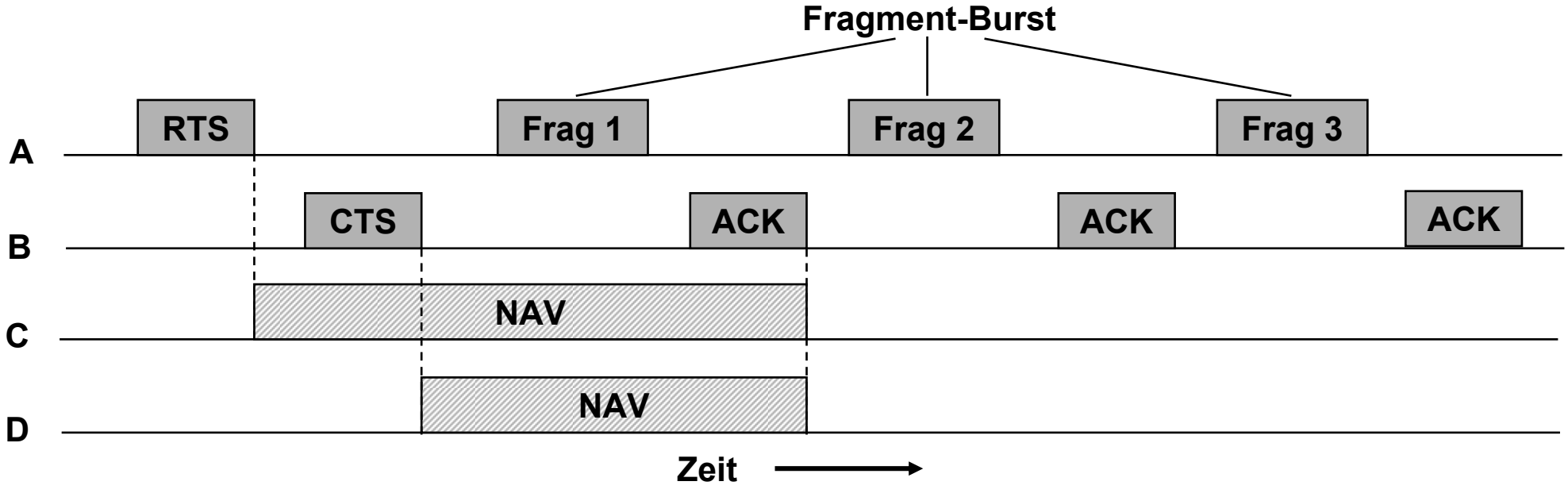
3.3.1.2.2 CSMA/CA-Verfahren (3)

- **Senden von Unicast-Paketen**
  - Daten können nach Abwarten von DIFS gesendet werden
  - Empfänger antworten sofort (nach SIFS), falls das Paket korrekt empfangen wurde (CRC)
  - Im Fehlerfall wird das Paket automatisch wiederholt



3.3.1.2.2 MAC-Schicht: Fragmentierung

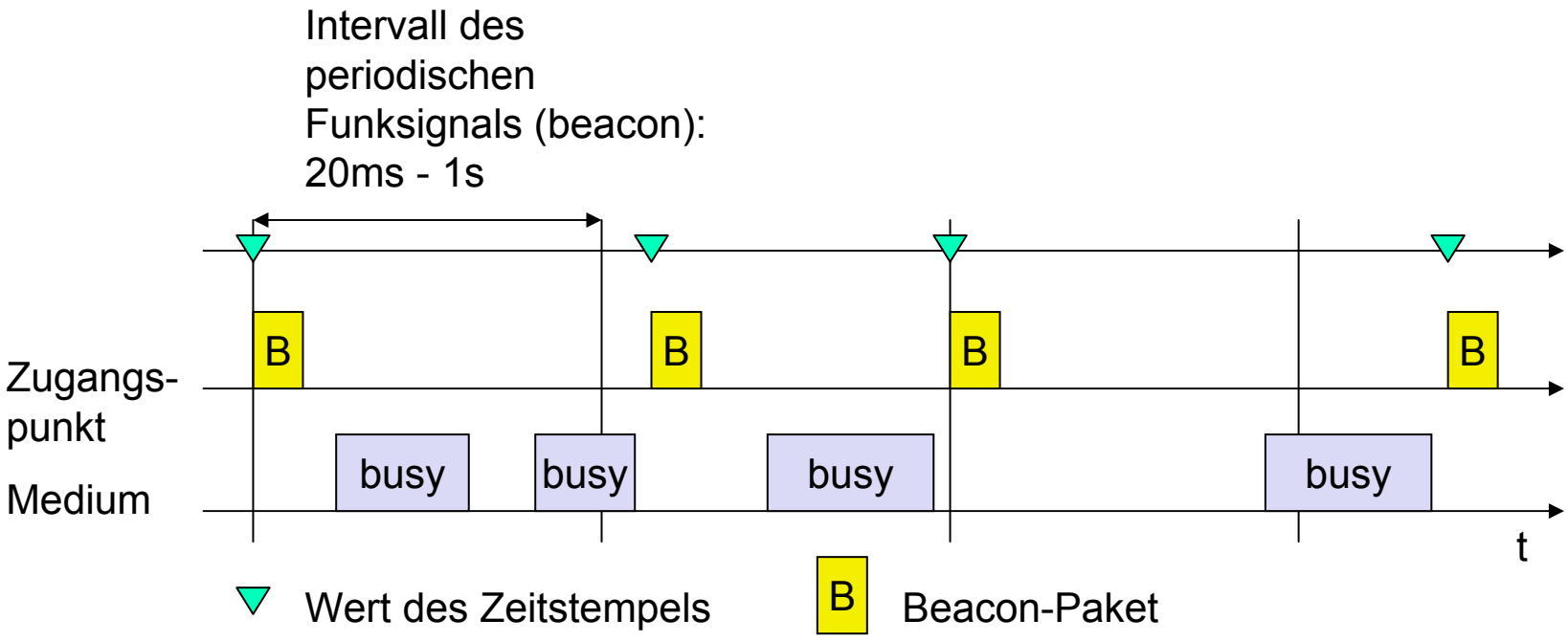
- Um nicht eine hohe Wahrscheinlichkeit zu haben, dass Rahmen durch Fehler erneut gesendet werden müssen, können Rahmen fragmentiert werden
- Jedes Fragment hat seine eigene Prüfsumme
- Fragmente werden durchnummeriert und mit dem Stop-and-Wait-Protokoll bestätigt



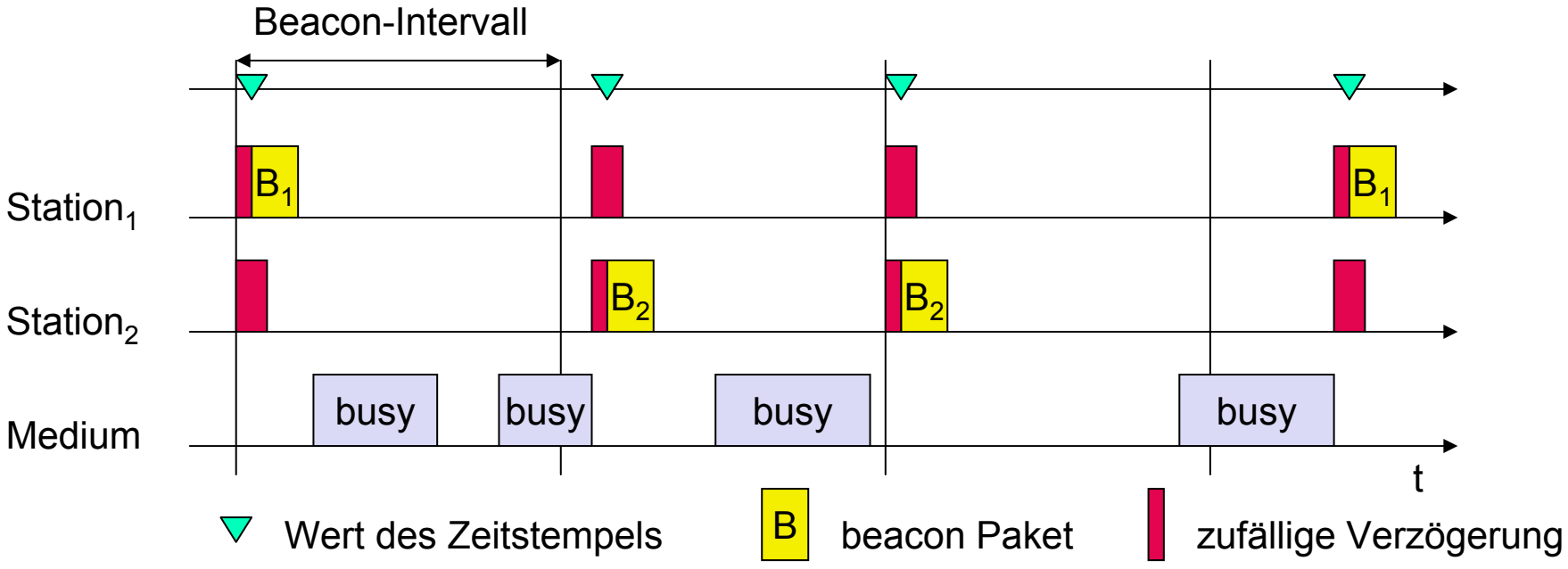
3.3.1.2.2 MAC-Schicht: PCF-Modus

Synchronisation mit einem „Leuchtfeuer“ (Infrastruktur)

- Ein Beacon-Rahmen wird in periodischen Abständen gesendet
- Enthält Systemparameter (Frequenzsprungfolgen, Verweilzeiten, Taktsynchronisation ...)
- Fordert neue Stationen für das „polling“ auf

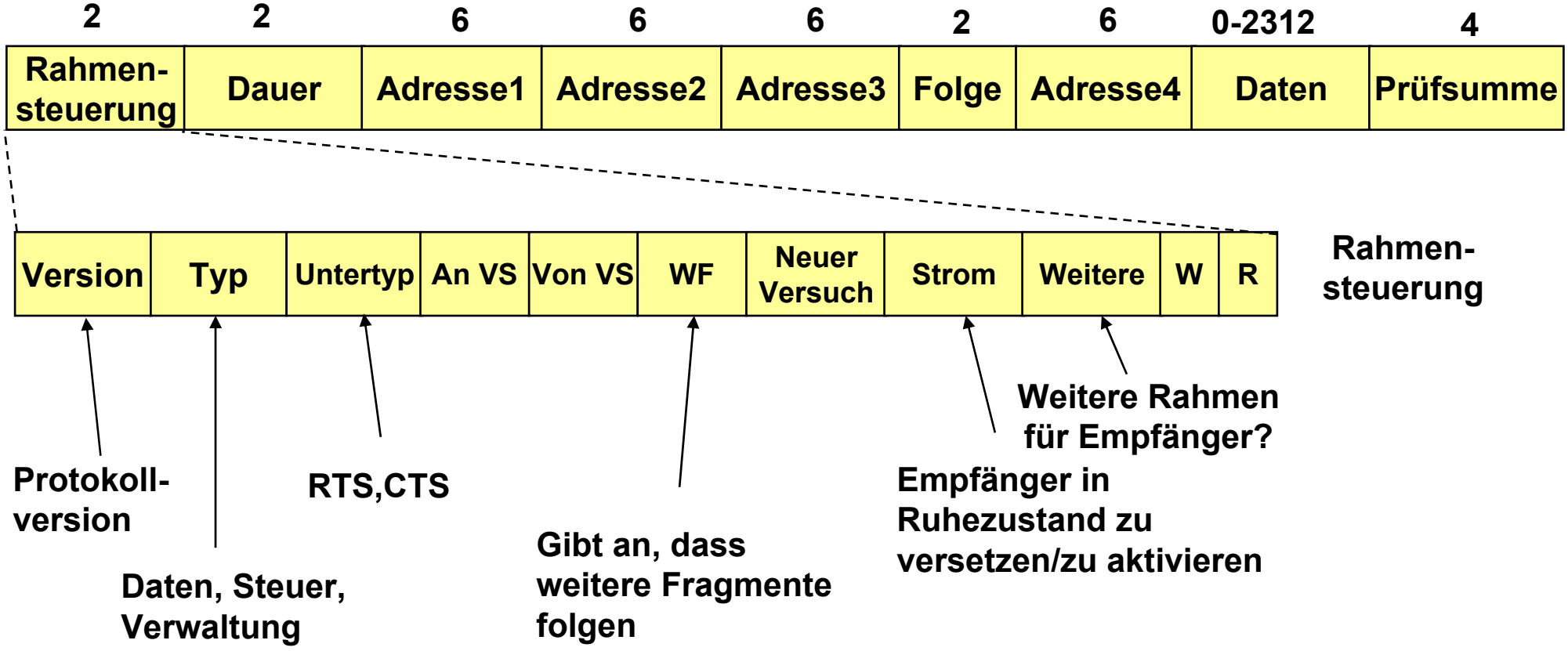


3.3.1.2.2 Synchronisation mit Beacon (ad-hoc)



3.3.1.2.2 MAC-Schicht: Rahmenstruktur

- Es sind drei verschiedene Rahmenklassen definiert für Daten, Steuerung und Verwaltung
- Datenrahmen



3.3.1.3 Dienste (1)

- **Dienste sind in 2 Kategorien unterteilt:**
  - **Verteilungsdienste**
    - Verwaltung der Zellenzugehörigkeit und die Interaktion mit den Stationen **außerhalb** der Zelle
  - **Stationsdienste**
    - Aktivität **innerhalb** einer Zelle
- **Verteilungsdienste**
  - **Assoziation**
    - Mit diesen Dienst bauen Mobilstationen eine Verbindung zur Basisstation auf
    - Beim Eintritt gibt Station ihre Identität und Leistungsmerkmale bekannt
    - Wird eine Mobilstation angenommen, muss sie sich zunächst authentifizieren
  - **Trennung**

3.3.1.3 Dienste (2)

- **Erneute Verbindung**
  - Station kann Basisstation wechseln
- **Verteilung**
  - Legt fest, wie Rahmen zur Basisstation weitergeleitet werden (Funk, Festnetz)
- **Integration**
  - Übersetzung von 802.11-Format in das vom Zielnetz benötigte Format

❑ **Stationsdienste**

- **Authentifizierung**
  - Basisstation sendet einen speziellen Herausforderungsrahmen (Challenge Frame), um zu prüfen, ob die Mobilstation den geheimen Schlüssel (Passwort) kennt
  - Mobilstation entschlüsselt den Rahmen und schickt ihn an die Basisstation zurück

3.3.1.3 Dienste (3)

- **Aufhebung der Authentifizierung**
- **Datenschutz**
  - Verschlüsselungsalgorithmus RC4
- **Datenzustellung**

3.3.1.4 Problemstellung - Roaming

- **Keine oder schlechte Verbindung? - Dann:**
- **Scanning**
  - Abtasten der Umgebung (Medium nach „Leuchtfeuer“ von APs abhören oder Probe ins Medium senden und Antwort abwarten)
- **Reassociation Request**
  - Station sendet Anfrage an AP(s)
- **Reassociation Response**
  - bei Erfolg, d.h. ein AP hat geantwortet, nimmt Station nun teil
  - bei Misserfolg weiterhin Scanning
- **AP akzeptiert Reassociation Request**
  - Anzeigen der neuen Station an das Distribution System
  - Distribution System aktualisiert Datenbestand (d.h. wer ist wo)
  - normalerweise wird alter AP vom Distribution System informiert

3.3.1.5 IEEE 802.11 Standards: Übersicht (1)

- **802.11a**
  - High Speed Physical Layer im 5-GHz-Band
  - Der Standard basiert auf OFDM und der Direct-Sequence-Modulation (DSSS)
  - 802.11a arbeitet mit acht 20-MHz-Kanälen im Frequenzband von 5,15 GHz bis 5,35 GHz
  - Die Übertragungsgeschwindigkeit kann in 6-Mbit/s-Intervallen zwischen 6 Mbit/s und maximal 54 Mbit/s skaliert werden
- **802.11b**
  - Erweiterung im 2,4-GHz-Band
  - Diese Technik sieht Übertragungsraten von 5,5 Mbit/s über 11 Mbit/s bis 20 Mbit/s vor
  - Als Modulationstechnik wird CCK benutzt und zwar ausschließlich mittels Spreizbandtechnik
- **802.11c: Supplement to Bridge Standard**
- **802.11d: Regulatory Domain Updates**
- **802.11e: MAC Enhancement. Definition von Verfahren mit denen dem Anwender Quality of Service-Funktionen (QoS) zur Verfügung gestellt werden**

3.3.1.5 IEEE 802.11 Standards: Übersicht (2)

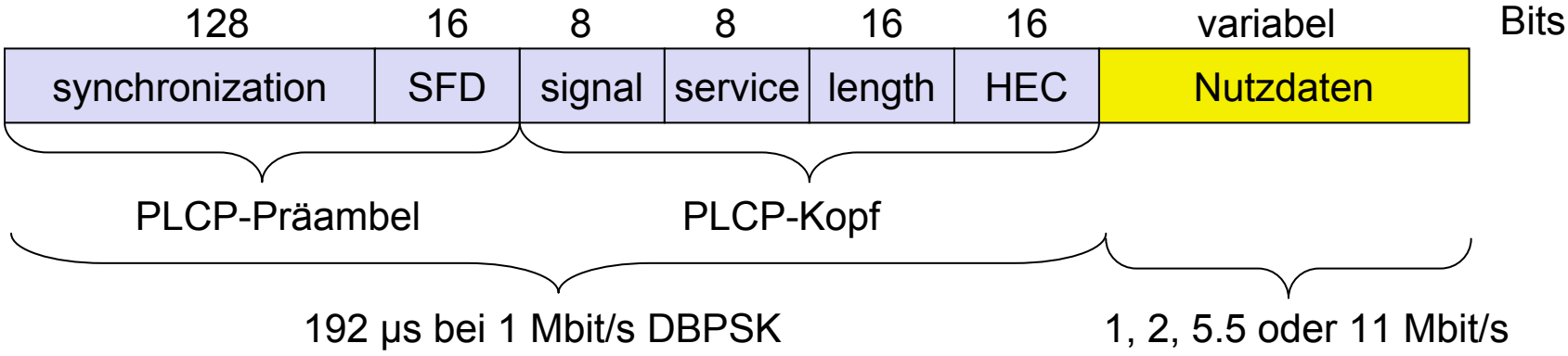
- **802.11f: Inter Access Point Protocol**
  - Ein Protokoll, über das sich Access Points (AP) miteinander unterhalten können
- **802.11g**
  - Übertragungsraten bis 54 Mbit/s, Übertragung im 2,4-GHz-Band
  - Modulationsverfahren ist das Orthogonal Frequency Division Multiplex (OFDM)
  - 802.11g ist rückwärtskompatibel zu 802.11b
  - Als Modulationsverfahren wird Complementary Code Keying (CCK) wie in 802.11b eingesetzt und Orthogonal Frequency Division Multiplexing (OFDM) wie in 802.11a; Optional sind außerdem die Modulationsverfahren CCK-OFDM und CCK- PBCC zugelassen
- **802.11h: Frequenzspektrum von 802.11a**
- **802.11i: Sicherheit, Verlängerung des Initialisierungsvektors von 24 Bit auf 128 Bit**
- **802.11 Hrb: Datenraten über 20 Mbit/s**

3.3.1.5.1 IEEE 802.11b

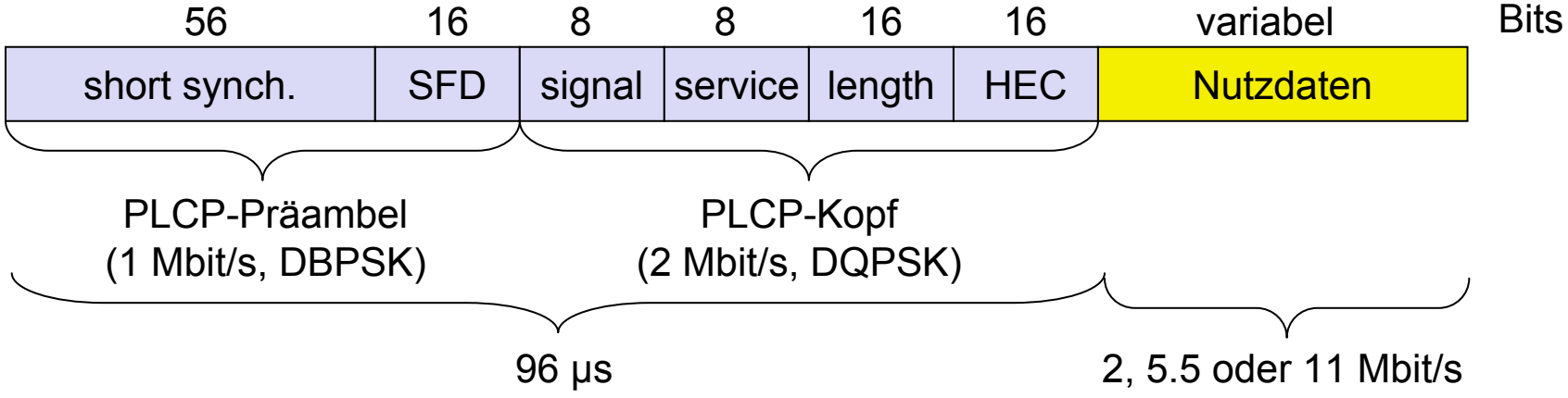
- Datenraten
  - 1, 2, 5,5, 11 Mbit/s, abhängig von SNR
  - Nutzdatenrate max. ca. 6 Mbit/s
- Kommunikationsbereich
  - 300m Außen-, 30m Innenbereich
  - Max. Datenrate bis ~10m (in Gebäuden)
- Frequenzbereich
  - Freies 2.4 GHz ISM-Band
- Sicherheit
  - Begrenzt, WEP unsicher, SSID
- Kosten
  - 150€ Adapter, 250€ Zugangspunkt
- Verfügbarkeit
  - Viele Produkte, viele Anbieter
- Verbindungsaufbaudauer
  - Verbindungslos, „always on“
- Dienstgüte
  - Typ: Best effort, keine Garantien (solange kein „Polling“ eingesetzt wird, nur begrenzte Produktunterstützung)
- Verwaltbarkeit
  - Begrenzt (keine automatische Schlüsselverteilung, symmetrische Verschlüsselung)
- Spezielle Vor-/Nachteile
  - Vorteil: viele installierte Systeme, große Erfahrung, weltweite Verfügbarkeit, freies ISM-Band, viele Firmen, integriert in Laptops, einfaches System
  - Nachteil: starke Störungen auf dem ISM-Band, keine Dienstgüte, relativ niedrige Datenraten

3.3.1.5.1 802.11b: PHY-Rahmenformate

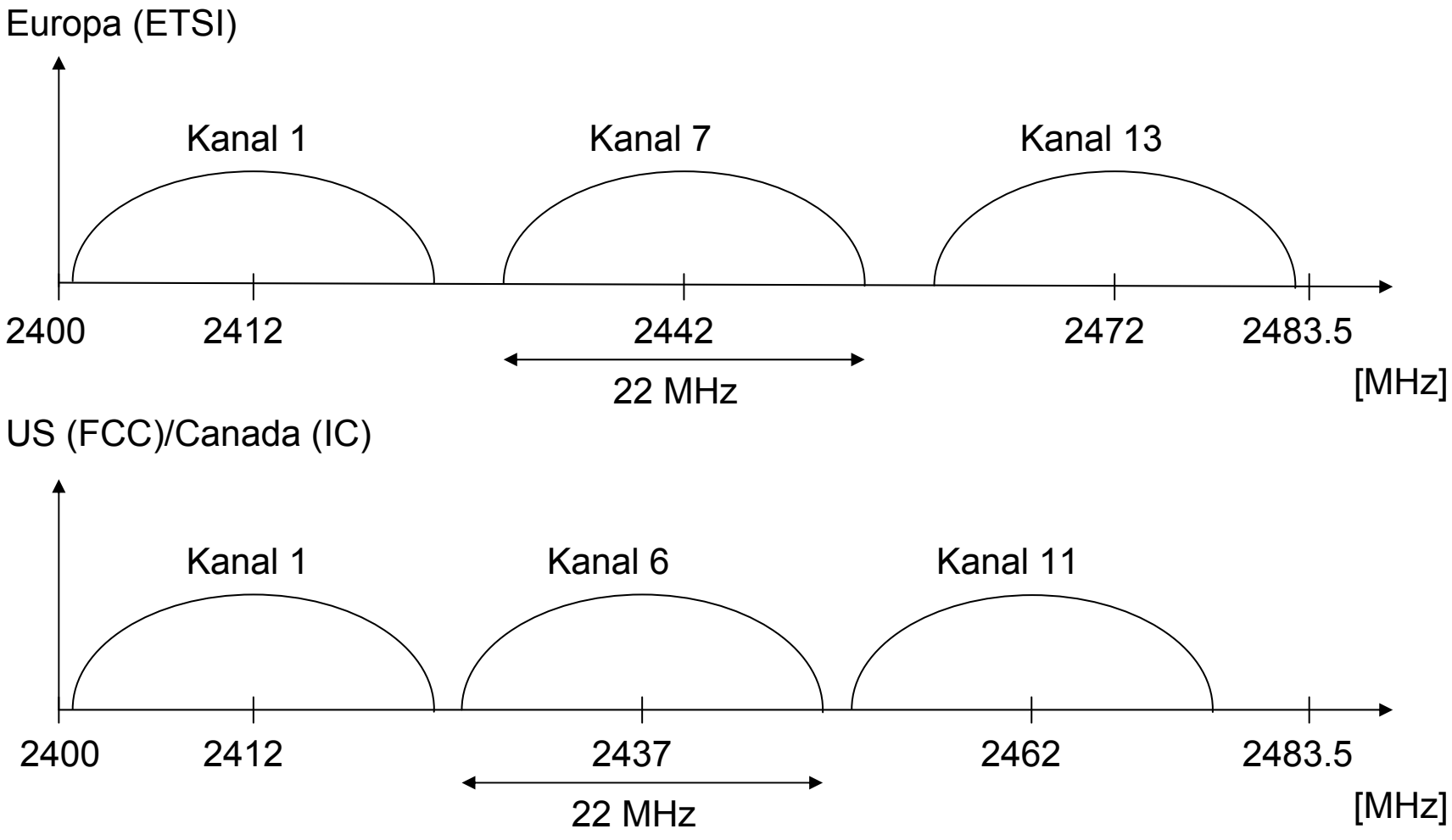
❑ Langes PLCP-PPDU-Format



❑ Kurzes PLCP-PPDU-Format (optional)



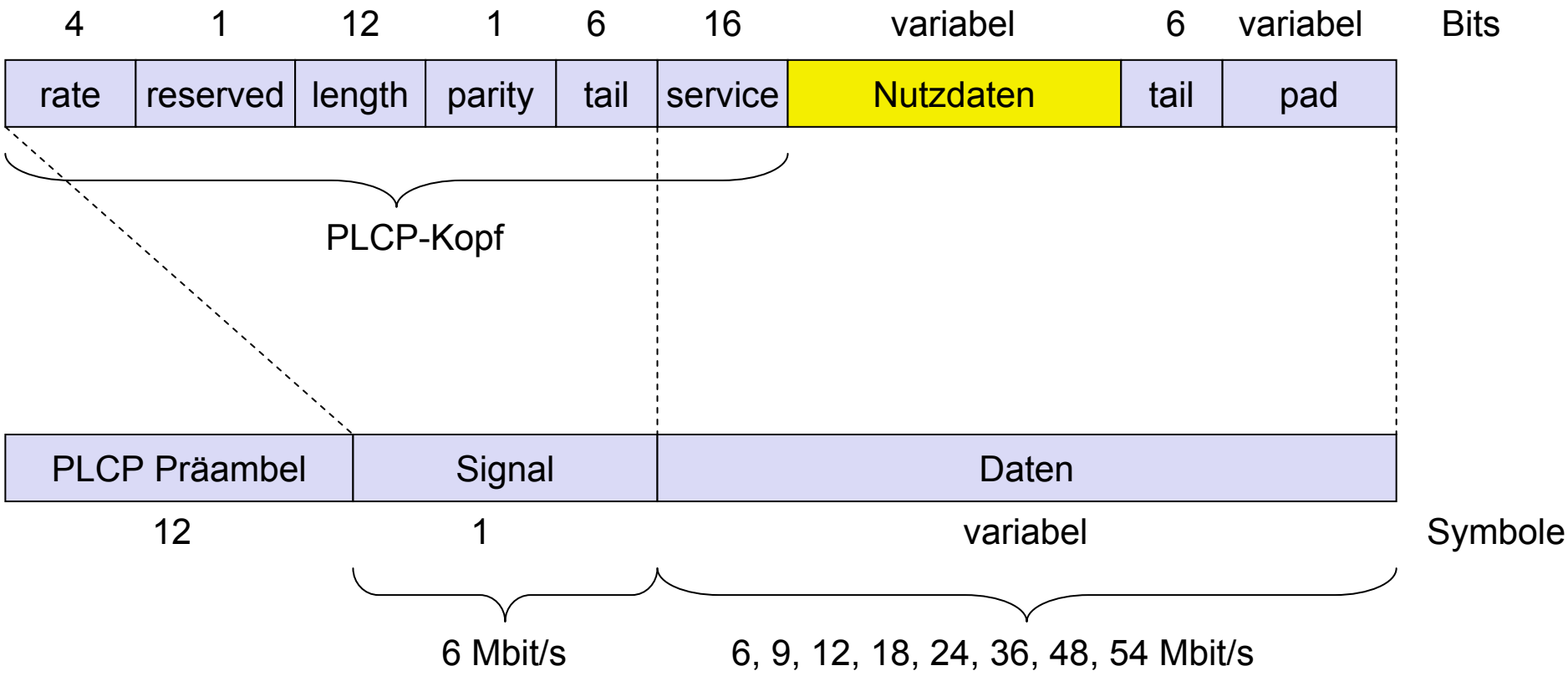
3.3.1.5.1 Nicht überlappende Kanalwahl



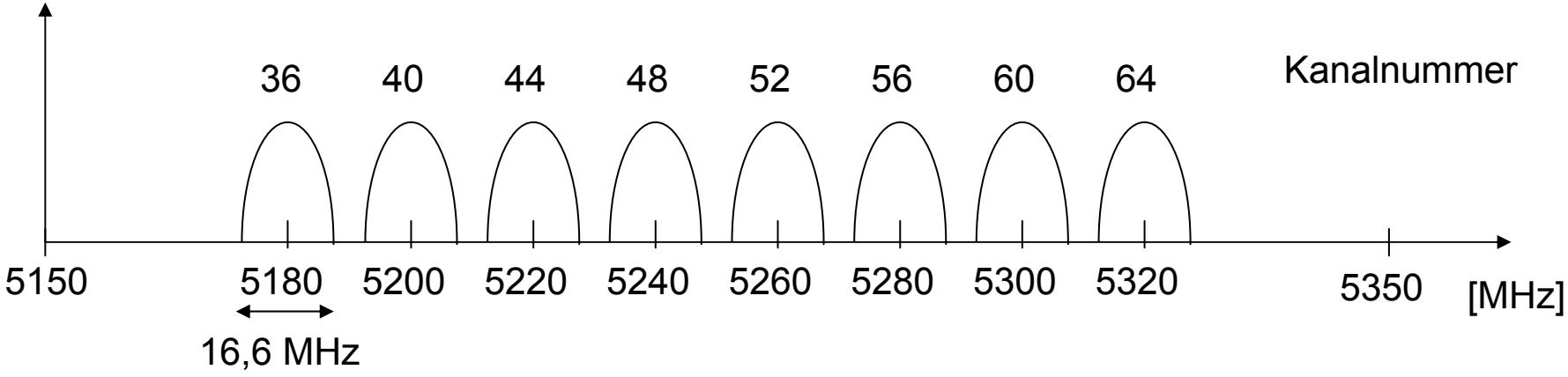
3.3.1.5.2 IEEE 802.11a

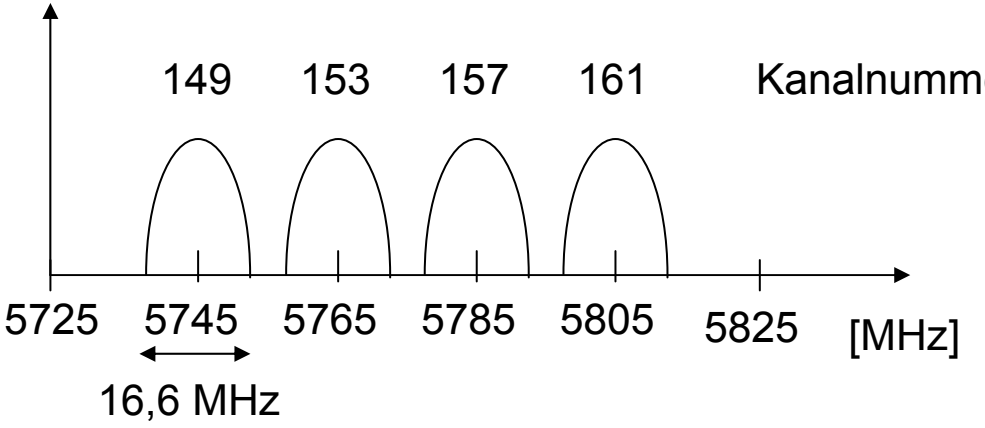
- **Datenraten**
  - **6, 9, 12, 18, 24, 36, 48, 54 Mbit/s,** abhängig von SNR
  - Nutzdatenrate **(1500 byte Pakete): 5,3 (6), 18 (24), 24 (36), 32 (54)**
  - **6, 12, 24 Mbit/s verpflichtend**
- **Kommunikationsbereich**
  - **100m Außen-, 10m Innenbereich**
    - **E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m**
- **Frequenzbereich**
  - **Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band**
- **Sicherheit**
  - **Begrenzt, WEP unsicher, SSID**
- **Kosten**
  - **280€ Adapter, 500€ Z**ugangspunkt
- **Verfügbarkeit**
  - **Einige Produkte, einige Firmen**
- **Verbindungsaufbaudauer**
  - **Verbindungslos, „always on“**
- **Dienstgüte**
  - **Typ. Best effort, keine Garantien (wie alle anderen 802.11 Produkte)**
- **Verwaltbarkeit**
  - **Begrenzt (keine automatische Schlüsselverteilung, symmetrische Verschlüsselung)**
- **Spezielle Vor-/Nachteile**
  - **Vorteil: passt in das 802.x System, freies ISM-Band, verfügbar, einfach, nutzt das (noch) freiere 5 GHz Band**
  - **Nachteil: (noch) nicht in Europa zertifiziert, derzeit nur USA (Harmonisierung derzeit im Gange), stärkere Abschattung auf Grund der höheren Frequenz, keine Dienstgüte**

3.3.1.5.2 IEEE 802.11a: PHY-Rahmenformat



3.3.1.5.2 Nutzbare Kanäle für 802.11a / US U-NII

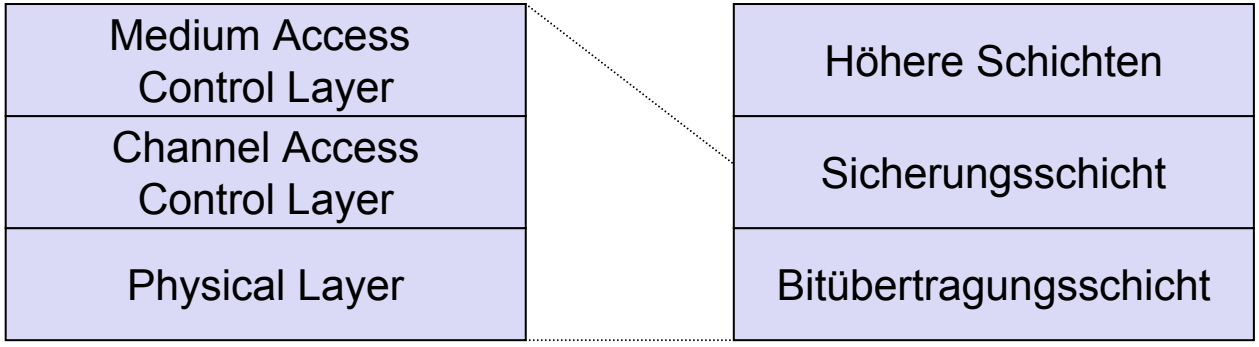




Mittenfrequenz =
5000 + 5*Kanalnummer [MHz]

3.3.2 ETSI - HIPERLAN

- **ETSI-Standard**
  - europäischer Standard, vgl. GSM, DECT, ...
  - Ergänzung lokaler Netze und Ankopplung an Festnetze
  - zeitkritische Dienste von Anfang an integriert
- **HIPERLAN-Familie**
  - ein Standard kann nicht alle Anforderungen abdecken
    - Reichweite, Bandbreite, Dienstgüteunterstützung
    - kommerzielle Rahmenbedingungen
  - HIPERLAN 1 1996 verabschiedet – keine Produkte!



3.3.2 Übersicht: ursprüngliche HIPERLAN-Familie

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Anwendung	drahtloses LAN	Zugang zu ATM-Festnetzen	funkbasierte Anschlußnetze	Punkt-zu-Punkt drahtlose ATM-Verbindungen
Frequenz	5,1-5,3GHz			17,2-17,3GHz
Topologie	dezentral ad-hoc/infrastruktur	zellular, zentral	Punkt-zu-Mehrpunkt	Punkt-zu-Punkt
Antenne	omnidirektional		direktional	
Reichweite	50m	50-100m	5000m	150m
Dienstgüte	statistisch	wie ATM-Festnetze (VBR, CBR, ABR, UBR)		
Mobilität	<10m/s		quasistationär	
Schnittstelle	konventionelle LAN	ATM-Netze		
Datenrate	23,5Mbit/s	>20Mbit/s		155Mbit/s
Energiespar-maßnahmen	ja		nicht zwingend	

HIPERLAN 1 erreichte nie richtigen Produktstatus,
die anderen Standards wurden umbenannt und modifiziert!

3.3.3 Wireless LAN: Komponenten

Wireless USB-Adapter

WLAN-Karte

Access Point für 802.11b

Access Point mit Routing-Funktionen

Access Point mit Zusatzfunktionen

Access Point für 802.11g

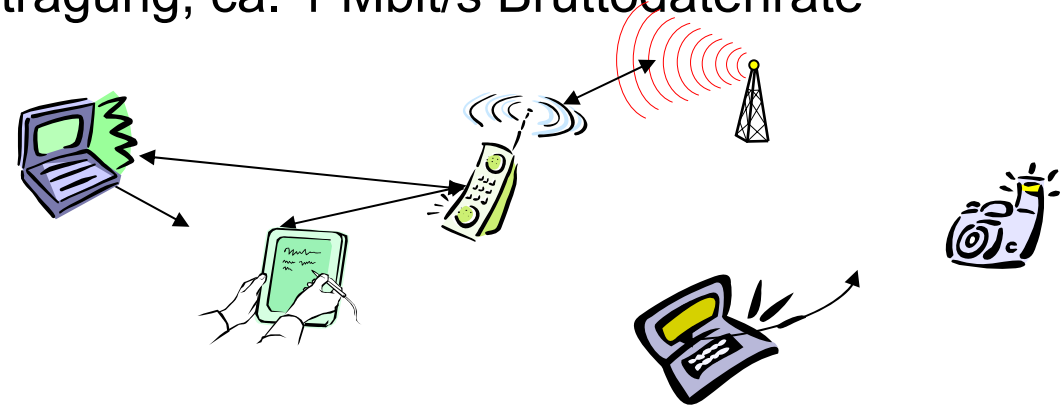
3.4 Bluetooth

- 3.4.1 Eigenschaften
- 3.4.2 Netztopologien
- 3.4.3 Technologie
- 3.4.4 Komponenten
- 3.4.5 Weiterentwicklungen

3.4 Bluetooth - IEEE 802.15 (1)

- **Idee**
  - Universelles Funksystem für drahtlose Ad-hoc-Verbindungen
  - Verknüpfung von Computer mit Peripherie, tragbaren Geräten, PDAs, Handys – im Wesentlichen ein leistungsfähigerer IrDA-Ersatz
  - Eingebettet in andere Geräte, Ziel: 5€/Gerät (2002: 50€/USB Bluetooth)
  - Kleine Reichweite (10 m), niedrige Leistungsaufnahme, lizenzfrei im 2,45 GHz-ISM-Band
  - Sprach- und Datenübertragung, ca. 1 Mbit/s Bruttodatenrate

Eines der ersten Module (Ericsson).



3.4 Bluetooth - IEEE 802.15 (2)

- **Geschichte**
  - 1994: Ericsson (Mattison/Haartsen), “MC-link”-Projekt
  - Umbenennung des Projekts: Bluetooth nach Harald “Blåtand” Gormsen [Sohn des Gorm], König von Dänemark im 10. Jahrhundert
  - 1998: Gründung der Bluetooth SIG, www.bluetooth.org
  - 1999: Errichtung eines Runsteins durch Ercisson/Lund ;-)
  - 2001: Erste Produkte für den Massenmarkt, Verabschiedung des Standards 1.1

(früher: Bluetooth)

Bluetooth™

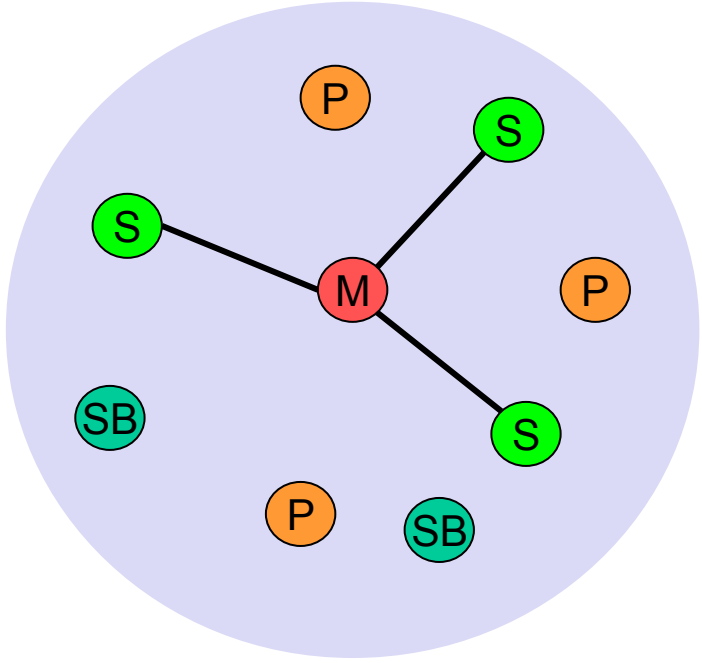
- **Special Interest Group**
  - Gründungsmitglieder: Ericsson, Intel, IBM, Nokia, Toshiba, später hinzugekommene Förderer: 3Com, Agere (früher: Lucent), Microsoft, Motorola; über 2500 Mitglieder
  - Gemeinsame Spezifikation und Zertifizierung von Produkten
- **IEEE 802.11 – Konkurrenz, erster PAN-Standard 802.15.1 genehmigt**

3.4.1 Eigenschaften

- **2.4 GHz ISM Band, 79 (23) RF Kanäle, 1 MHz Trägerabstand**
  - Kanal 0: 2402 MHz … Kanal 78: 2480 MHz
  - G-FSK Modulation, 1-100 mW Sendeleistung
- **FHSS und TDD**
  - Frequenzsprungverfahren mit 1600 Sprüngen/s
  - Sprungfolge pseudozufällig, vorgegeben durch einen Master
  - Time division duplex zur Richtungstrennung
- **Sprachverbindung – SCO (Synchronous Connection Oriented)**
  - FEC (forward error correction), keine Übertragungswiederholung, 64 kbit/s duplex, Punkt-zu-Punkt, leitungsvermittelt
- **Datenverbindung – ACL (Asynchronous ConnectionLess)**
  - Asynchron, schnelle Bestätigung, Punkt-zu-Mehrpunkt, bis zu 433,9 kbit/s symmetrisch oder 723,2/57,6 kbit/s asymmetrisch, paketvermittelt
- **Topologie**
  - Überlappende Pikonetze (Sterne) bilden ein „Scatternet“ (Streunetz)

3.4.2 Netztopologien: Pikonetze

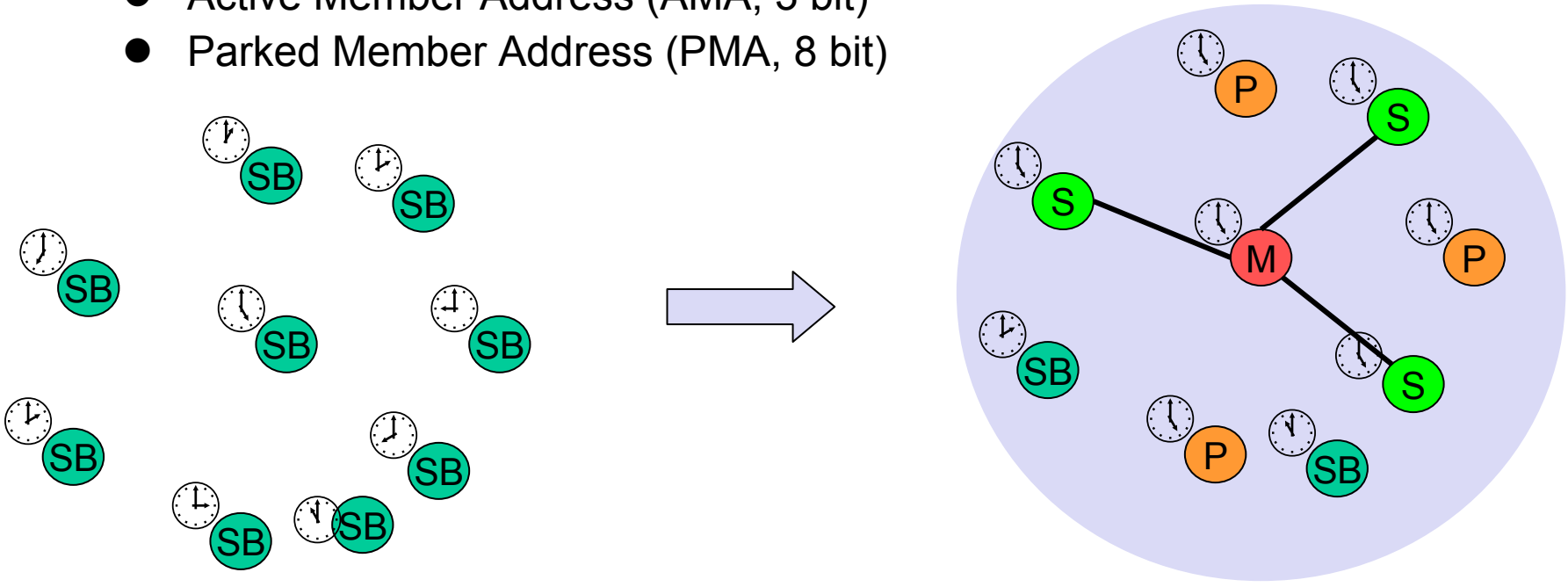
- Eine Ansammlung von Geräten welche spontan (ad-hoc) vernetzt wird
- Ein Gerät wird zum Master, die anderen verhalten sich als Slaves während der Lebensdauer des Pikonetzes
- Der Master bestimmt die Sprungfolge, die Slaves müssen sich darauf synchronisieren
- Jedes Pikonetz hat eine eindeutige Sprungfolge
- Teilnahme an einem Pikonetz = Synchronisation auf die Sprungfolge
- Jedes Pikonetz hat einen Master und gleichzeitig bis zu 7 Slaves (> 200 können „geparkt“ werden)



M=Master P=Parked
S=Slave SB=Standby

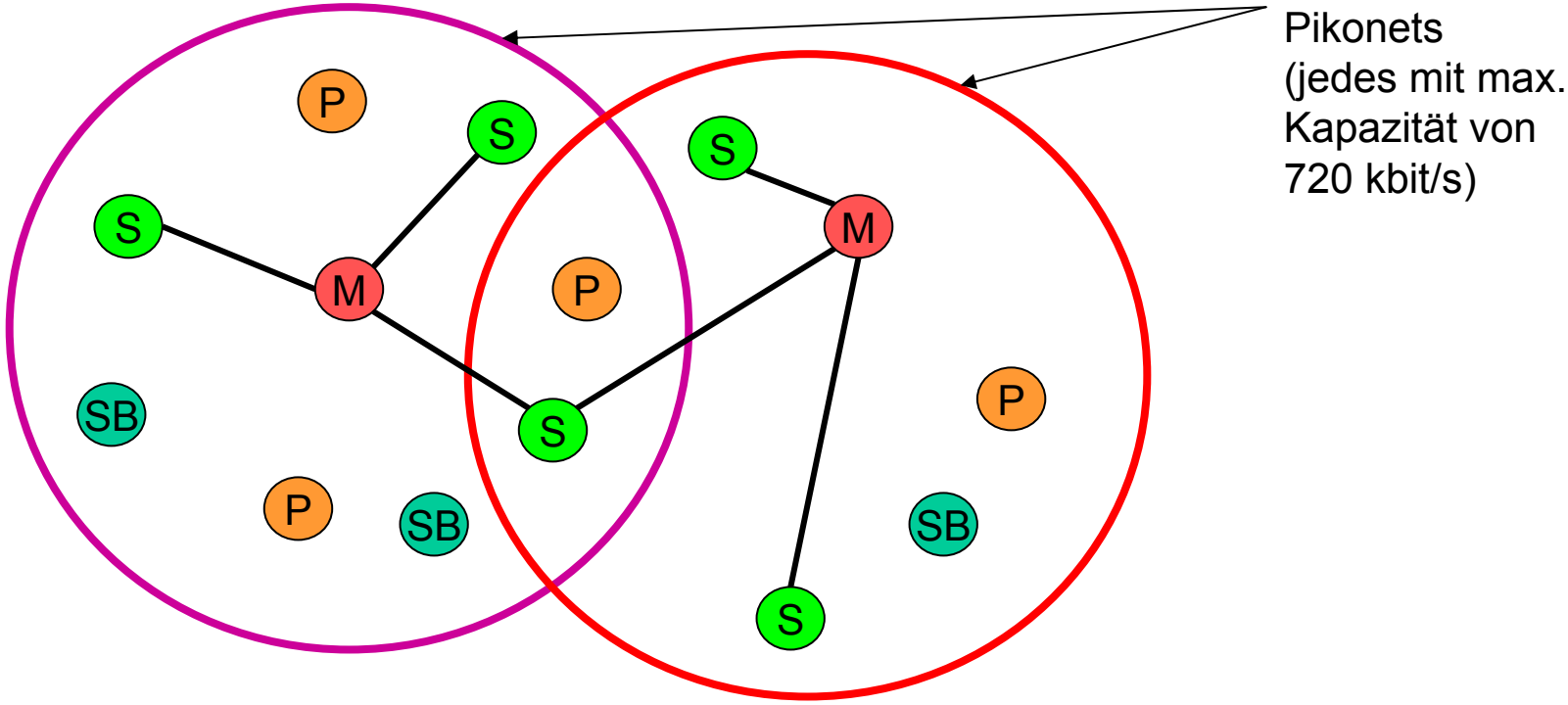
3.4.2 Netztopologien: Bildung eines Pikonetzes

- **Alle Geräte im Pikonetz springen synchron**
  - Der Master übergibt dem Slave seine Uhrzeit und Gerätekennung
    - **Sprungfolge: bestimmt durch die Gerätekennung (48 Bit, weltweit eindeutig)**
    - **Die Phase in der Sprungfolge wird durch die Uhrzeit bestimmt**
- **Adressierung**
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

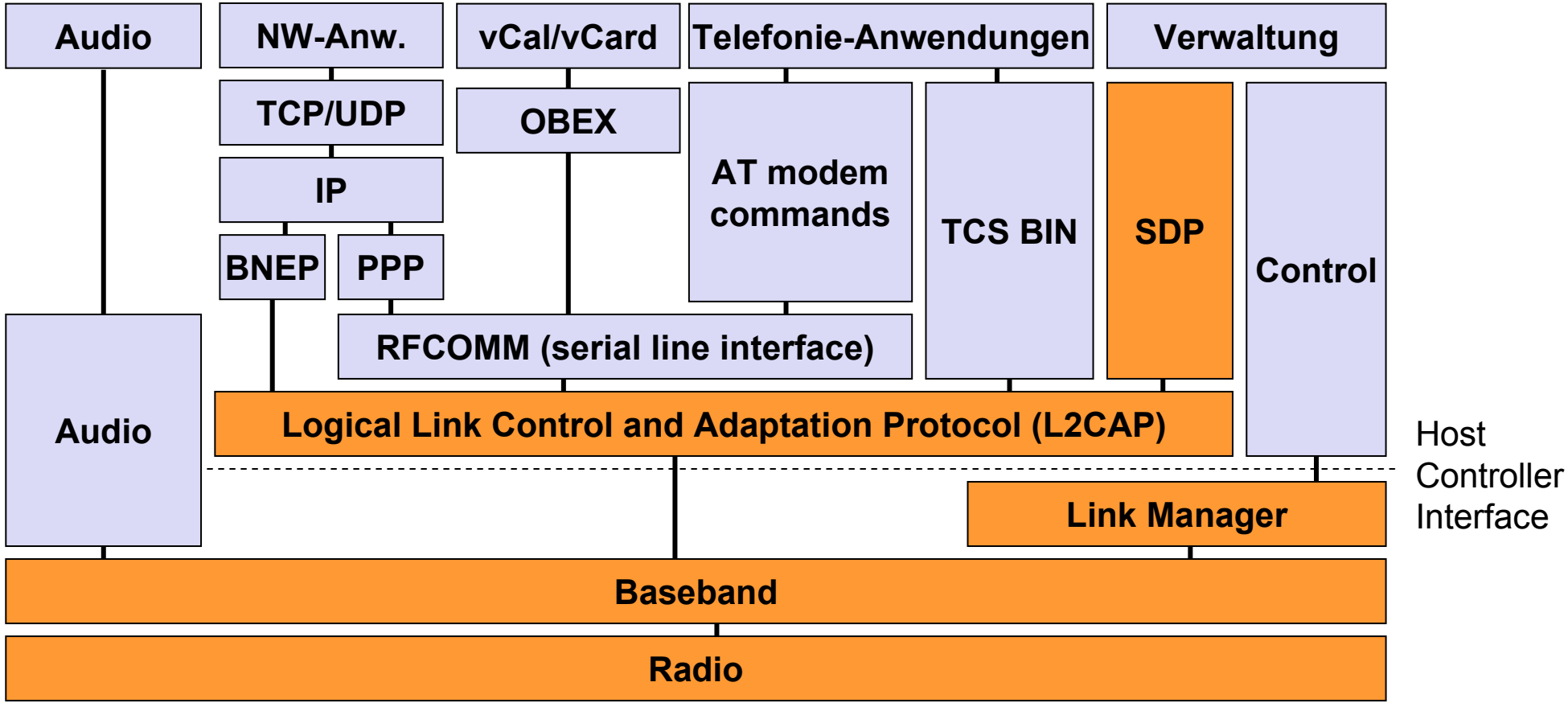


3.4.2 Netztopologien: Scatternet

- **Verbindung mehrerer räumlich naher Pikonetze durch gemeinsame Master- oder Slave-Geräte**
  - Geräte können Slaves in einem Pikonetz sein, Master in einem anderen
- **Kommunikation zwischen Pikonetzen**
  - Geräte, welche zwischen den Pikonetzen hin und her springen



3.4.3 Bluetooth Technologie: Protokolle (1)

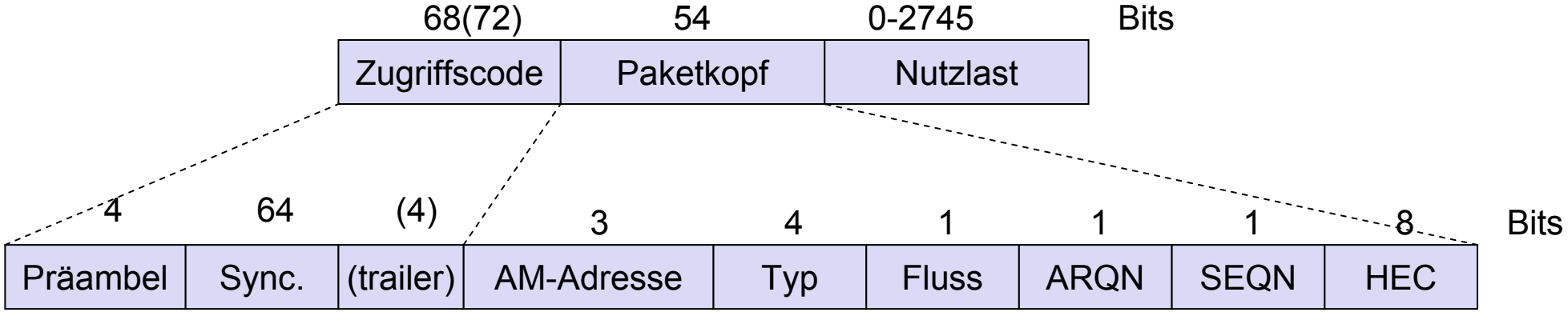


AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

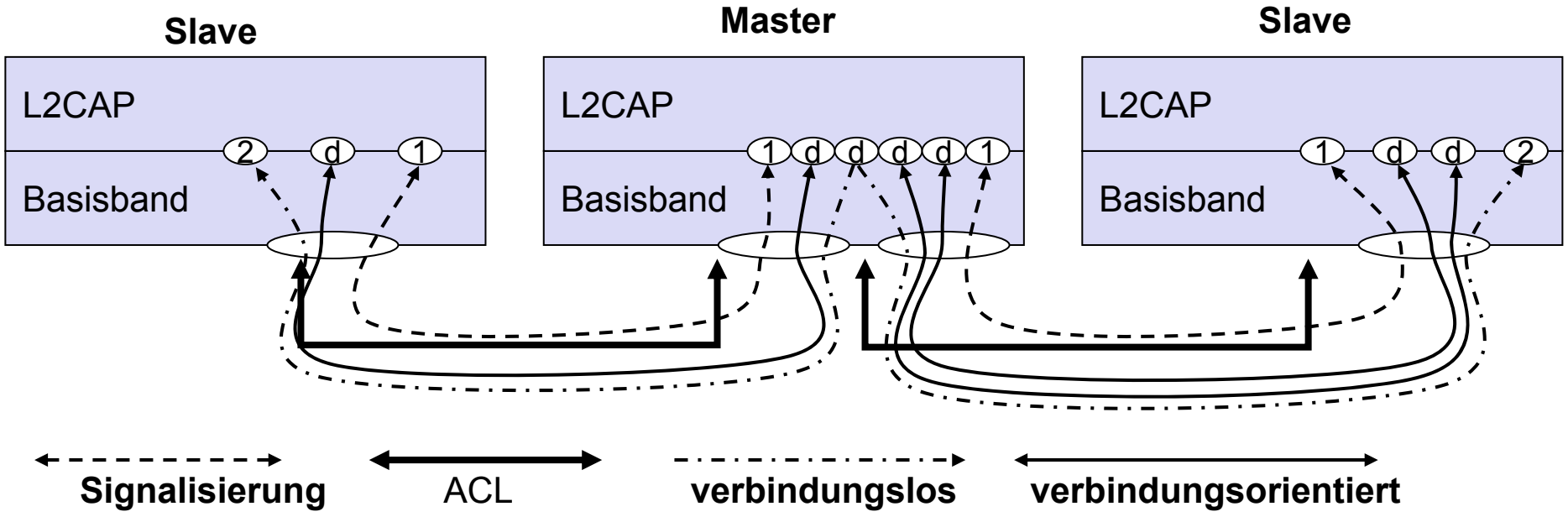
SDP: service discovery protocol
RFCOMM: radio frequency comm.

3.4.3 Bluetooth Technologie: Protokolle (2)

- **Pikonetz/Kanaldefinition**
- **PHY-Pakete**
  - Zugriffscode
    - Kanal, Gerätezugriff, z.B., vom Master abgeleitet
  - Paketkopf
    - 1/3-FEC, Active Member-Adresse (1 master, 7 slaves), Verbindungstyp, Alternating Bit ARQ/SEQ, Prüfsumme



3.4.3 Bluetooth Technologie: L2CAP – logische Kanäle

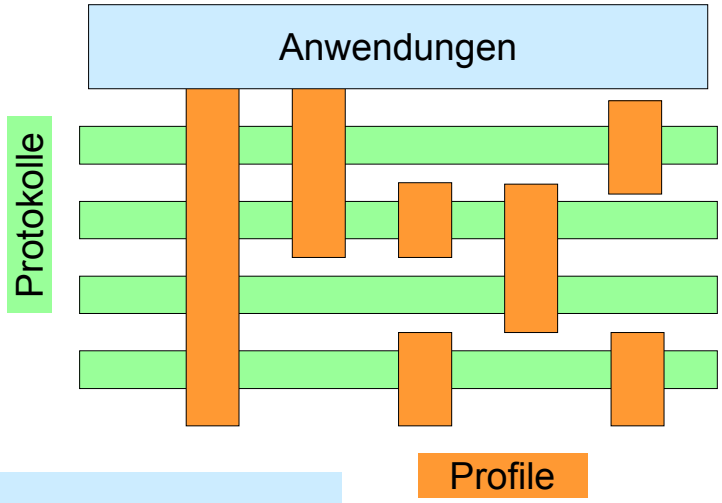


3.4.3 Bluetooth Technologie: SDP – Service Discovery Protocol

- **Protokoll zum Suchen und Erkennen von Diensten**
  - Suchen nach Diensten in Funkreichweite
  - Angepasst an das hochdynamische Umfeld
  - Kann durch weitere Protokolle wie z.B. SLP, Jini, Salutation, ... ergänzt werden
  - Definiert nur das Endecken, nicht die Nutzung von Diensten
  - Zwischenspeicherung bereits erkannter Dienste
  - Schrittweise Entdeckung
- **Dienstbeschreibung**
  - Informationen über Dienste durch Attribute dargestellt
  - Attribute bestehen aus einer 16-bit-Kennung (Name) und einem Wert
  - Kennungen können von 128 bit Universally Unique Identifiers (UUID) abgeleitet werden

3.4.3 Bluetooth Technologie: Profile

- **Stellen Standardlösungen für bestimmte Nutzungsszenarien dar**
  - Vertikaler Schnitt durch den Protokollstapel
  - Basis für Interoperabilität
- **Generic Access Profile**
- **Service Discovery Application Profile**
- **Cordless Telephony Profile**
- **Intercom Profile**
- **Serial Port Profile**
- **Headset Profile**
- **Dial-up Networking Profile**
- **Fax Profile**
- **LAN Access Profile**
- **Generic Object Exchange Profi**
- **Object Push Profile**
- **File Transfer Profile**
- **Synchronization Profile**

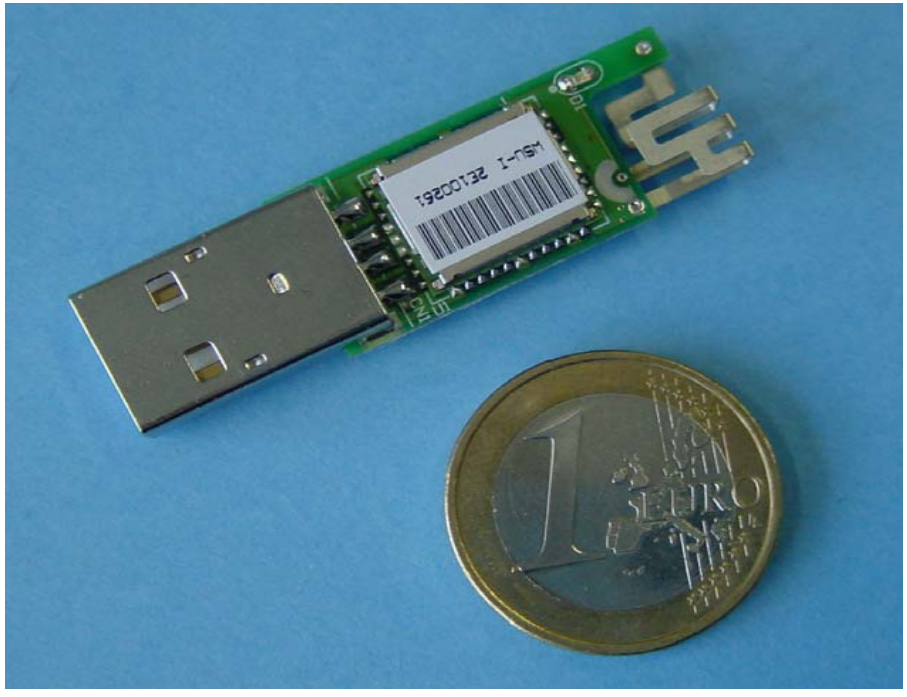


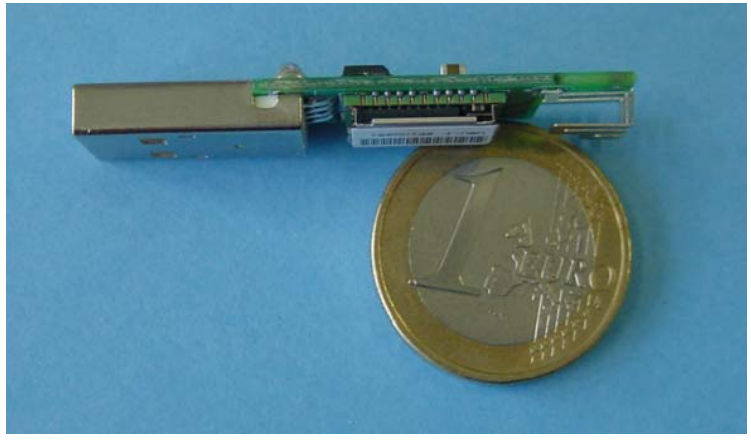
Weitere Profile
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

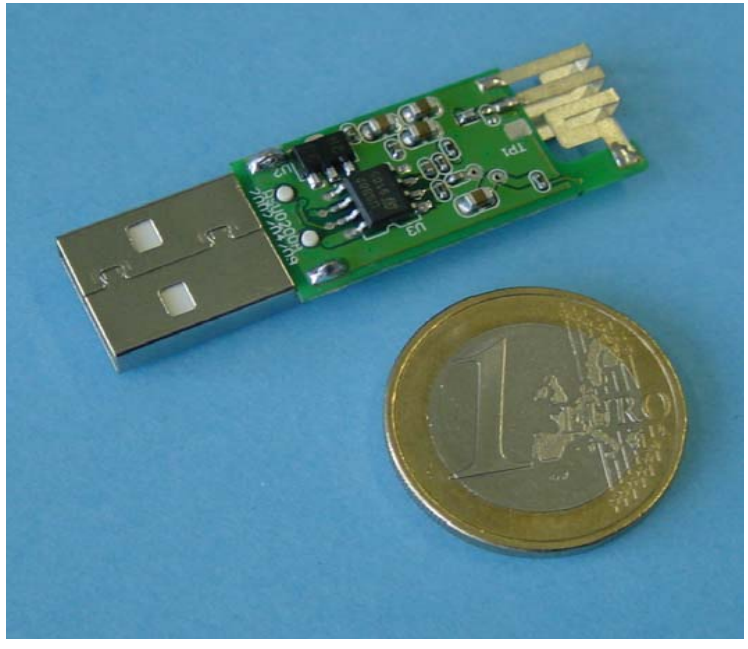
3.4.3 Bluetooth Technologie: Überblick

- Datenraten
  - Synchron, verbindungsorientiert: 64 kbit/s
  - Asynchron, verbindungslos
    - 433,9 kbit/s symmetrisch
    - 723,2 / 57,6 kbit/s asymmetrisch
- Reichweite
  - POS (Personal Operating Space) bis zu 10 m
  - Spezielle Sender bis zu 100 m
- Frequenz
  - Free 2.4 GHz ISM-band
- Sicherheit
  - Challenge/response (SAFER+), Sprungfolge
- Kosten
  - 50€ Adapter, fallen auf bis zu 5€
- Verfügbarkeit
  - Bereits in einige Produkten integriert, viele Anbieter
- Verbindungsaufbaudauer
  - Hängt von der Betriebsart ab
  - Max. 2,56 s, im Mittel 0,64 s
- Dienstgüte
  - Garantien, ARQ/FEC
- Verwaltbarkeit
  - Öffentliche/private Schlüssel benötigt, Schlüsselverwaltung nicht spezifiziert, einfache Systemintegration
- Vorteile/Nachteile
  - Vorteile: bereits in Produkte integriert, weltweit verfügbar, freies ISM-Band, diverse Anbieter, einfaches System, einfache spontane Kommunikation, Punkt-zu-Punkt
  - Nachteile: Interferenzen auf dem ISM-Band, eingeschränkte Reichweite, max. 8 Geräte pro Netz, hohe Verbindungsaufbauverzögerung

3.4.4 Bluetooth Komponenten (1)







3.4.4 Bluetooth Komponenten (2)

Bluetooth Tastatur und Maus

Stift mit Bluetooth

Bluetooth USB-Stick

Mobiltelefon mit Bluetooth

Bluetooth Headset

Bluetooth-Drucker Adapter

3.4.5 Weiterentwicklungen (1): WPAN - IEEE 802.15

- **802.15-2: Koexistenz**
  - Koexistenz von drahtlosen persönlichen Netzen (802.15) und drahtlosen lokalen Netzen (802.11), Beschreibung der Störungen
- **802.15-3: Höhere Datenraten**
  - Standard für WPANs mit höheren Datenraten (20 Mbit/s or mehr), aber immer noch billig und niedrige Leistungsaufnahme
  - Datenraten: 11, 22, 33, 44, 55 Mbit/s
  - Dienstgüte: isochrones Protokoll
  - Ad hoc peer-to-peer Netze
  - Sicherheit
  - Batteriebetrieb muss möglich sein
  - Billig, einfach, ...
  - Speziell ausgerichtet, um den wachsenden Bedarf im Bereich der Bildübertragung, Multimedia-Datenübertragung im Konsumerbereich abzudecken

3.4.5 Weiterentwicklungen (2): WPAN - IEEE 802.15

- **802.15-4: Niedrige Datenraten und sehr niedrige Leistungsaufnahme**
  - Lösung für niedrige Datenraten, Batterielebensdauern von Monaten bis zu Jahren, sehr geringe Komplexität
  - Mögliche Anwendungen: Sensoren, interaktive Spielzeuge, Fernsteuerungen, Heimautomatisierung, ...
  - Datenraten 2-250 KBit/s, Latenz bis hinunter zu 15 ms
  - Master-Slave oder Peer-to-Peer Betrieb
  - Bis zu 254 Geräten oder 64516 Verteilknoten
  - Unterstützung für verzögerungskritische Geräte, z.B. Joysticks
  - CSMA/CA Medienzugriff (datenzentriert) mit/ohne Zeitschlitze
  - Automatischer Netzaufbau durch einen Koordinator
  - Dynamische Geräteadressierung
  - Hohe Übertragungszuverlässigkeit durch Bestätigungen
  - Gezielte Leistungssteuerung um eine geringe Aufnahme sicher zu stellen
  - 16 Kanäle im 2,4-GHz-ISM-Band, 10 Kanäle im 915-MHz-US-ISM-Band und ein Kanal im europäischen 868-MHz-Band

3.5 Power over Ethernet (PoE)

- 3.5.1 Systemaufbau
- 3.5.2 PoE-Technik
- 3.5.3 Einschränkungen
- 3.5.4 Komponenten
- 3.5.5 PoE vs. Powerline

3.5 Power over Ethernet (PoE): IEEE 802.3af

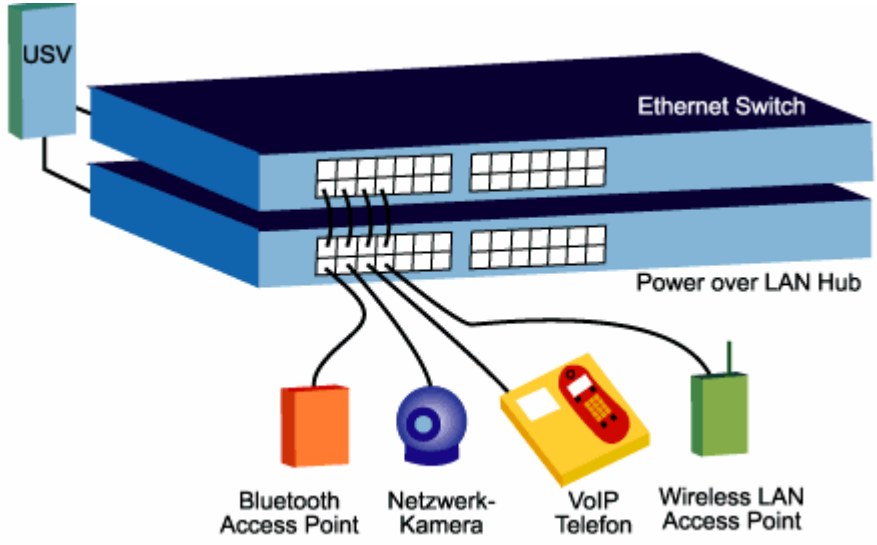
- **Grundidee:**
  - Geräte in lokalen Netzen könnten ihren Strom auch über die Netzkabel (Twisted Pair) beziehen
  - Kabel für die Stromversorgung könnten eingespart werden
- **Einsatzgebiete**
  - Consumer (Netz-Kameras, Lautsprecher usw.)
  - Access Points für drahtlose Netze (WLAN oder Bluetooth)
  - Kommunikation, wobei VoIP-Geräte besonders profitieren können
  - Industrie (Embedded Internet, intelligente Sensoren/Aktoren)
  - Weltweit genormte Stromversorgung

- **Bisher:**
  - Proprietäre Lösungen von einigen Herstellern ohne große Verbreitung -> Gefahr eine alte Komponente durch die Stromzufuhr zu beschädigen
- **1999: Bildung einer Task Force in der IEEE-Arbeitsgruppe 802**
- **Seit Juli 2003: IEEE Standard 802.3af**

3.5 Power over Ethernet (PoE): IEEE 802.3af

- **Alternative Bezeichnungen:**
  - Power over LAN (PoL) oder Active Ethernet
- **Idee nicht neu: Problemstellungen**
  - Es existieren proprietäre Lösungen bereits auf den Markt
  - Jedoch mangelnde Kompatibilität und Interoperabilität
    - ➔ keine allzu große Verbreitung
    - ➔ Gefahr, Komponenten durch Verschaltung mit inkompatiblem Equipment zu beschädigen
- **Kompatibilität von PoE-Geräten**
  - getestet vom **Power over Ethernet Consortium am Interoperability Lab (IOL)** der Universität von New Hampshire

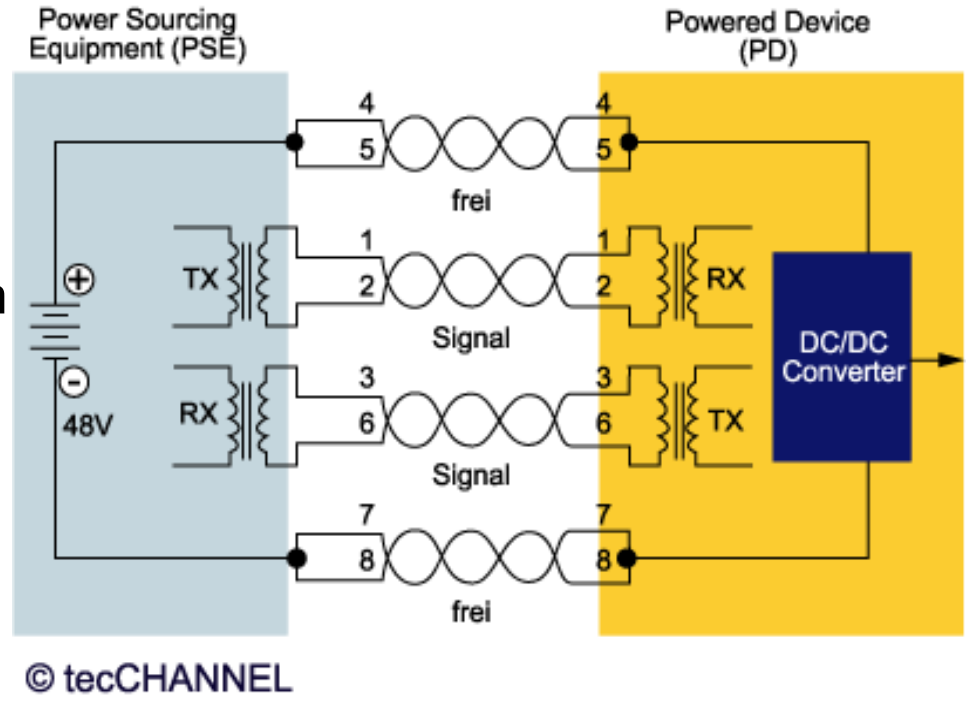
- **IEEE 802.3af unterscheidet zwischen zwei Basiskomponenten:**
  - Powered Devices (PD): Energieverbraucher; müssen den „DTE Power via MDI“-Modus unterstützen
  - Power Sourcing Equipment (PSE): Energieversorger; aktive Netzkomponenten mit direktem PoE-Support oder Patchfelder mit „DTE Power via MDI“-Unterstützung in Frage; Unterscheidung nach der Stromeinspeisung
    - Endspan Insertion: aktive Komponenten (meist Switches), die Netzgeräte über Ethernet direkt mit Strom versorgen
    - Midspan Insertion: Zwischenschaltung eines Power-Hubs (siehe rechts)



3.5.2 Technik allgemein

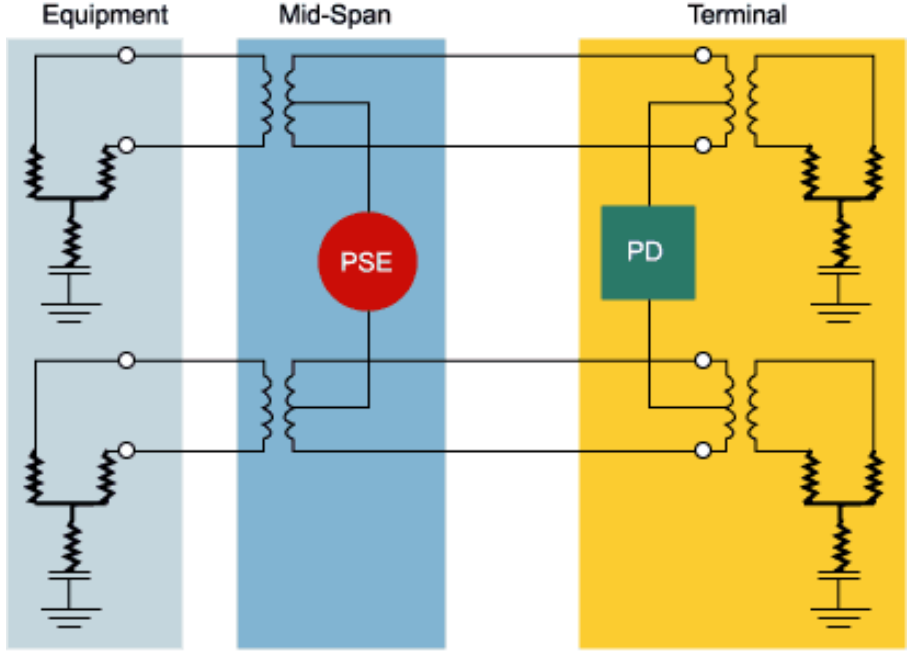
❑ Eckdaten

- Gleichspannung von 48 V
- Maximale Übertragungsstrecke 100 m
- Stromaufnahme im Dauerbetrieb maximal 350 mA
- Maximale Einspeiseleistung 15,4 Watt
- Maximale Leistungsaufnahme eines Endgerätes 13 Watt (nach Abzug der Leitungsverluste)
- Während einer Startphase von 100 ms darf ein Gerät auch bis zu 500 mA abnehmen
- Stromversorgung erfolgt über normale Kat3 oder Kat5-Kabel, Standard-RJ45-Stecker (möglich, da von 4 Kabeln nur 2 für die Signalübertragung verwendet werden)



3.5.2 Technik: Strom über Signalleitungen

- **Alternative:**
  - Strom bei Bedarf auch über die Signalleitungen (TX/RX) transportieren (so genannte „Phantom-Einspeisung“)
  - PoE nutzt die Tatsache, dass Ethernet-Transceiver über Übertrager angeschlossen sind, an denen die Ein- und Auskopplung des Gleichstroms erfolgen kann
  - eignet sich speziell für Installationen, bei denen die anderen zwei Adernpaare für zusätzliche Anwendungen wie etwa ISDN
  - auch GBit-Ethernet belegt alle acht Adern



© tecCHANNEL

3.5.2 Technik: Schutz der Geräte

- **Zentrale Aufgabe der Standardisierung**
  - Verhinderung von Schäden an nicht PoE-fähigen Endgeräten -> automatische Erkennung der angeschlossenen Endgeräte
    - Nicht PoE-fähige Endgeräte dürfen bei Anschluss an PoE keine Schäden erleiden
    - PoE-Geräte müssen schon vor dem Einschalten mitteilen, dass sie eine Stromversorgung benötigen
    - In beiden Fällen dürfen auch Fehlkonfigurationen nicht zu Schäden führen
- **Verfahren: Resistive Power Discovery**
  - Der Energieversorger (PSE) prüft das Endgerät (PD) auf Kompatibilität, bevor der Strom angelegt wird
  - Hierzu werden periodisch minimale Ströme erzeugt und so erkannt, ob das Gerät einen 25-kOhm-Abschlusswiderstand enthält
  - Ist dies der Fall kann die Stromversorgung über das Netz erfolgen

3.5.3 Einschränkungen

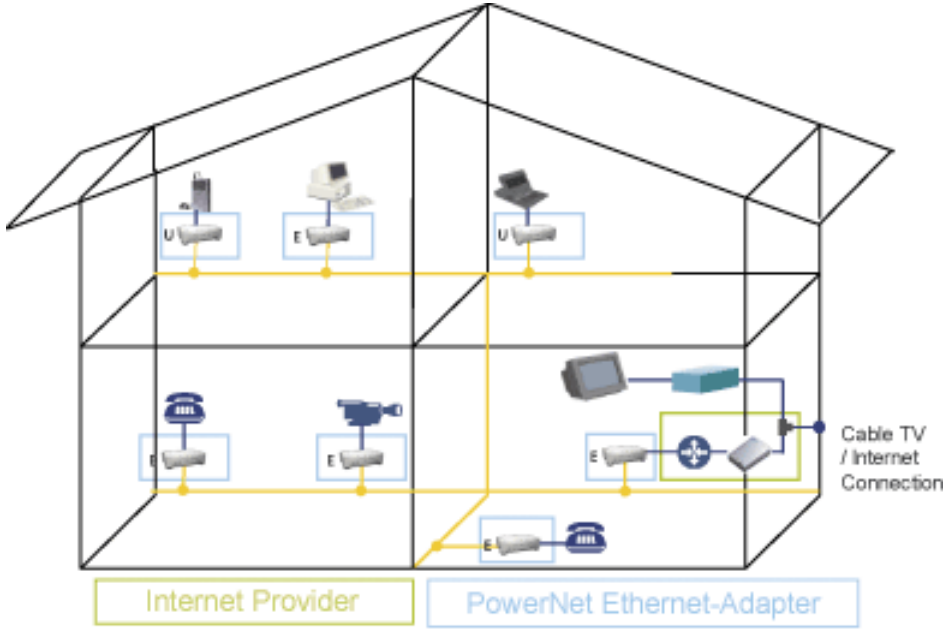
- **Einsatz mit 10- und 100-MBit/s-Ethernet**
  - GBit-Ethernet verwendet alle vier Adernpaare zur Übertragung, hier wäre jedoch eine Energieversorgung über die Signalleitungen möglich (aber Stromversorgung führt zu zusätzlichen Störsignalen auf den Signalleitungen)
- **SNMP-Schnittstelle fehlt bis dato**
  - 802.3af regelt lediglich die Implementation, nicht aber das Management.
  - IEEE und IETF arbeiten dem Vernehmen nach bereits zusammen an einem entsprechenden PoE-MIB-Modul

3.5.4 Komponentenbeispiele

Summit 300-48

3.5.5 PoE vs. Powerline

- **Powerline (LAN aus der Steckdose)**
  - ist eine Technik, mit der Sprache, Daten und Bewegtbild über das Stromnetz übertragen werden können
  - Diese Technik kann im Anschlussbereich zur Überbrückung der letzten Meile und für die In-House-Vernetzung eingesetzt werden

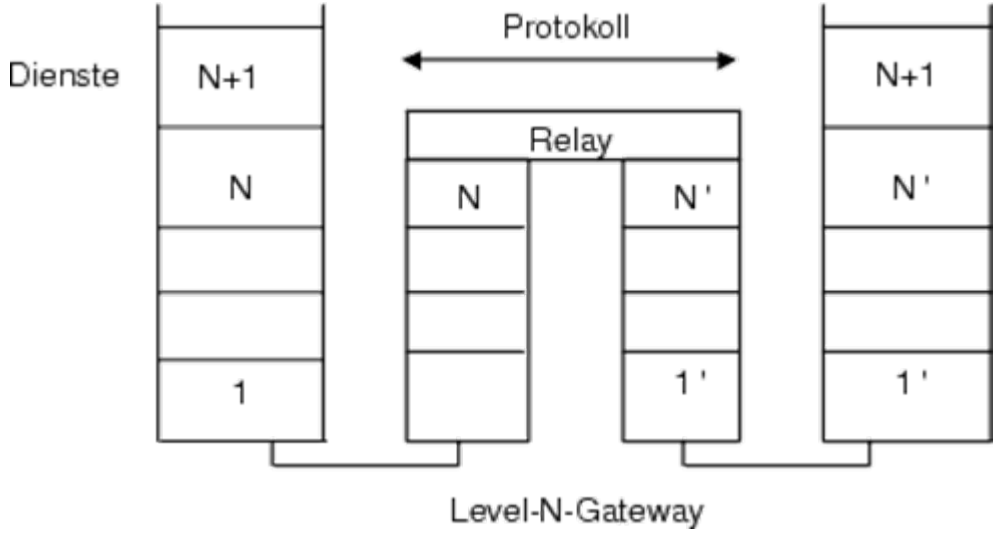


3.6. LAN-Verbundkomponenten

- 3.6.1 Generelle Kopplungsmöglichkeiten
- 3.6.2 Gateways
- 3.6.3 Repeater
- 3.6.4 Hubs
- 3.6.5 Bridges
- 3.6.6 Verknüpfung unterschiedlicher LAN-Typen
- 3.6.7 Transparente Bridges
- 3.6.8 Spanning-Tree-Algorithmus für Bridges

3.6 LAN-Verbundkomponenten: Einführung

- **Problemstellungen: Längenbeschränkungen von LAN-Segmenten**
  - Ethernet-Segmente dürfen höchstens 500 m bei Standard-Koaxialkabel lang sein (wegen Dämpfung)
    - ➢ Einfügung eines Repeaters zur Signalverstärkung (Schicht 1)
- **Notwendig:**
  - Kopplung von LANs
- **Gateway: allgemeiner Begriff für eine Kopplung auf Schicht *N***



3.6.1 Generelle Kopplungsmöglichkeiten (1)

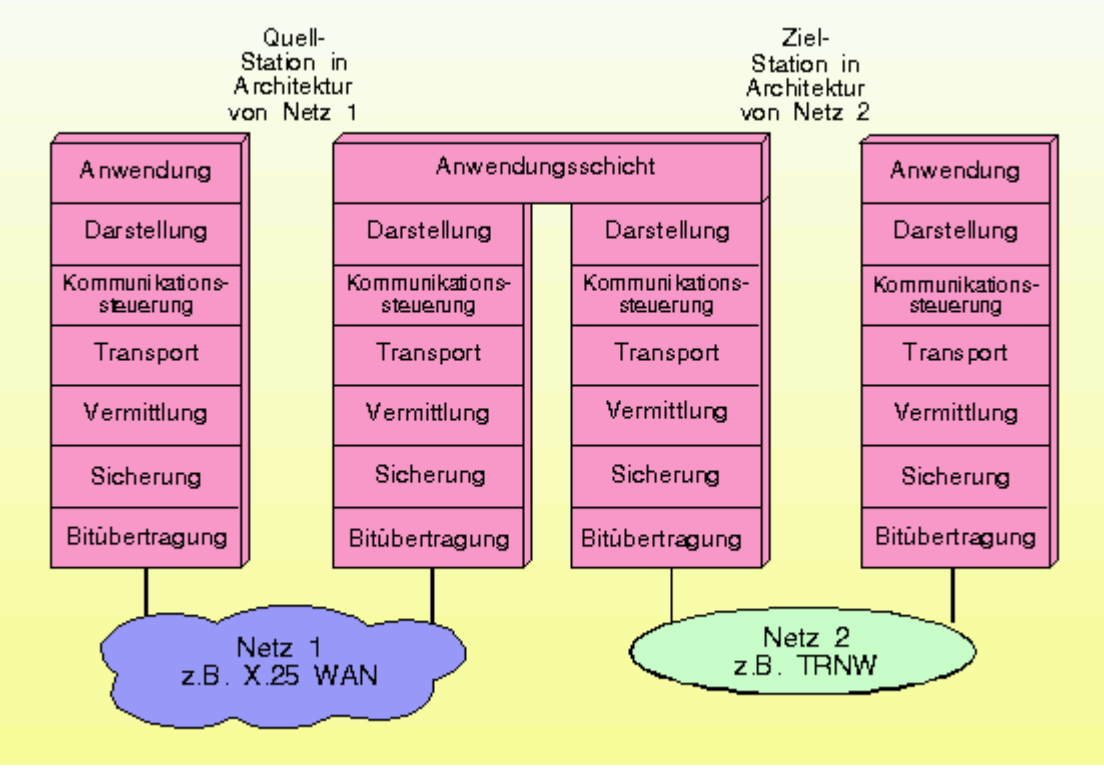
- **Kopplung entsprechend der Ebenen**
  - **Physical Layer**: **Repeater** (bitserielle Weitergabe), Hubs (Multiport-Repeater mit Medienanpassung)
  - **Data Link Layer: Bridges** (Store-and-Forward auf Frame-Ebene, benützt zusätzliche Informationen über Netztopologie), ferner **Switch**
  - **Network Layer**: **Router** (benutzt IP-Protokolle)

3.6.1 Generelle Kopplungsmöglichkeiten (2)

	Repeater/Hub	Bridges/Switch	Router/Switch
OSI/ISO-Layer	Physical	Data Link	Network
Store-and-Forward	Bits	Frames	Messages
Adressierung	keine	MAC-Adresse/Port	Internet-Adresse
Netzerweiterung	nein	ja	ja
Filter	nein	ja	ja
Durchsatz	hoch	mittel	geringer
Kosten	gering	mittel	mittel
Entfernung	beschränkt	beliebig	beliebig
Medienanpassung	nein/ja	ja	ja

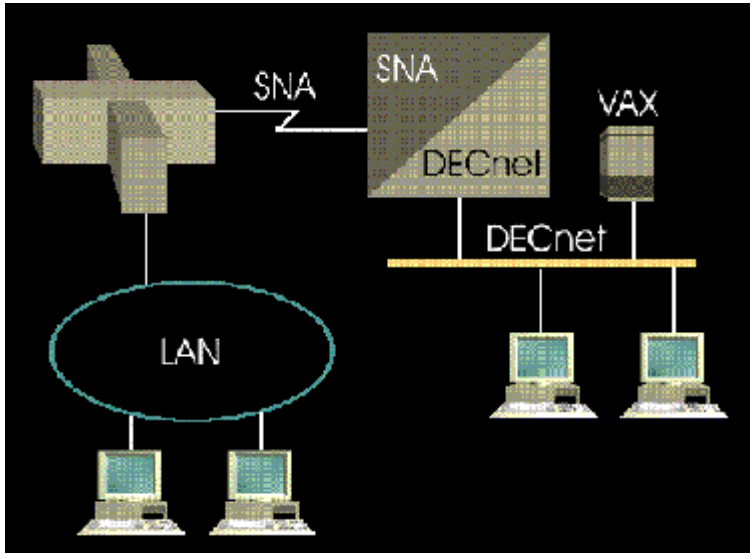
3.6.2 Gateways (1)

- **Eigenschaften:**
  - Schnittstellenkomponente zwischen gekoppelten Netzen
- **Aufgaben eines Gateways**
  - Adressierung über Netzgrenzen und Adress-abbildung
  - Abbilden unterschiedlicher Wegewahlstrategien in Teilnetzen auf (globale) Wegewahl
  - Anpassen der Nachrichten bzgl. Format, Länge, Reihenfolge
  - Anpassung von Netzzugangsmechanismen
  - Abstimmung von Protokollparametern (Fenstergrößen, Timeouts)
  - Anpassung von Flusssteuerungsmechanismen, Fehlermeldemechanismen
  - Abbildung von Diensten (z.B. verbindungsorientiert -> verbindungslos) und deren Dienstgüteparametern



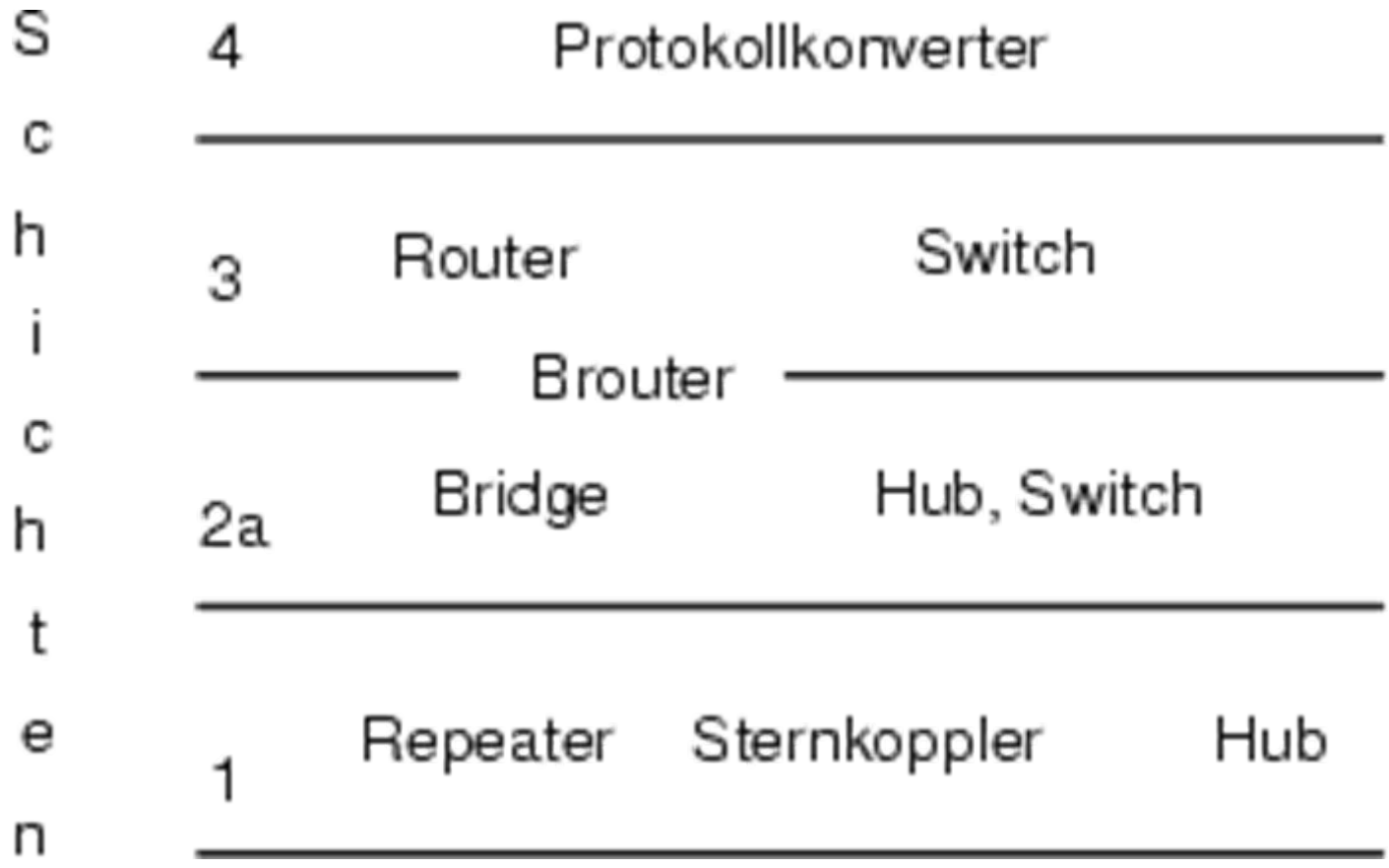
3.6.2 Gateways (2)

- **Umfang der unterstützten Funktionen eines Gateways ist abhängig von der Schicht des Gateways**
- **Beispiel: Gateways zwischen unterschiedlichen Netzarchitekturen**
- **Folgende LAN-Kopplungen sind denkbar (LANx und LANy sind unterschiedliche LANs u.U. sogar unterschiedliche LAN-Typen):**
  - LANx – GW – LANx
  - LANx – GW – LANy
  - LANx – GW – WAN – GW – LANx
  - LANx - GW – WAN – GW – LANy



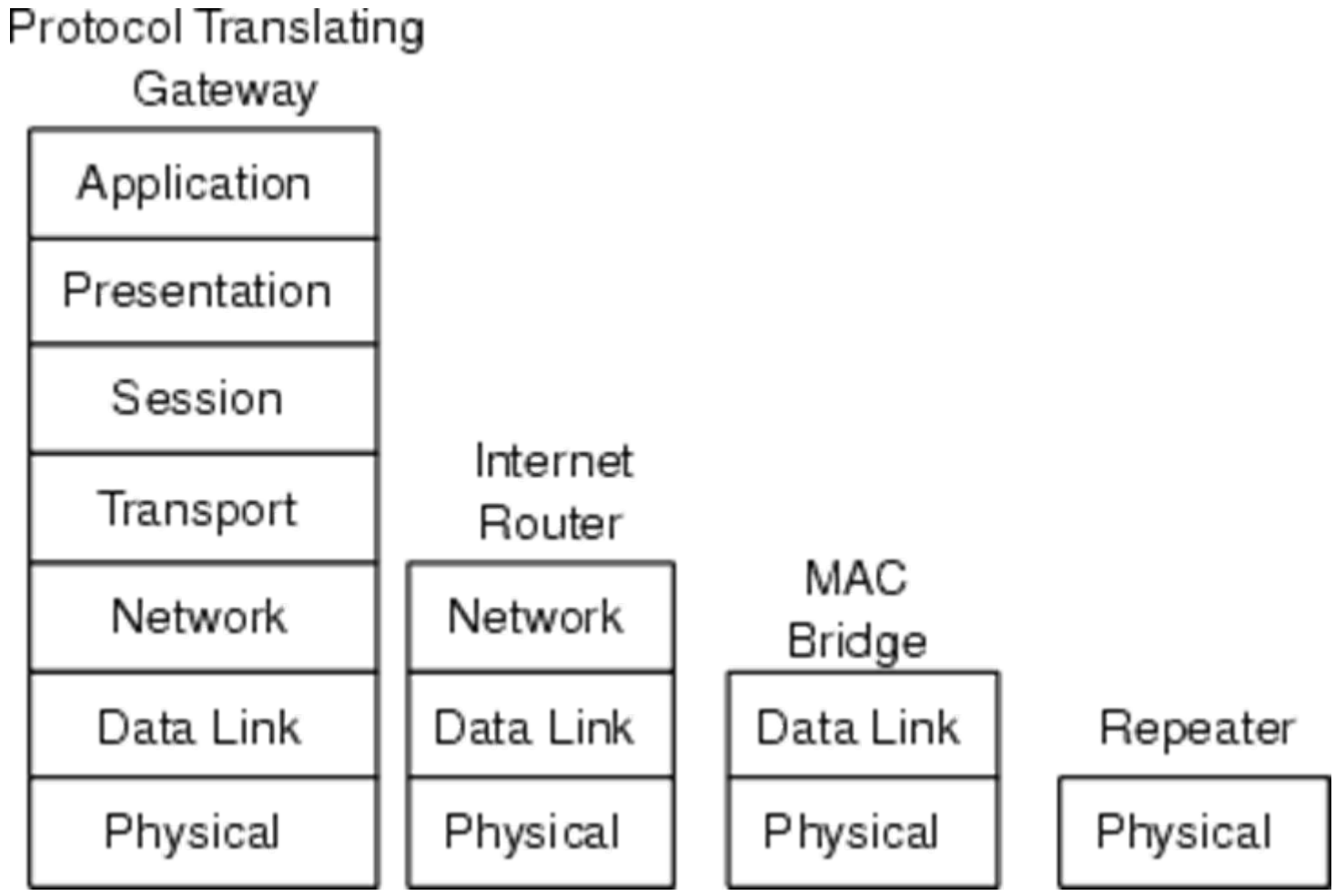
3.6.2 Gateways (3)

- **Klassifizierung der Schicht-N-Gateway nach dem ISO/OSI-Modell**



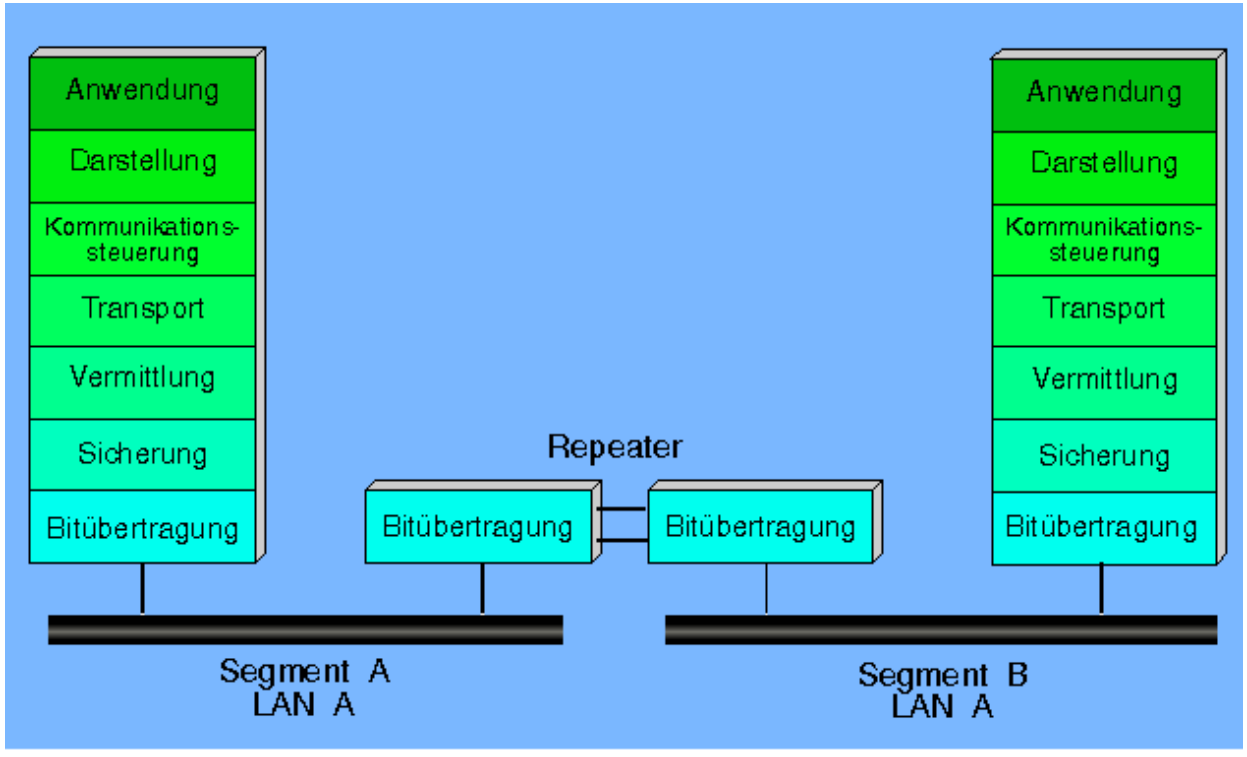
3.6.3 Gateways (4)

- **Ebenen der verschiedenen Gateways**



3.6.3 Repeater (1)

- Repeater verknüpfen LAN-Segmente zu einem größeren LAN
- Verstärken die elektrischen Signale (entspricht Physical Layer Relay)
- Weiterleiten der Signale an alle Segmente (Frame gelangt ins gesamte LAN, auch wenn er nur für ein Segment bestimmt ist -> verstärkte Netzlast)
- Repeater-Funktionalität im OSI-Referenzmodell

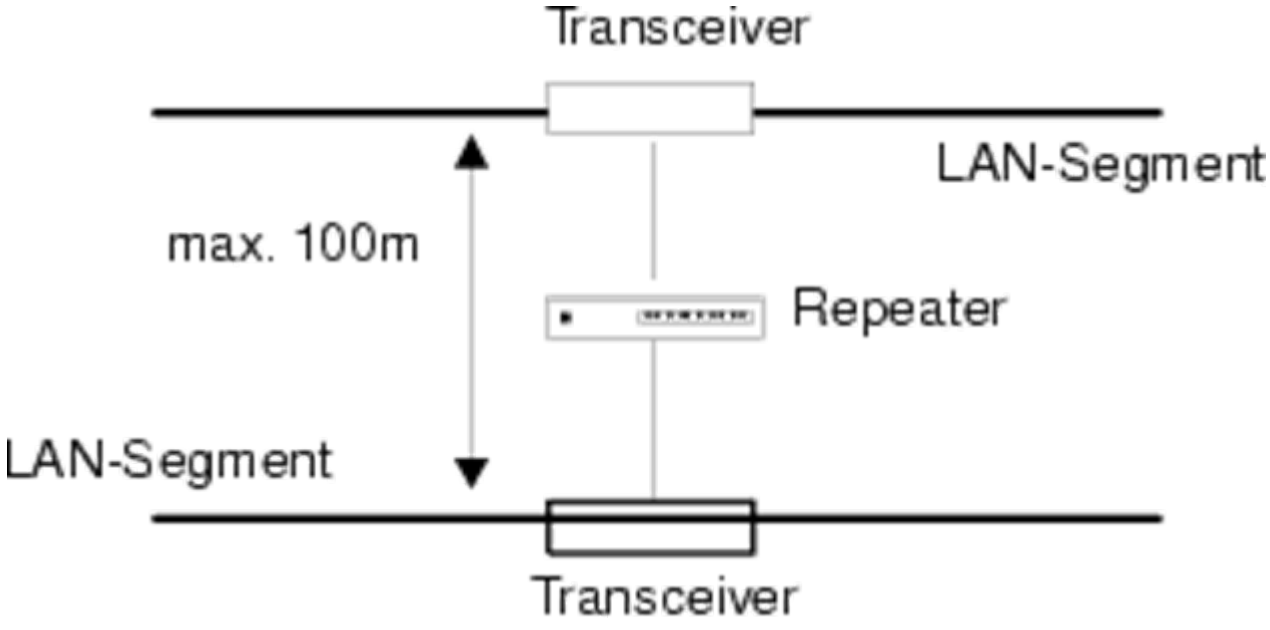


3.6.3 Repeater (2)

- **Aufgaben eines Repeaters:**
  - Kollisionserkennung und Erzeugung eines Störsignals bei Kollisionen (bei Ethernet-Repeatern)
  - Abtrennen fehlerhafter LAN-Segmente
  - Unterscheidung zwischen
    - **Lokale Repeater**
    - **Entfernte Repeater**
  - Achtung: Repeater-gekoppelte Netze bilden einen Kollisionsbereich (z.B. ein LAN auf Basis von Ethernet)
- **Repeater sind protokolltransparent**

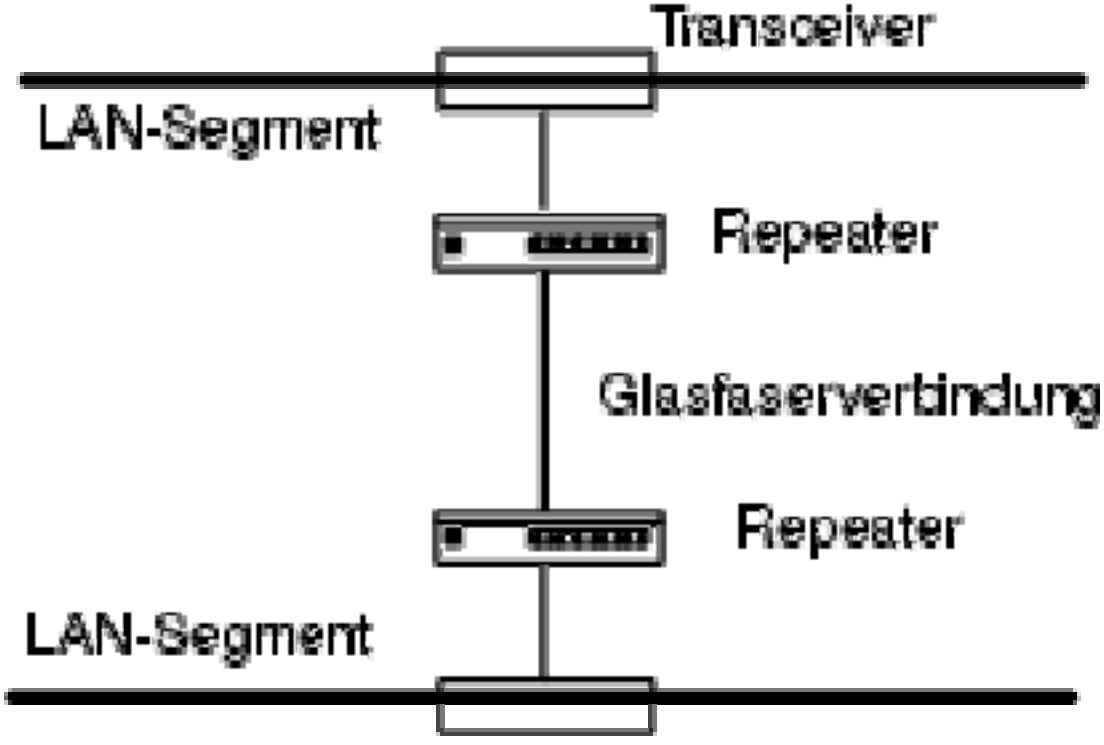
3.6.3 Lokale Repeater

- **Ein lokaler Repeater dient zur direkten Verknüpfung zweier LAN-Segmente; maximale Transceiver-Kabellänge ist 50 m**



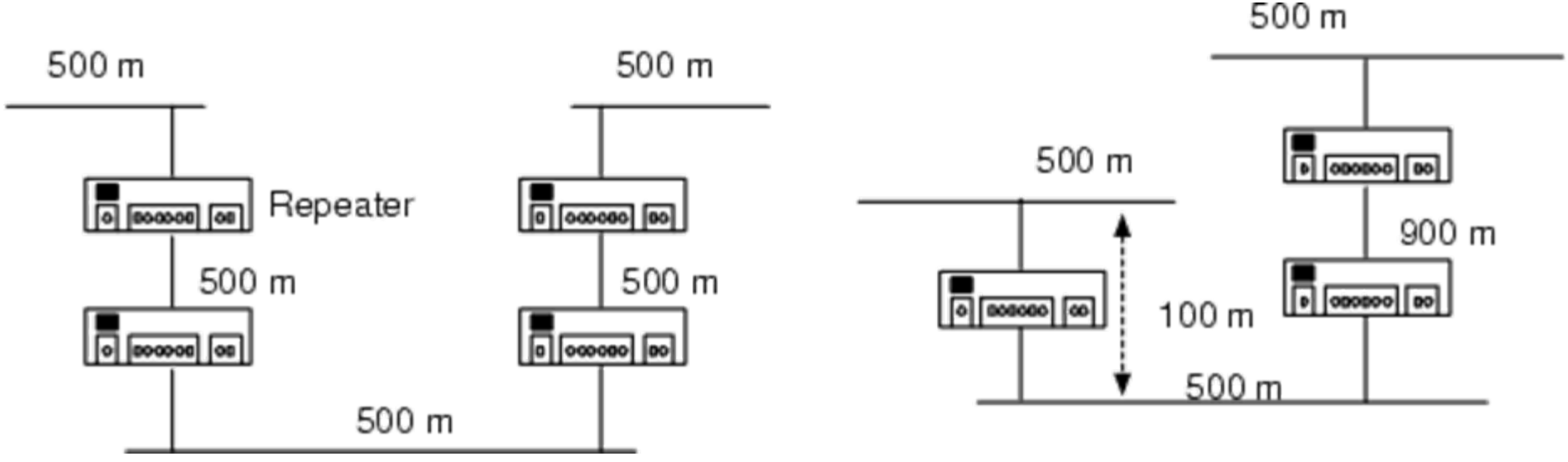
3.6.3 Entfernte Repeater

- Ein entfernter Repeater ist in zwei Hälften geteilt -> LAN-Segmente können weiter entfernt sein
- Bis zu maximal 12 km bei Einsatz von Glasfaserverbindungen
- Ein Multiport-Repeater: mehrere Ausgangsports (10Base2, 10BaseT), obsolete



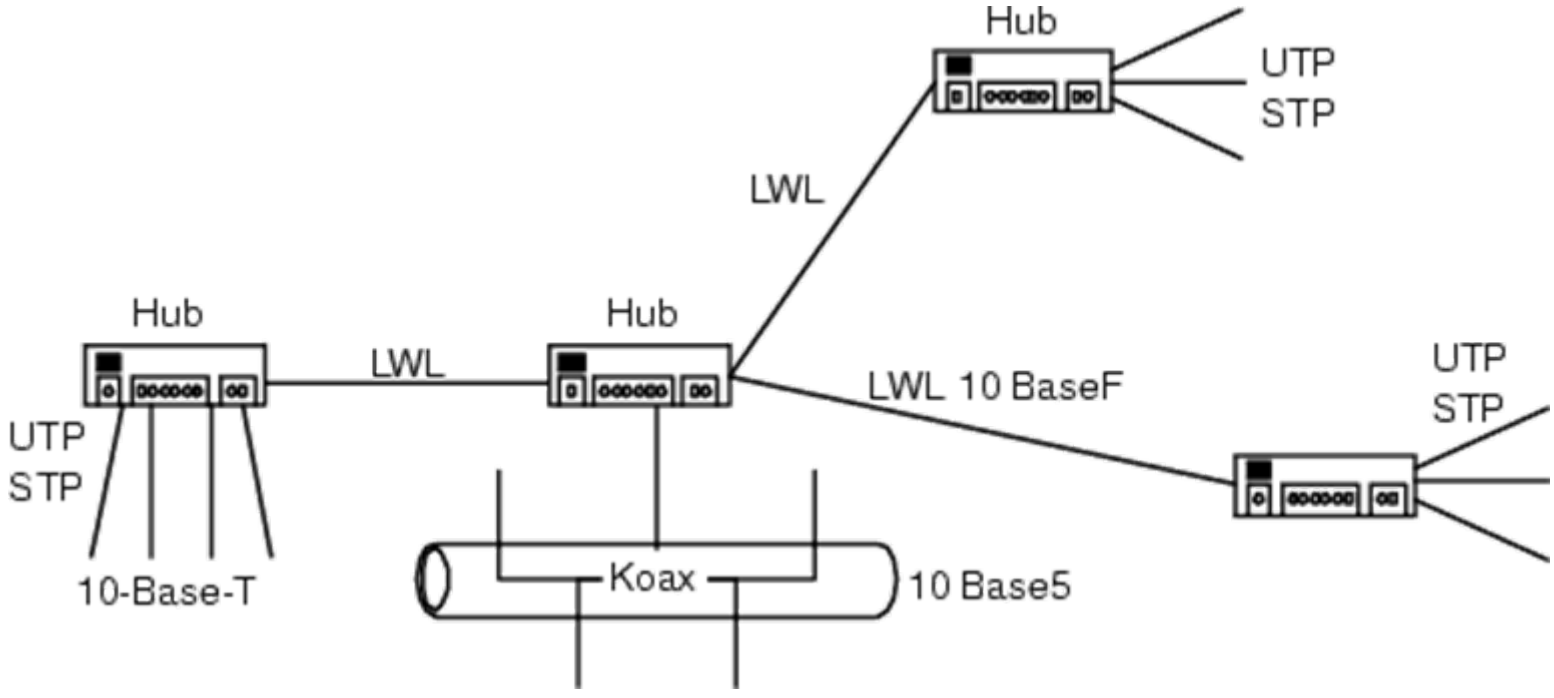
3.6.3 Repeater: maximale Konfiguration eines Ethernets

- **5 Segmente und 4 Repeater, davon max. 3 Koaxsegmente und 2 Linksegmente -> 2500m zwischen zwei DTEs. Die maximale Konfiguration wurde durch den IEEE Standard vorgeschrieben.**
  - Bei 4 Repeatern: Länge FOIRL (Fiber Optic Inter Repeater Link) <= 500 m
  - Bei 3 Repeatern: Länge FOIRL <= 1000 m; d.h. Summe Linksegmente <= 1000 m
  - Maximal 2 entfernte Repeater auf Kommunikationsweg



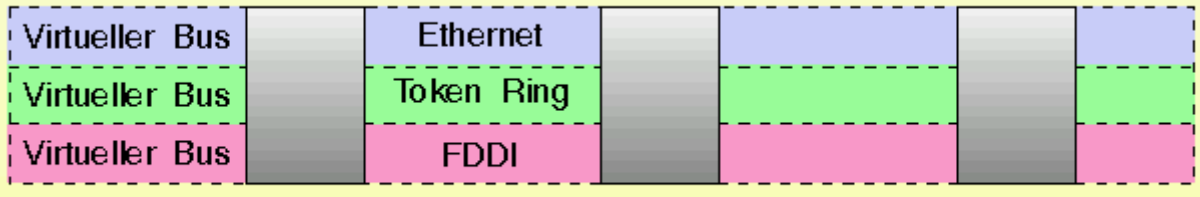
3.6.4 Hubs / Sternkoppler (1)

- Hubs als zentrales Kopplungselement (Wiring Hub), koppelt verschiedenste Medien auf Ebene 1
- Hubs dienen hier zur Verstärkung und zur Signalumsetzung



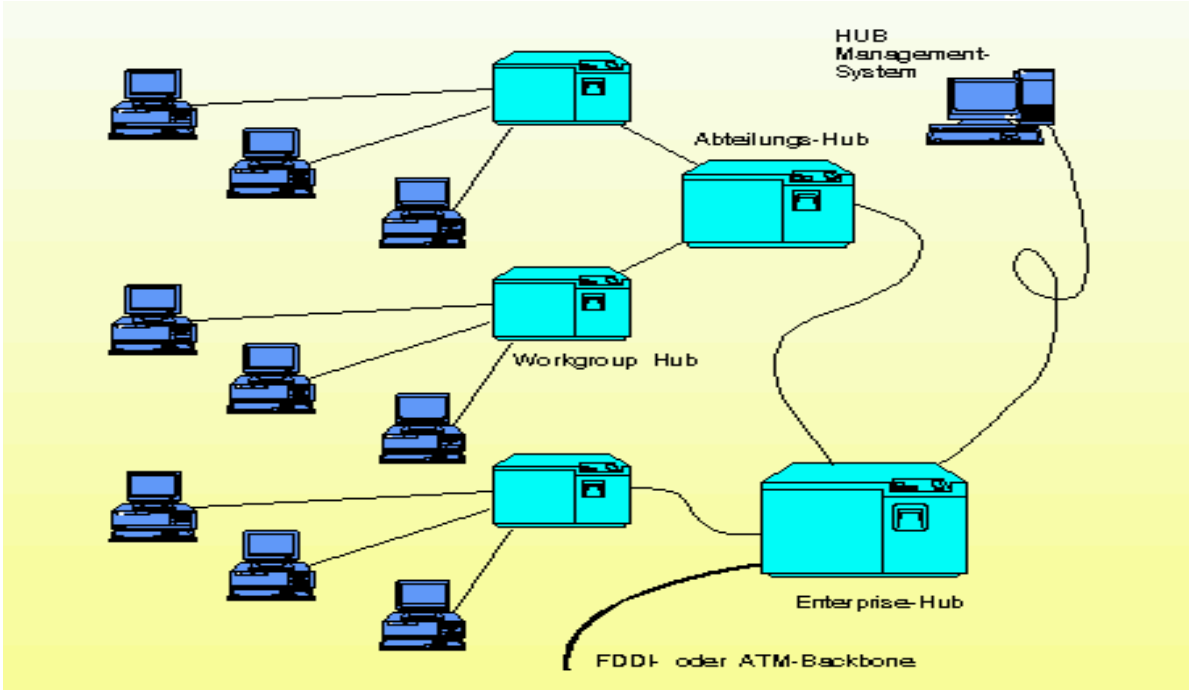
3.6.4 Hubs / Sternkoppler (2)

- **Hub-Backplane als segmentierter Bus**



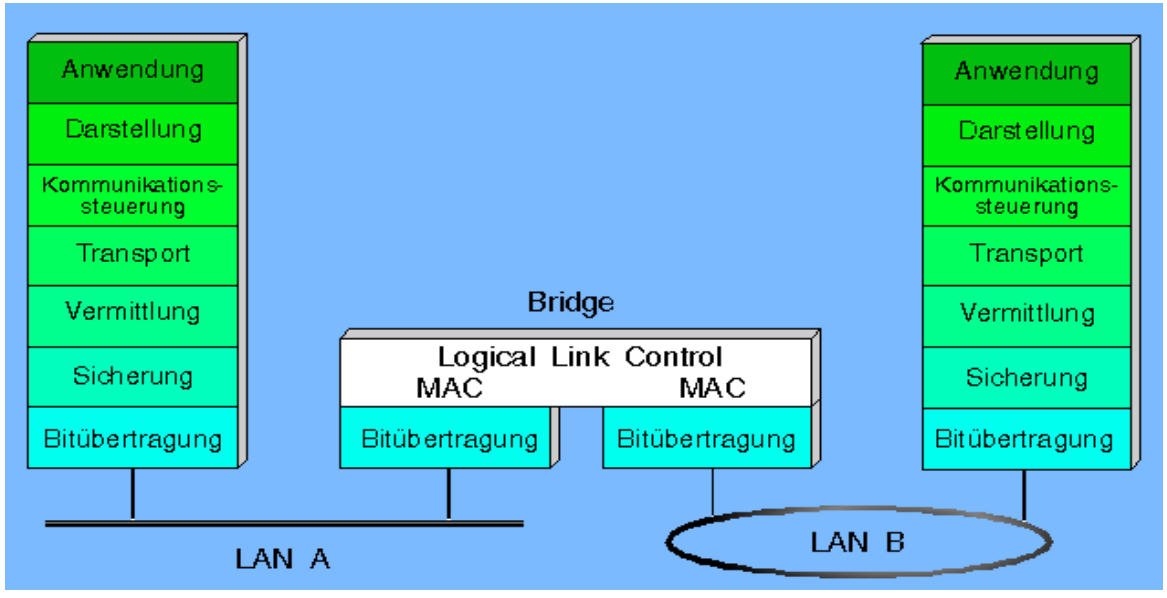
  - Ein Backplane implementiert die logische und physische Zusammenschaltung der Einsteckmodule

- **Beispiel einer Hub-Hierarchie**
- **Bei Neubeschaffungen**
  ➔ Switches



3.6.5 Bridges / Brücken

- **Einführung:**
  - Über Repeater verbundene LAN-Segmente sind an LAN-Beschränkungen gebunden (d.h. maximale Ausdehnung, Anzahls DTEs)
  - Beschränkungen können durch Brücken (**Level-2a-Gateways**) aufgehoben werden
  - Einsatz von Brücken, die als „Store-and-Forward“-Geräte agieren, d.h. jedes LAN-Segment wird als eigenes LAN interpretiert
  - Im Allgemeinen hat eine einfache Bridge nur 2 Ports

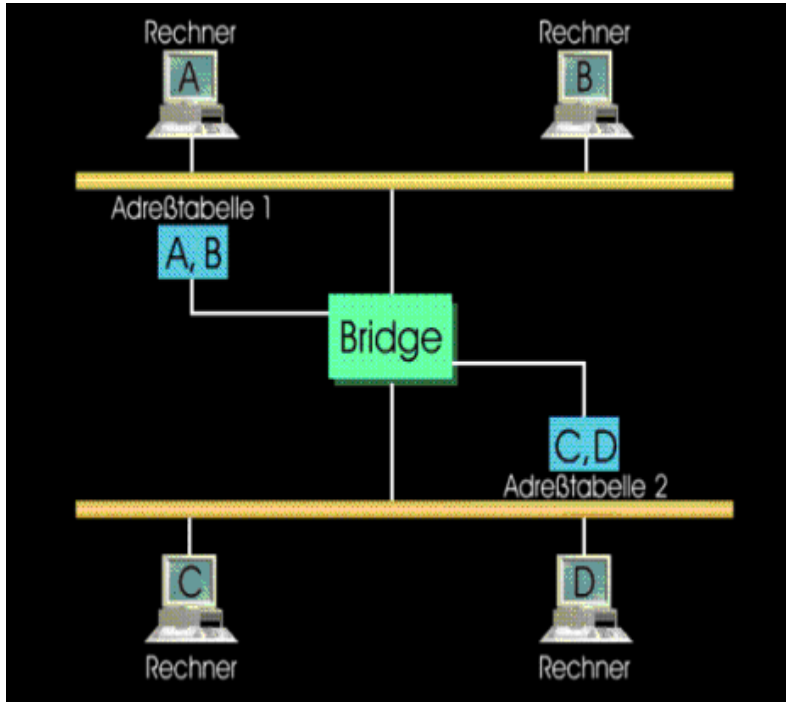


Kopplung von LAN-Segment auf der Medium-Zugangsschicht (Schicht 2a); Verwendung meist zur Verknüpfung von zwei IEEE 802-LANs -> Eventuell Modifikation des MAC-Frames (transparent für höhere Schichten)

3.6.5 Eigenschaften von Brücken (1)

- **Bridges puffern empfangene Frames**
  - Store-and-Forward Modus; fehlerhafte Frames werden herausgefiltert; nur fehlerfreie, relevante Frames werden propagiert
  - durch Pufferung unterschiedliche MAC-Protokolle verwendbar;
- **Fehlende Flusskontrolle auf Schicht 2a**

  ➔ Puffer in Bridge können überlaufen
- **Aufgaben einer Bridge:**
  - Medienunabhängigkeit bei Kopplung
  - Unabhängigkeit vom Zugriffsverfahren der Einzel-LANs z.B. CSMA/CD oder Token-Ring
  - Adresstransparenz für höhere Protokolle
  - Lastentkopplung des lokalen Verkehrs; es werden nur relevante Frames propagiert
  - Fehlereingrenzung bis Ebene 2a

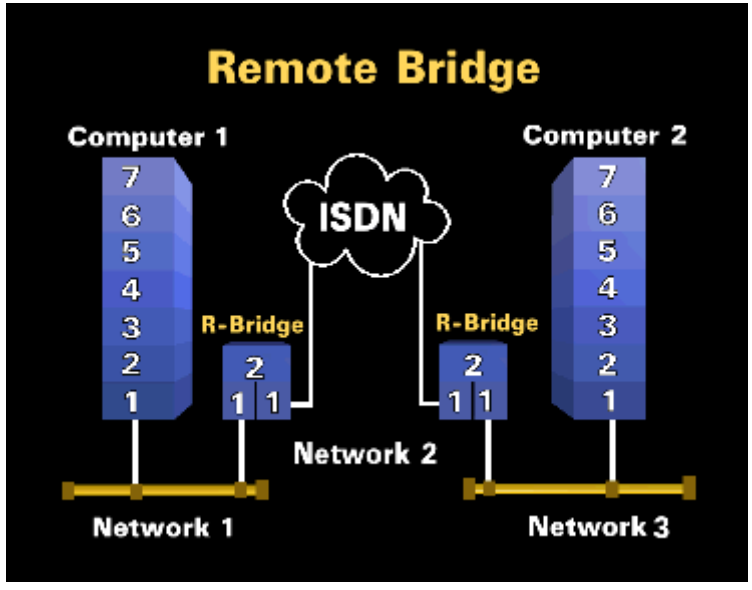


3.6.5 Eigenschaften von Brücken (2)

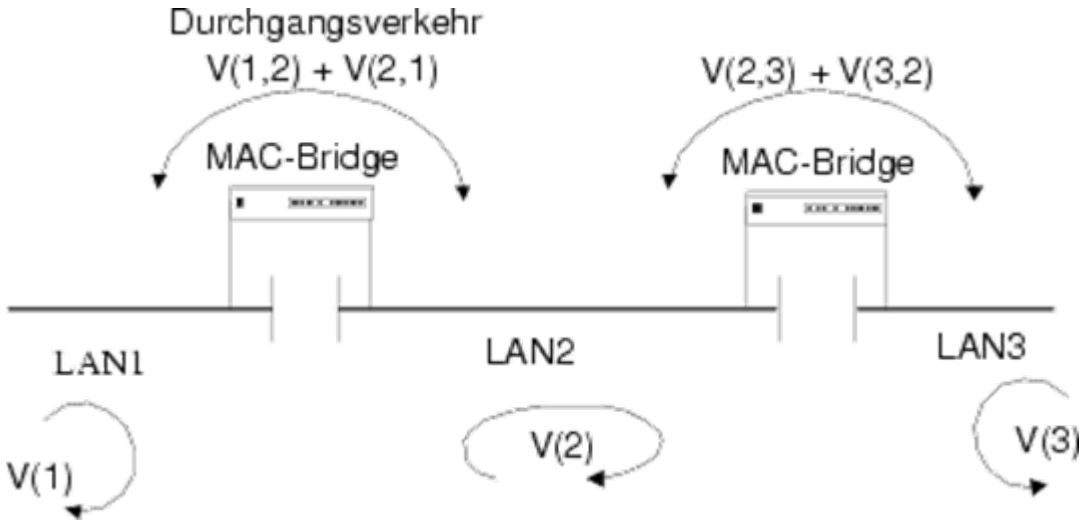
- **Aufgaben einer Bridge:**
  - Schutzfunktionen über Filtermechanismen
    Darunter versteht man das gezielte Weiterleiten bzw. Blockieren von Frames
  - Redundanz-Möglichkeit durch Alternativ-Wege
    Achtung: Schleifen müssen vermieden werden
  - Grundsätzliche Management-Funktionalität der Komponente Bridge
- **Interne Schnittstellen, z.B. zwischen den beiden unabhängigen MAC-Instanzen und der Relay-Instanz**
- **Filter-Bridges**
  - Filterkriterien sind u.a.: das Typfeld eines Ethernet-Paketes, die Paketlänge, Broadcastpakete oder die Absender-/Empfängeradresse
  - Filterfunktion wird durch den „Forwarding Process“ wahrgenommen, der sich der Einträge in Filterdatenbank bedient; Filtereinträge können statisch oder dynamisch sein.

3.6.5 Einsatzgebiete von Bridges

- **Lokale Bridges**
  - Verbinden LAN-Segmente direkt, als Subnetzkopplung innerhalb eines Unternehmens- oder Campus-Netzes
  - Die Verbindung wird über die LAN-Eingangsports und -Ausgangsports der Brücke hergestellt, d.h. mit Ein- und Ausgangsgeschwindigkeiten der LAN-Bandbreite
- **Remote Bridges**
  - Die Remote-Brücke verbindet räumlich entfernte Subnetze auf der MAC-Schicht über private Leitungen oder Weitverkehrsnetze
  - Wird immer paarweise eingesetzt
- **Multiport Bridges**
  - Hat mehr als zwei Ports, kann also mehrere Subnetze miteinander verbinden; bis zu 20



3.6.5 Bridge: Charakteristische Zahlen

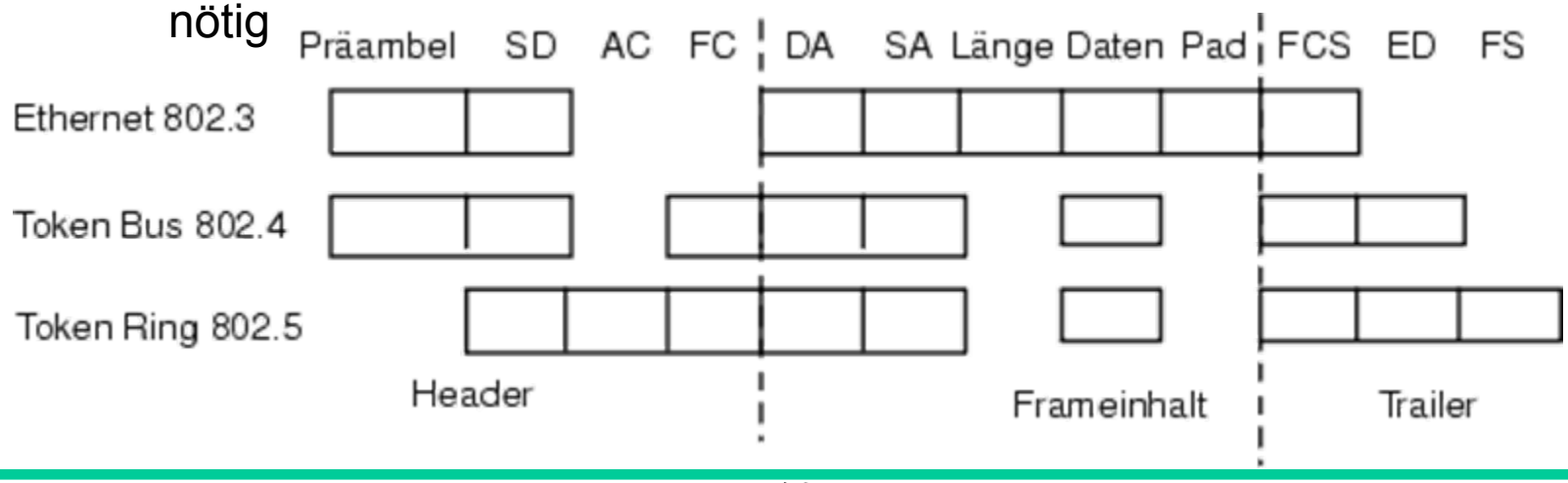


- **Definition**
  - V(i): mittlere Verkehrsraten im Ethernet (i) (lokaler Verkehr)
  - V(i,j): Segmentübergreifende Verkehrsrate, d.h. von i nach j.
  - F(i,j): Filterrate der Bridge. Und zwar bzgl. dem Verkehr von i nach j.
  - D(i,j): Durchsatzrate der Bridge
- **Forderung**
  - D(i,j) >= V(i,j) + V(j,i): Der Durchsatz ist größer als der Verkehr in beide Richtungen
  - F(i,j) >= V(i) + V(j): Die Filterrate ist größer als der Verkehr in beiden Netzen

3.6.6 Verknüpfung unterschiedlicher LAN-Typen (1)

- **Probleme bei der Verknüpfung unterschiedlicher LANs wegen:**
  - Unterschiedlichen Frameformats
  - Unterschiedlicher Framelänge
  - Verwendung von Prioritäten
  - Broadcasting (extreme Auswirkungen auf Netzlast möglich)
- **Frame-Format**
  - Unterschiedliche Formate für Ethernet, Token-Ring und Token-Bus (historisch bedingt)

    ➔Eventuell Reformatierung und neue Berechnung der Prüfsumme nötig



3.6.6 Verknüpfung unterschiedlicher LAN-Typen (2)

- **Datenrate**
  - Probleme bei der Verbindung von LANs mit unterschiedlichen Datenraten
    - 802.3 (Ethernet): 1, 2, 10, 100, 1000 Mbps,10Gbps
    - 802.4 (Token Bus): 1, 5, 10 Mbps
    - 802.5 (Token Ring): 1, 4, 16, 100 Mbps
  - Propagieren von einem langsamen Netz in ein schnelleres Netz ist kein Problem; andere Richtung: Gefahr von Pufferüberläufen in der Bridge
- **Frame Länge**
  - Unterschiedliche Frame Längen erfordern die Aufteilung von zu langen Frames (Segmentierung)
    - 802.3: 1518 Bytes
    - 802.4: 8191 Bytes
    - 802.5: abhängig vom Ringumfang

3.6.6 Verknüpfung unterschiedlicher LAN-Typen (3)

- Spezielle Probleme, falls Frame für Ziel-LAN zu lang; es existieren 3 Möglichkeiten, die Situation zu behandeln:
  - Löschen des Frames
  - Sender muss Obergrenzen auf Weg zu Ziel-DTE kennen oder
  - Segmentierung von zu großen Frames
- Letztere Funktionalität wird meist auf Vermittlungsschicht angeboten, d.h. Einsatz von Router

❑ **Prioritäten**

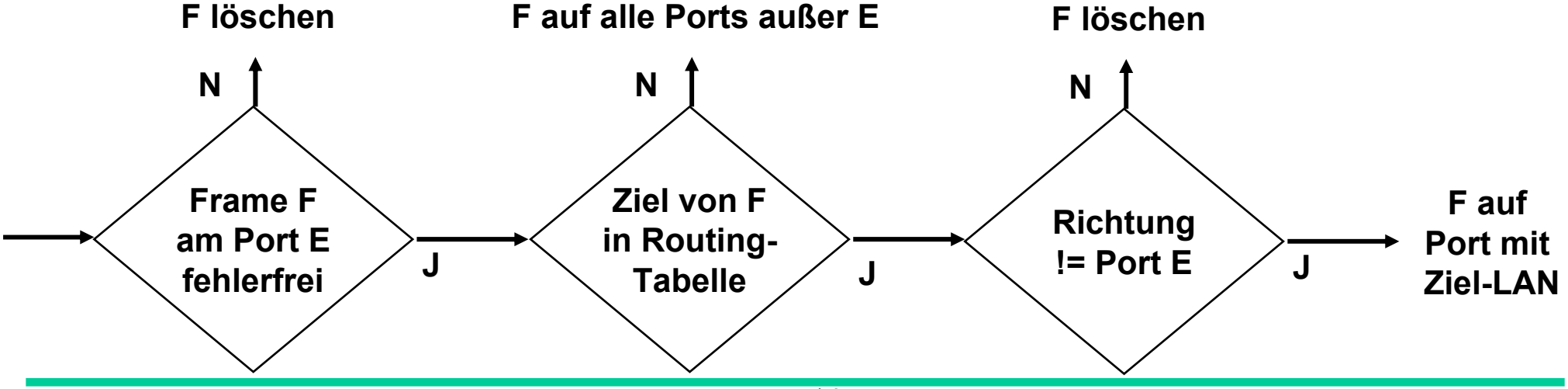
- Behandlung der Prioritäten hängt von den Übergängen ab:
  - Token Bus/Token Ring -> Ethernet: Verlust der Priorität, bei Token Ring wird FS als Bestätigung verwendet, hier bestätigt ersatzweise die Bridge, ohne den wirklichen Empfang überprüfen zu können
  - Ethernet -> Token Bus/Token Ring: Generierung von Prioritäten

3.6.6 Verknüpfung unterschiedlicher LAN-Typen (4)

- **Wegewahl in Bridge-Verbunden**
  - Abhängig von dem Routing der zu propagierenden Bridges können 2 Klassen von Bridges unterschieden werden:
    - Transparente Bridges:
      - überträgt Frames auf Hop-Basis und arbeitet nach einer Tabelle, in der die Endknoten und Brückenports einander zugeordnet sind (je nach Lernmechanismus und Spanning-Tree-Verfahren)
      - Dieses Verfahren heißt transparent, weil die Lage der Brücken für die Endknoten transparent ist
      - Dieser Ansatz wird für das Ethernet verwendet
    - Quell-Routing Bridges:
      - Spezifizierung eines Routing-Algorithmus auf LLC-Ebene
      - Der Hauptteil der Wegfindung wird von den Quellstationen (sendende Station handhabt die Routing-Tabellen über alle offenen, aktiven Verbindungen) durchgeführt, d.h. gesendeter Frame muss Routing-Information enthalten
      - Komplementäres Verfahren zum Spanning-Tree-Protokoll, um redundante Strukturen zu erkennen. DTEs müssen Topologie kennen
      - Dieser Ansatz wird für den Token Ring verwendet

3.6.7 Transparente Bridges (1)

- **Ziel ist die vollkommene Transparenz für die kommunizierenden DTEs, d.h. sie sind sich nicht bewusst, dass ihre Kommunikation über ein/mehrere Bridges erfolgt**
- **Eigenschaften:**
  - Routing-Tabelle je Bridge
  - Diese dient zur Entscheidung, ob und wie die gepufferten Frames propagiert werden müssen
  - Routing-Tabelle enthält eine Zuordnung zwischen DTE-Adresse und den für diese Adresse zu wählenden Ausgang der Bridge (Port)

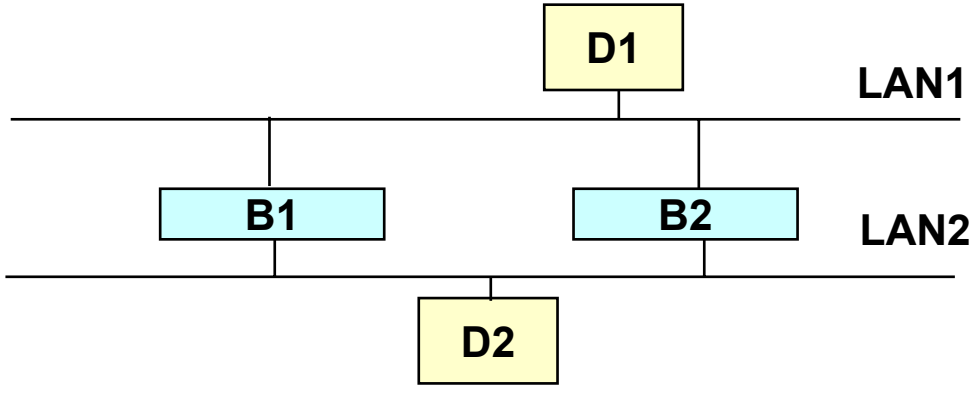


3.6.7 Transparente Bridges (2)

- **Bei der Initialisierung des Netzverbundes ist Routing-Tabelle i.a. leer**
  - ➔ **Lernmechanismus** und **Flooding**-Algorithmus notwendig, d.h. falls kein Eintrag in Routing-Tabelle, wird Frame auf alle Ausgangsports propagiert
- **Lernmechanismus zur Bestimmung der Routing-Tabelle**
  - Hier werden die Quelladressen der empfangenen Frames betrachtet; falls Quelladresse noch nicht in Routing-Tabelle -> Eintrag mit Zuordnung des Ausgangsports, auf dem Frame empfangen wurde
  - Der Mechanismus ist ein-/ausschaltbar; Verwendung eines Alterungsmechanismus (löscht Einträge aus Routing-Tabelle), um auf Veränderungen zu reagieren
- **Vermeidung von Schleifen:**
  - Falls mehrere Bridges parallel zwischen 2 LANs eingesetzt werden, führt dies zu Problemen

3.6.7 Transparente Brücken: Schleifenbeispiel

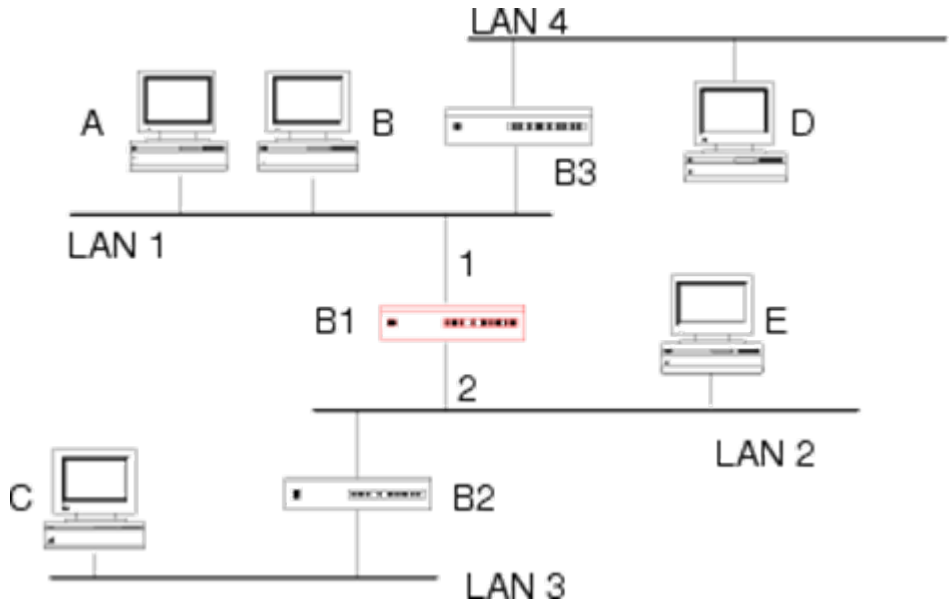
- Beispiel:
  - LAN1 und LAN2 jeweils direkt mit den Bridges B1 und B2 verbunden; D1 ist verbunden mit LAN1 und D2 mit LAN2
  - Ein Frame F wird von D1 nach D2 gesendet, wobei D2 vorher unbekannt ist
  - Bei Verwendung von Flooding durch B1 und B2 oszilliert F zwischen LAN1 und LAN2; falls Bridge bzgl. D1 immer noch im Flooding-Modus ist, würde der Ausgangsport jeweils aktualisiert werden, z.B. zuerst LAN1, dann LAN2, dann LAN1, etc.



➔Abwendung des Algorithmus zur Bestimmung des minimal aufspannenden Baumes („Spanning Tree Algorithm“); es ergibt sich eine aktive Verbundtopologie

3.6.7 Transparente Brücken: Beispiel Lernmechanismus

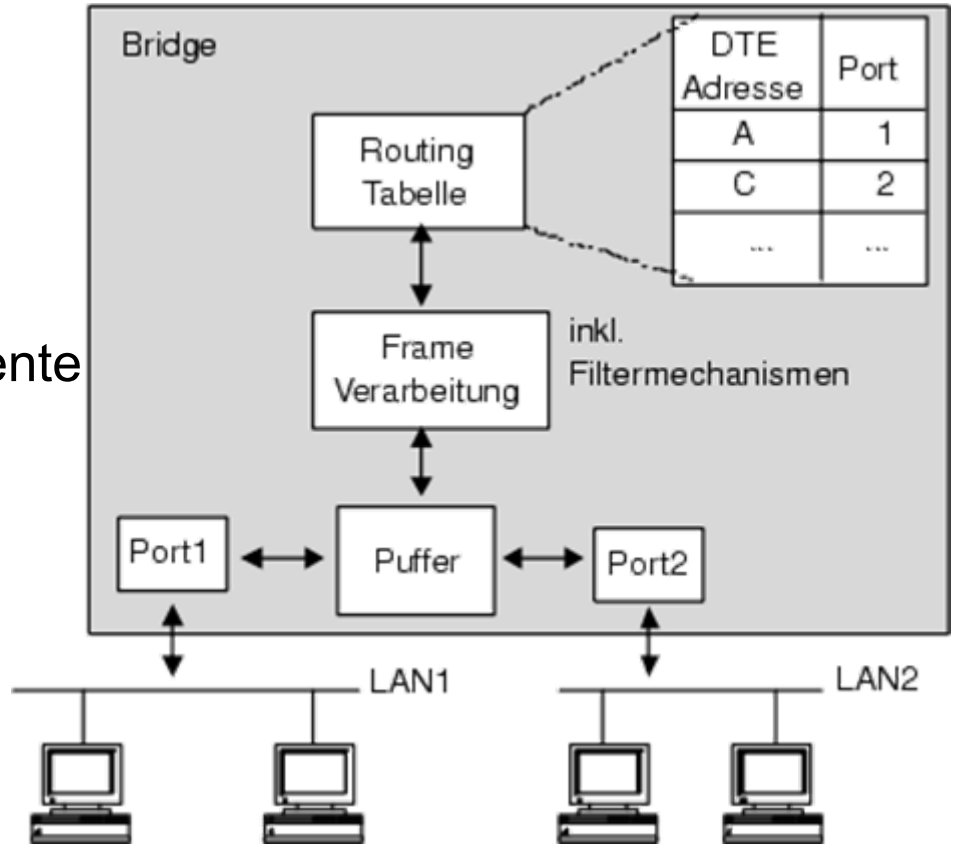
- **Auswirkungen des Lern-mechanismus auf Routing-tabelle von B1:**
  - Initialisierung: leere Tabelle
  - Nachricht A -> E: Eintrag (A,1); ->Propagieren auf 2 (Flooding)
  - Nachricht E -> A: Eintrag (E,2); -> Propagieren auf 1
  - Nachricht C -> D: Eintrag (C,2); -> Propagieren auf 1 (Flooding)
  - Nachricht E -> C: - -> -, weil auf Port 2-Seite



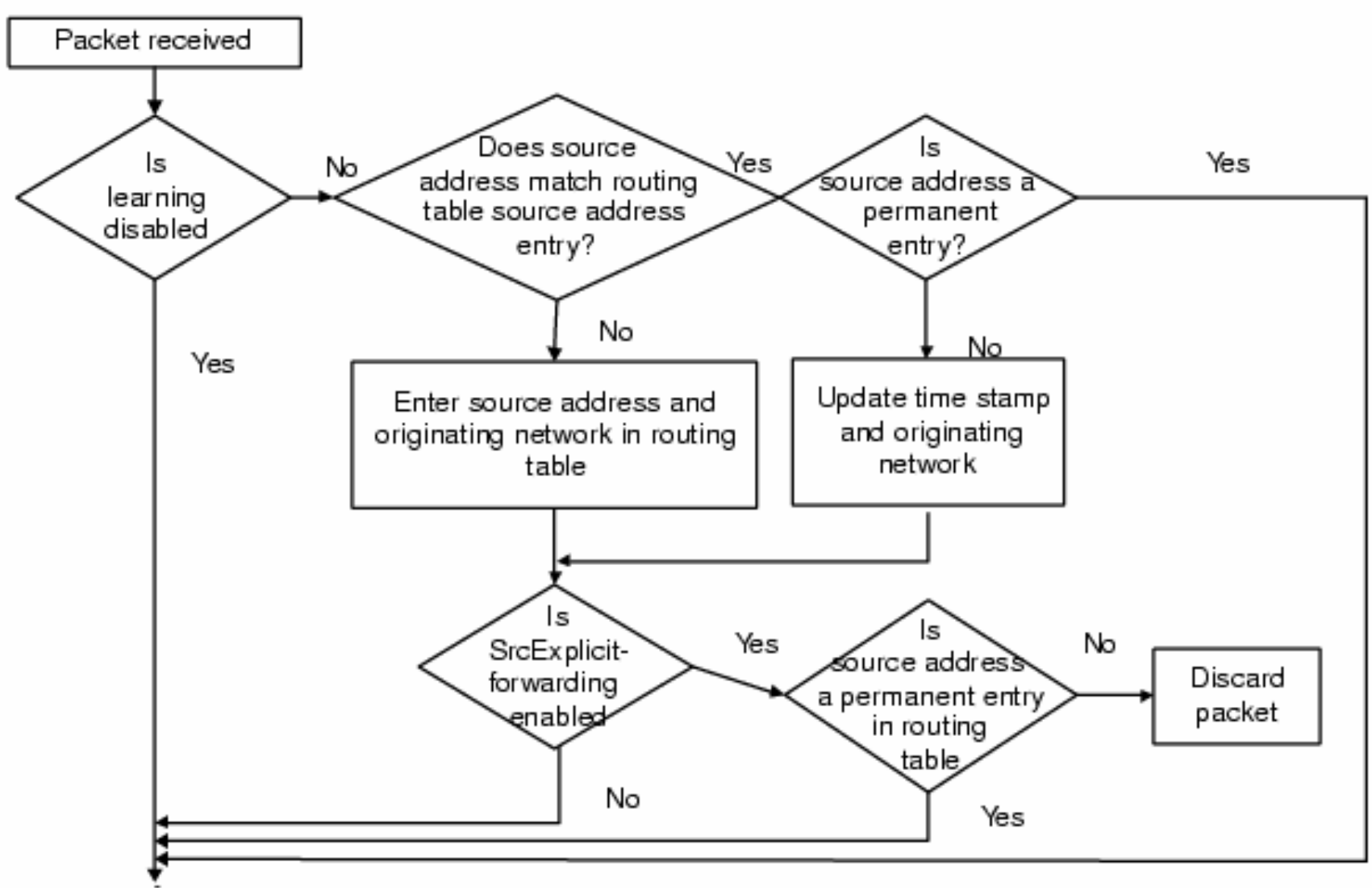
- **Lernen setzt vollständige Beobachtung des Netzverkehrs voraus**
- **Lokalverkehr wird nicht über eine Bridge weiter übertragen!**

3.6.7 Transparente Brücken: Architektur

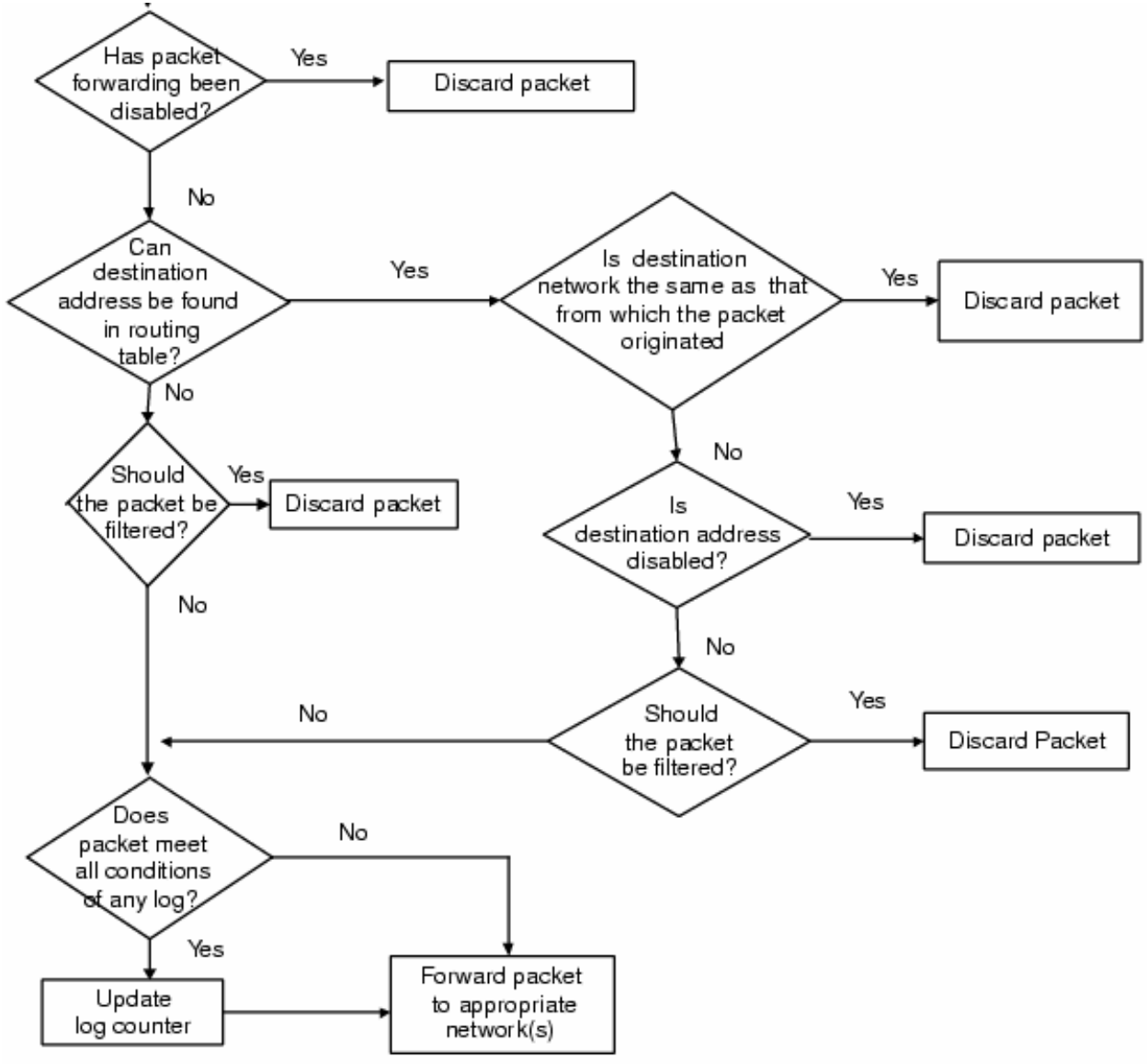
- **Eine Bridge besteht aus:**
  - Ports
  - Puffer
  - Routingtabelle
  - Frame-Verarbeitungskomponente
- **Aktualisierung der Routing-tabelle nach Topologieänderung -> Alterungsmechanismus: d.h. Rücksetzen eines Eintrags in der Routing-Tabelle nach längerer Inaktivität; Umfang der Routing-Tabelle wird begrenzt, da nur für aktive DTE ein Eintrag besteht; mittels Lernmechanismus/Flooding erfolgen Neueintragungen**



3.6.7 Transparente Brücken: Arbeitsweise einer Bridge (3Com)



3.6.7 Transparente Brücken: Arbeitsweise einer Bridge (3Com)



3.6.8 Spanning-Tree-Algorithmus für Bridges (1)

- **Ablauf (Bridge ist spezifiziert durch Paar (eindeutiger Identifikator, Priorität), ID stammt vom Hersteller, Priorität kann benutzt werden, um Bandbreite für Topologie zu optimieren**
  - Bestimmung der „Root-Bridge“ R: Bridge mit kleinstem Identifikator; andere Möglichkeit wäre höchste Priorität (bei mehrere gilt wiederum ID) -> Root-Bridge eindeutig
  - Jede Bridge B (außer Root-Bridge) bestimmt Wegekosten zwischen B und Root R bzgl. Ports -> Port mit minimalen Kosten wird Root-Port; Wegekostenbestimmung mit Hilfe der LAN-Datenraten (höhere Datenrate = geringere Wegekosten); bei Gleichheit gilt Portnummer; Wegekosten können Laufzeit, Zahl der durchlaufenen Bridges oder echte Gebühren sein
  - Für jedes LAN S werden Bridge-Ports zur Propagierung von Frames bestimmt („Designated Bridge“ und „Designated Port“)

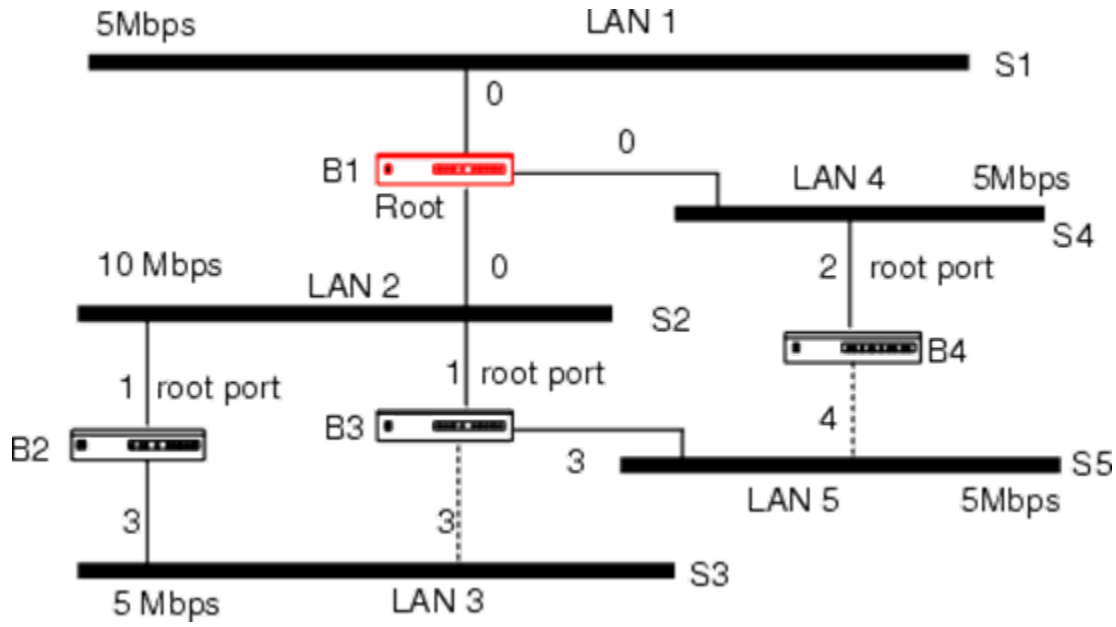
    = Port mit geringsten Wegekosten zur Wurzel über alle in Frage kommenden Bridges

3.6.8 Spannung-Tree-Algorithmus für Bridges (2)

- Für jedes LAN wird eine Bridge zu R bestimmt (Bridge mit kostengünstigsten Port) und dann dessen Port; ein Root-Port ist immer ein Designated Port, da gewisse LANs nur über Root-Port erreichbar; bei allen Bridge-Ports wird Port mit geringsten Wegekosten gewählt (bei Gleichheit kleinste ID); andere Ports erhalten Zustand blockiert d.h. es werden über diese keine Frames propagiert.

3.6.8 Spanning-Tree-Algorithmus für Bridges: Beispiel (1)

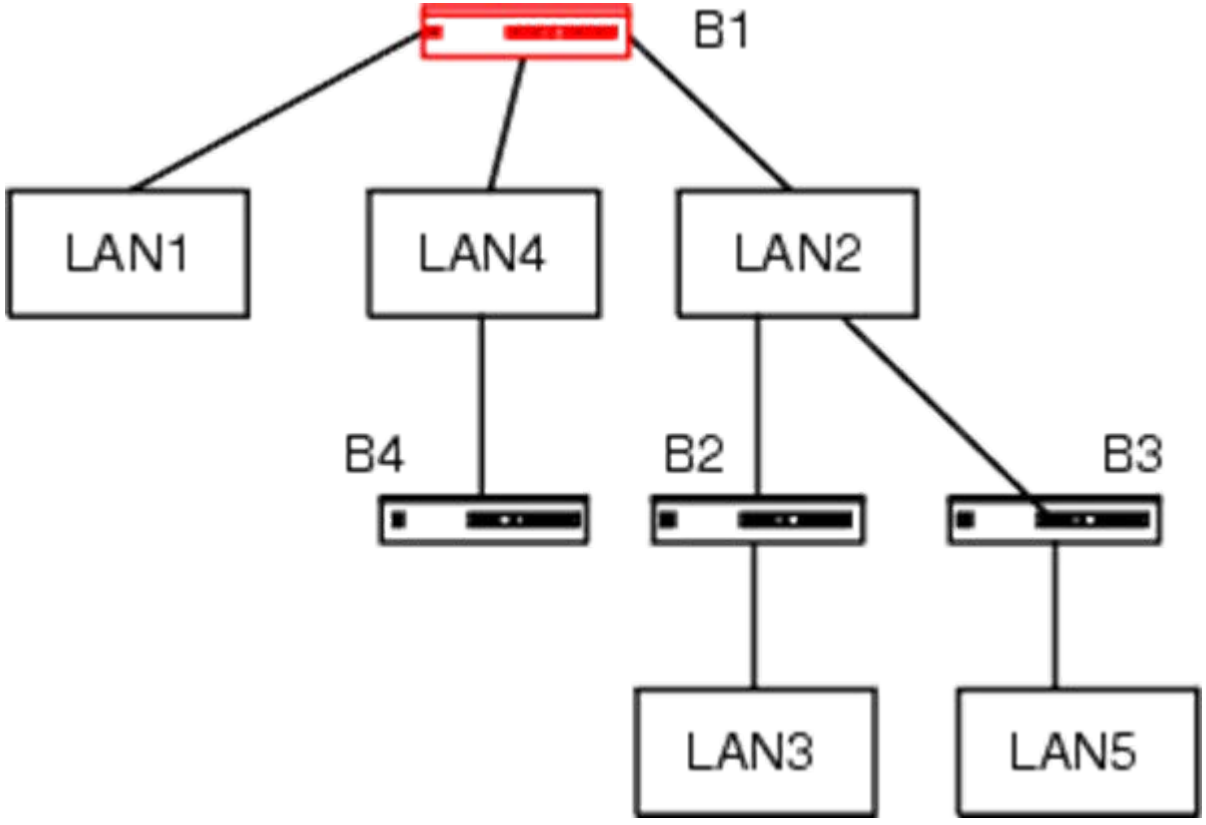
- **Beispiel**
  - B1 ist Root-Bridge
  - RP sind die bestimmten Root-Ports
  - Nummern an Port-ausgängen bezeichnen Wegekosten zur Root-Bridge



  - S2 hat Kosten 1, alle restlichen Segmente Si haben Kosten 2. Für S3 wird B2 als Designated Bridge ausgewählt (Wegekosten sind zwar gleich, aber B2 < B3); somit ist der Port zu S3 der Designated Port
  - Für S5 wird B3 statt B4 ausgewählt, da geringere Wegekosten

3.6.8 Spanning-Tree-Algorithmus: Beispiel (2)

- Es ergibt sich folgende Netzstruktur



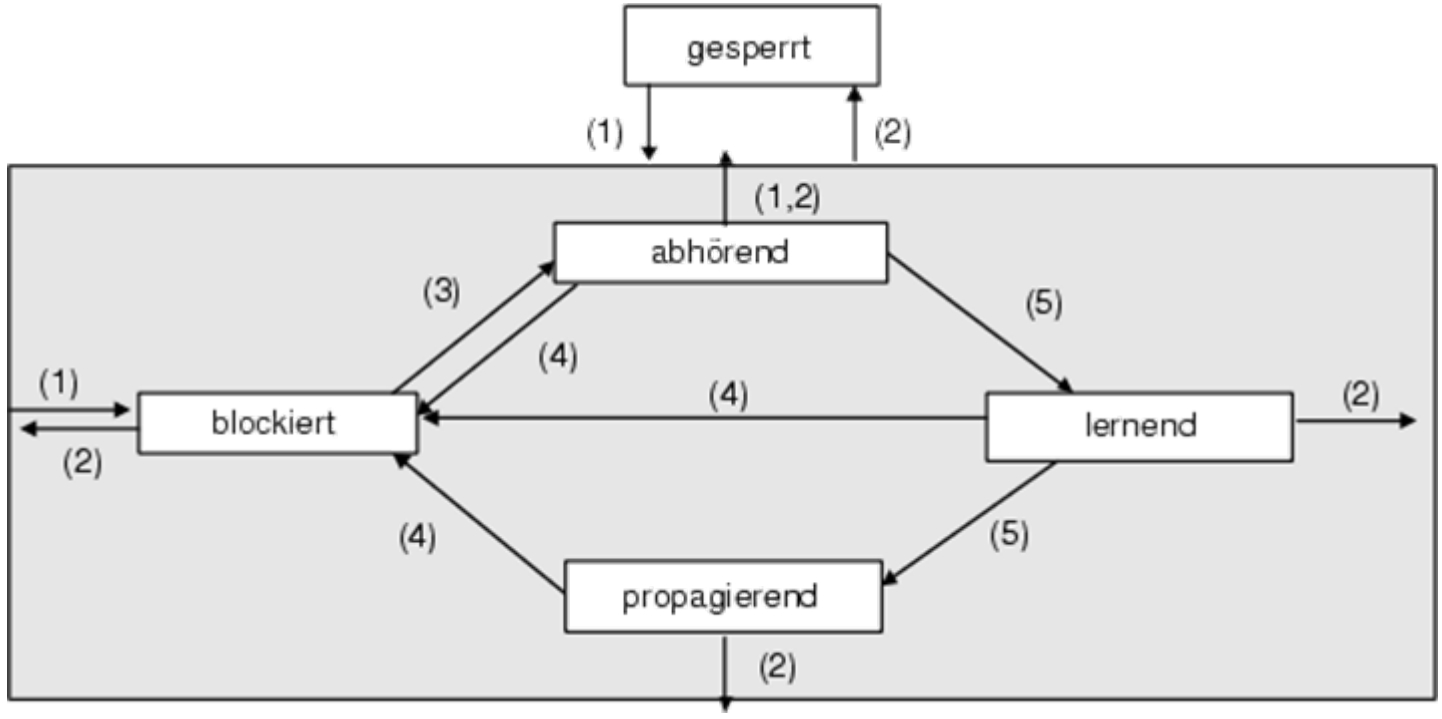
3.6.8 Spanning-Tree-Algorithmus: Kontrollframes

- **Spanning-Tree Algorithmus wird bei Initialisierung des Netzes und periodisch während aktivem Netzbetrieb durchgeführt**
- **Rapid Spanning Tree (IEEE 802.1d)**
  - Umschaltung im Bereich weniger Millisekunden (können aber nicht garantiert werden -> wichtig für Service Level Agreements)
  - Kritikpunkt an RSTP sind die fehlende Fehlerverwaltung
- **Aktualisierung bei Topologieänderungen notwendig**
  - **Konfigurations-Kontrollframe**
    - dient bei Initialisierung der Topologie zur Bestimmung der Root-Bridge und der Wegekosten
    - nach Initialisierung wird dieser Kontrollframe regelmäßig durch Root-Bridge zur Aktualisierung der Portzustände verschickt
  - **Management-Kontrollframe**
    - bei Änderung eines Portzustandes wird dies allen Bridges auf dem Weg zur Root-Bridge mitgeteilt

3.6.8 Spanning-Tree-Algorithmus: Zustände eines Ports

- **Ein Port befindet sich in einem der folgenden Zustände:**
  - **Gesperrt**: Nur Management-Kontrollframes werden empfangen und verarbeitet
  - **Blockiert**: Nur Management- und Konfigurations-Kontrollframes werden empfangen und verarbeitet
  - **Abhörend**: Alle Kontrollframes werden empfangen und verarbeitet, z.B. Benachrichtigung an Root-Bridge über Änderungen eines Portstatus
  - **Lernend**: Alle Kontrollframes werden empfangen und verarbeitet; Datenframes werden vom Lernmechanismus interpretiert, aber nicht propagiert
  - **Propagierend**: Alle Kontrollframes werden verarbeitet; Datenframes werden verarbeitet und propagiert

3.6.8 Spanning-Tree-Algorithmus: Zustandsübergänge



(1) Port enabled, by management or initialization (Übergang nach blockiert). Verwendung eines Management-Kontrollframes

(2) Port disabled, by management or failure (Übergang nach gesperrt) Verwendung eines Management-Kontrollframes

(3) Algorithm selects as Designated or Root Port

(4) Algorithm selects as not Designated or Root Port

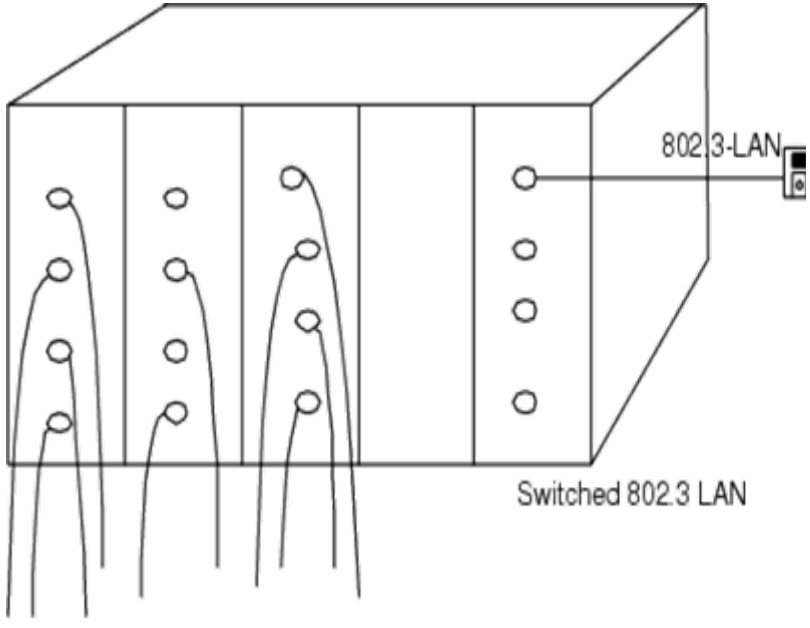
(5) Protocol timer expiry (Forwarding Timer)

3.7 Switches

- 3.7.1 Grundlagen
- 3.7.2 Kategorisierung von Switches
- 3.7.3 Angriffe
- 3.7.4 Realisierungsmöglichkeiten von VLANs
- 3.7.5 Zugangskontrolle mit 802.1x
- 3.7.6 Produkte
- 3.7.7 Managementwerkzeuge

3.7 Switches

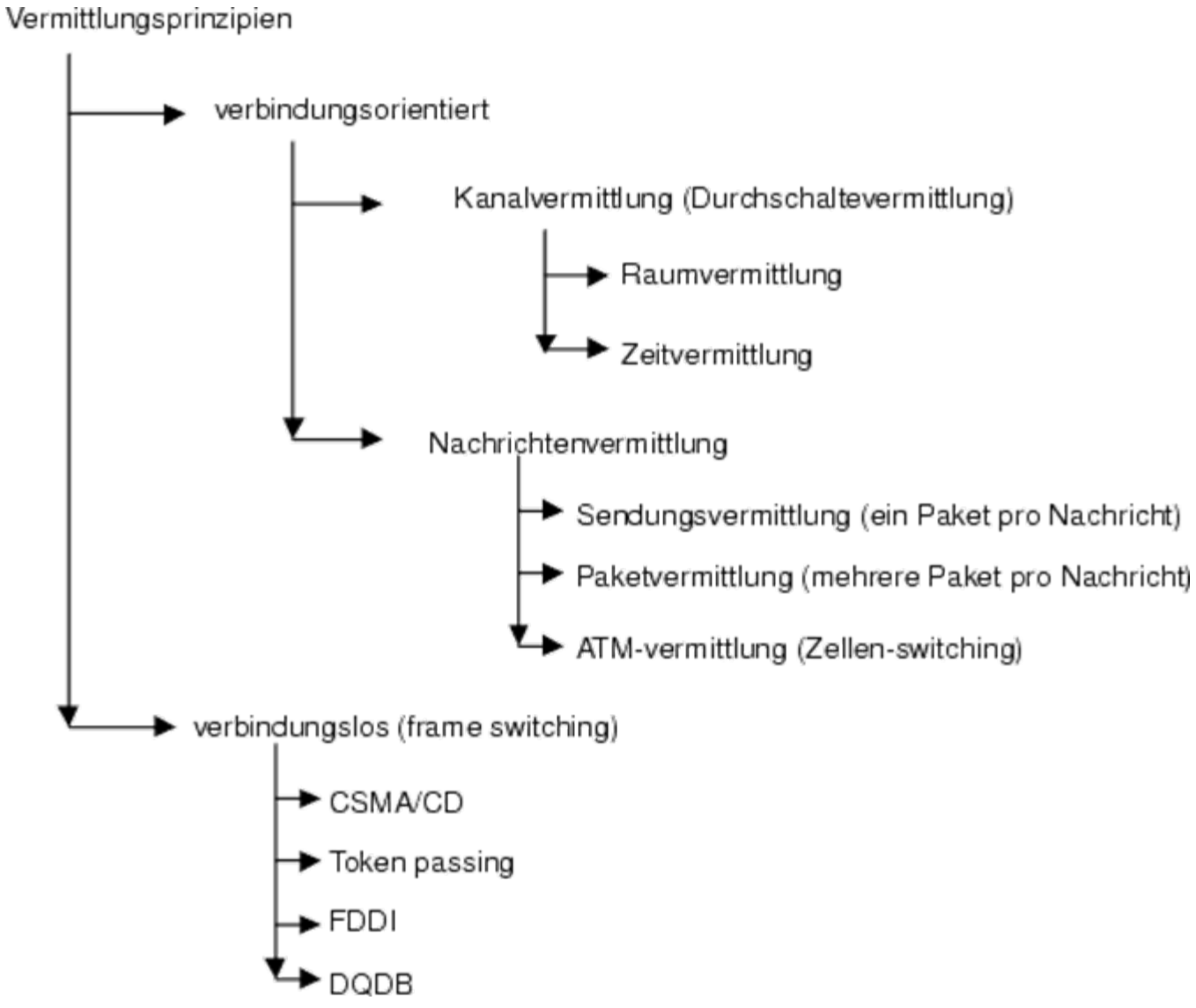
- ***Switch* (englisch für Schalter):**
  - Einheit, in der Vermittlungsfunktionen durchgeführt werden (Pfadschaltefunktion)
- **LAN-Switches sind Frame-Switches, arbeiten auf Ebene 2 wie Multiport-Bridges (i.a. hat Bridge nur 2 Ports)**



Eigenschaften

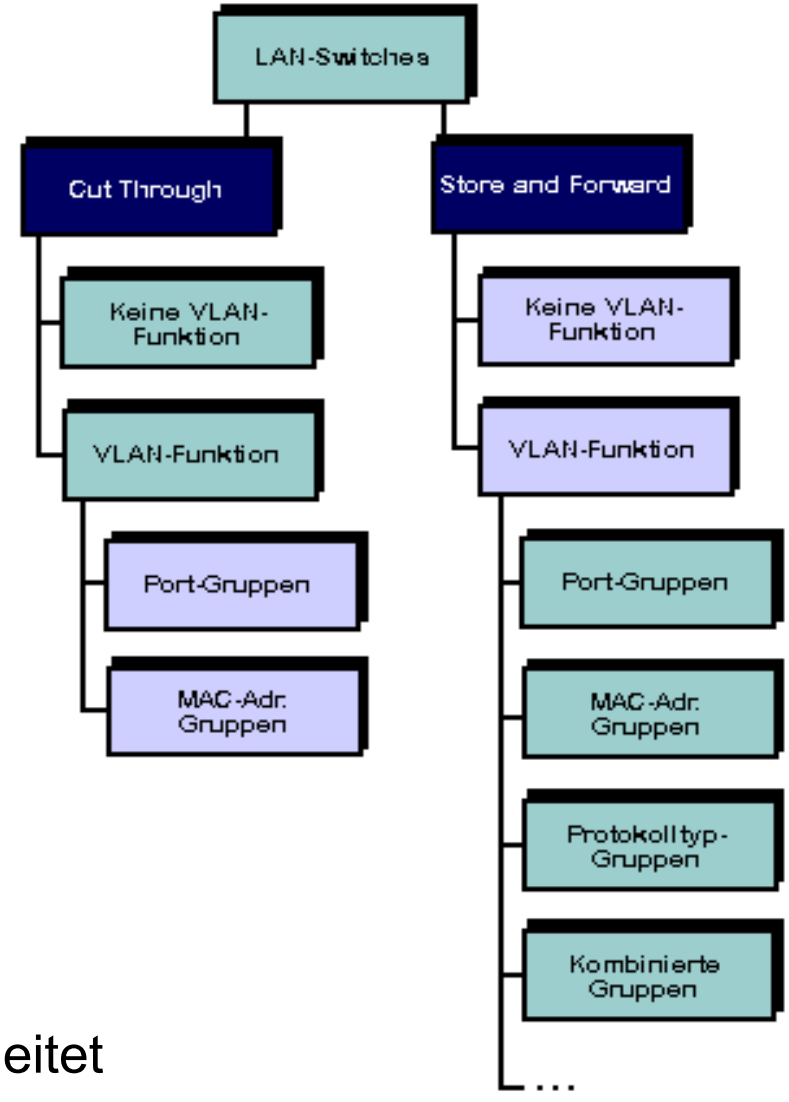
- Ermöglichen exklusive und nach Bedarf wechselnde Verbindungen zwischen angeschlossenen Segmenten
- Oft mehrere gleichzeitige Verbindungen in einem Switch, hardwareunterstützt an jedem Port mit kurzen Latenzzeiten (im Mikrosekunden-Bereich)
- Zuordnungstabelle MAC-Adresse <-> Port
  Zuordnungstabelle wird je Port gehalten oder auch global für Switch
- Üblicherweise große Portanzahl (> 10)

3.7.1 Switches - Grundlagen: Vermittlungsprinzipien



3.7.1 Switches - Grundlagen: Forwarding-Techniken (1)

- **Store-and-Forward/Buffered**
  - Check des gesamten Frames; CRC, Fehlerseparierung
  - Variable Framelängen
  - Latenzzeit variabel und relativ hoch, Zwischenspeicherung bei unterschiedlichen Port-geschwindigkeiten erforderlich
- **Cut-Through/Fast-Forwarding/ On-the-Fly**
  - Weitervermittlung bereits nach Auslesen der Adressinformation (die ersten 14 Bytes), also eventuell bevor Datenende am Eingangsport
  - Konstantes Transit-Delay, aber fehlerhafte Frames werden weitergeleitet



3.7.1 Switches - Grundlagen: Forwarding-Techniken (2)

- Adaptive Cut-Through
  - Cut-Through-Modus, aber gleichzeitig CRC überprüfen
    Ist Fehlerrate größer als Schwellwert, umschalten in Store-and-Forward
- Near-Cut-Through
  - Es werden die ersten 64 Bytes abgewartet. Damit bleiben Kollisionen lokal (minimale Framelänge)

3.7.1 Switches - Grundlagen: Forwarding-Techniken (2)

- Die Funktion Minimierung des Transit-Delays stand zu Beginn der Switching-Technologie immer im Vordergrund der Diskussion.
  Ein Store-and-Forward-Mechanismus war und muss aber in den meisten Fällen auch bei Cut-Through-Geräten implementiert sein, da
  - die Unterstützung unterschiedlicher Link-Geschwindigkeiten in einem Gerät (10/100/1000 Mbit/s Ethernet) und
  - das Belegtsein des Ausgabeports

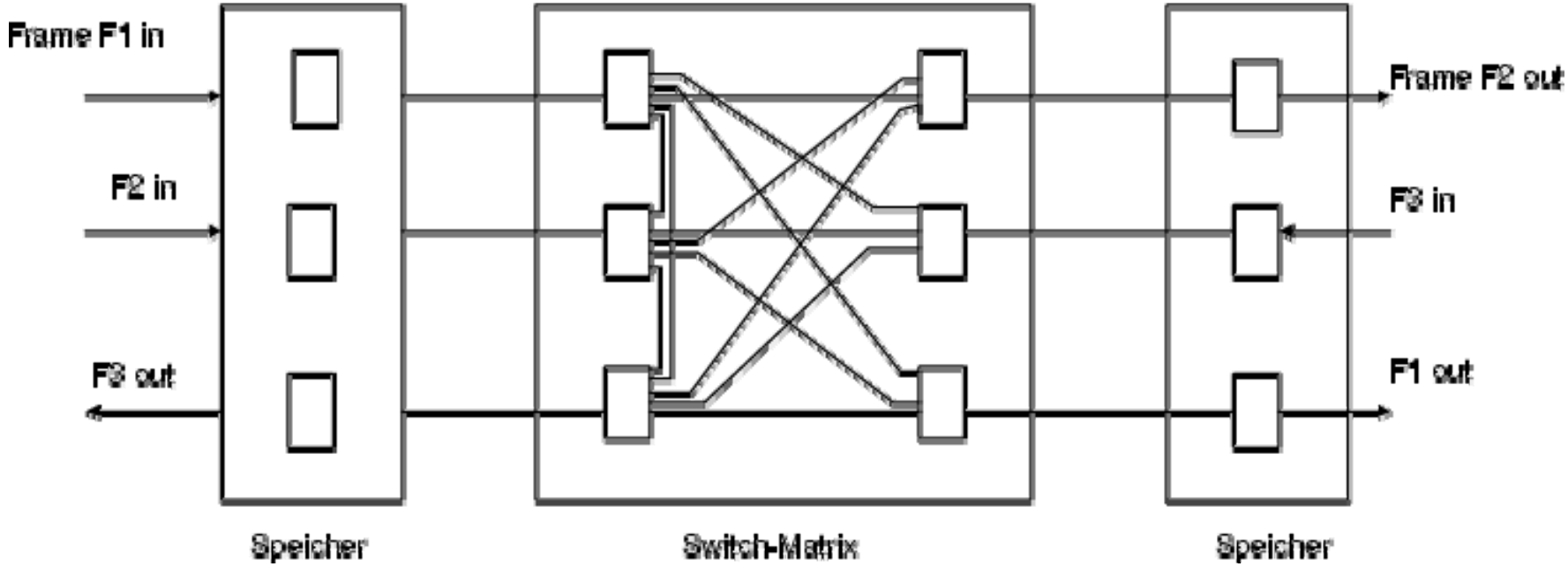
  immer eine Zwischenpufferung der entsprechenden Datenpakete notwendig macht

3.7.2 Kategorisierung von Switches (1)

- **Welche Vermittlungstechnologie?**
- **Wie sieht das Speicherkonzept aus? Ist Non-Blocking-Architecture vorhanden? Welche Puffer werden verwendet?**
- **Datendurchsatz unter Lastbedingungen?**
- **Möglichkeit zur Bildung von Portgruppen? Welche Ports werden zusammengefasst, Bildung von sogenannten Fatpipes.**
- **Latenzzeiten des Switches**
- **Effektive Aggregatbandbreite des Switches**
  - Unterstützt Switch mehrere parallele Übertragungen?
  - Kann Switch für VLANs nutzbar gemacht werden?
- **Sind Managementwerkzeuge integriert?**

3.7.2 Kategorisierung von Switches (2)

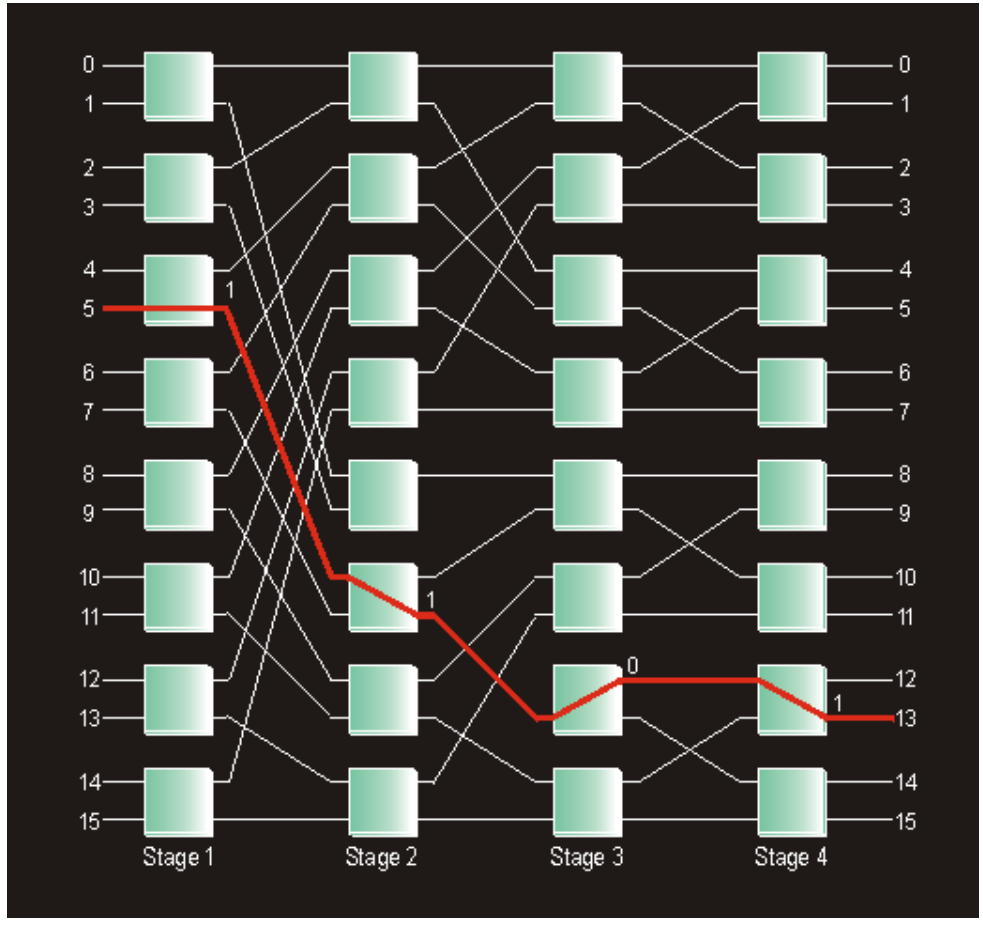
- **Kriterien der Unterscheidung**
  - Art der Switch-Fabric (internes Schaltnetz)
    - **Matrix-Struktur** (Cross-Point Matrix-Switches)



3.7.2 Kategorisierung von Switches (3)

❑ Kriterien der Unterscheidung

- Art der Switch-Fabric (internes Schaltnetz)
  - Matrix-Struktur
    - Alle Ports sind untereinander über eine Matrix verbunden
    - Weiterleitung eines Frames nach Dekodierung der Zieladresse über direkte Verbindung zum Ausgangsport
    - Falls Ausgangsport belegt, ist Zwischenspeicherung über FIFO-Puffer üblich; Größe des Puffers bestimmt Paketverlust durch Switch



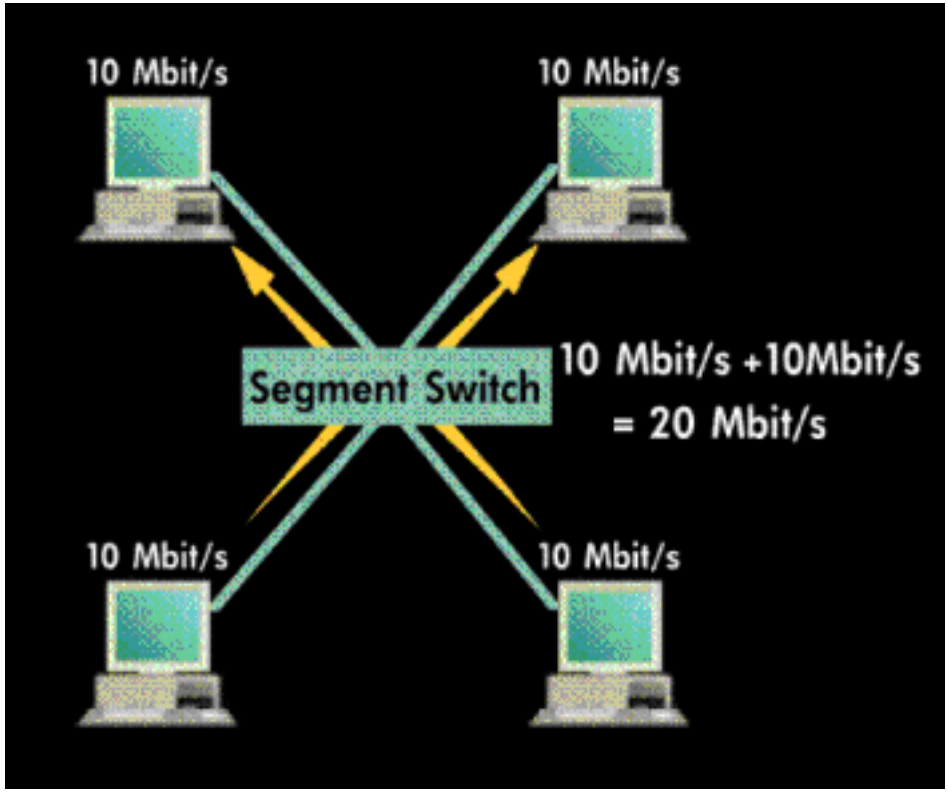
3.7.2 Kategorisierung von Switches (4)

- **Kriterien der Unterscheidung**
  - Art der Switch-Fabric (internes Schaltnetz)
    - **Shared-Memory (Zentralspeichertopologie)**
      - Im kleineren, preisgünstigeren Systemen eingesetzt
    - **Shared-Media Architekturen (High Speed Backplane)**
      - In modularen Switches mit hoher Portdichte (leistungsfähige Backplane) eingesetzt
  - Bandbreite der Switch-Fabric (kumulierte Bandbreite)
  - Internes Datenformat (Frames oder Zellen)
  - Pufferung (Überlastverhalten)
  - Anzahl Ports, Unterstützung von High-Speed-Ports, maximale Anzahl unterschiedlicher MAC-Adressen pro Port bzw. maximale Anzahl pro Switch (Private Switch, Segment-Switch), Fehlertoleranz
  - Management-Möglichkeiten

3.7.2 Kategorisierung von Switches (5)

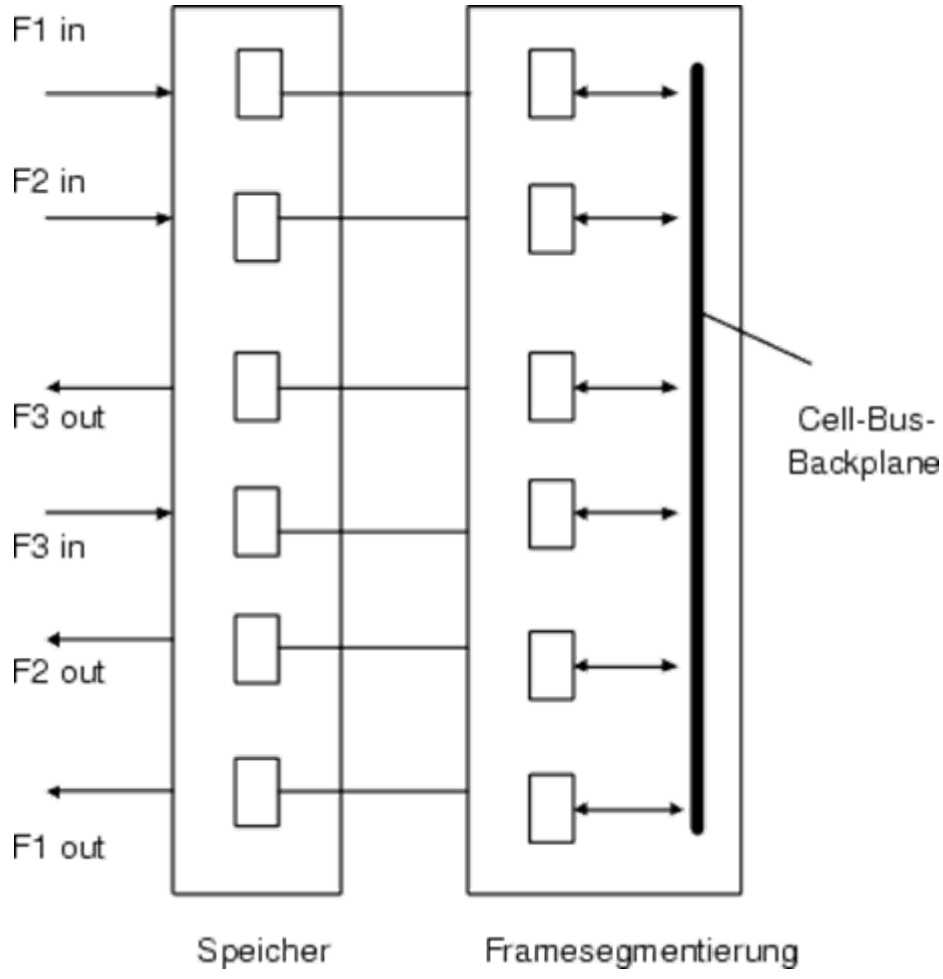
Ferner ist zu unterscheiden

- **Segment-Switching**
  - mehrere MAC-Adressen pro Port)
  - Häufigster Anwendungsfall
- **Port-Switching**
  - eine MAC-Adresse pro Port
  - Spezialkonfiguration (Sicherheitsaspekt, 802.1x)



3.7.2 Kategorisierung von Switches (6)

- **Cell-Bus-Switch**
  - Unterschiedlich lange Frames werden:
    - segmentiert in Zellen gleicher Länge
    - durch Segmentierung wird Ausgangsport-Blocking unwahrscheinlicher
    - Zwischenspeichern am Ausgangsport zu Reassemblierung, u.U. von parallel mehreren Frames
  - Bus wird durch Zeitmultiplexverfahren den Eingangsports zugeordnet; Speicherstruktur, Hierarchie und Backplane-Geschwindigkeit müssen aufeinander abgestimmt sein!

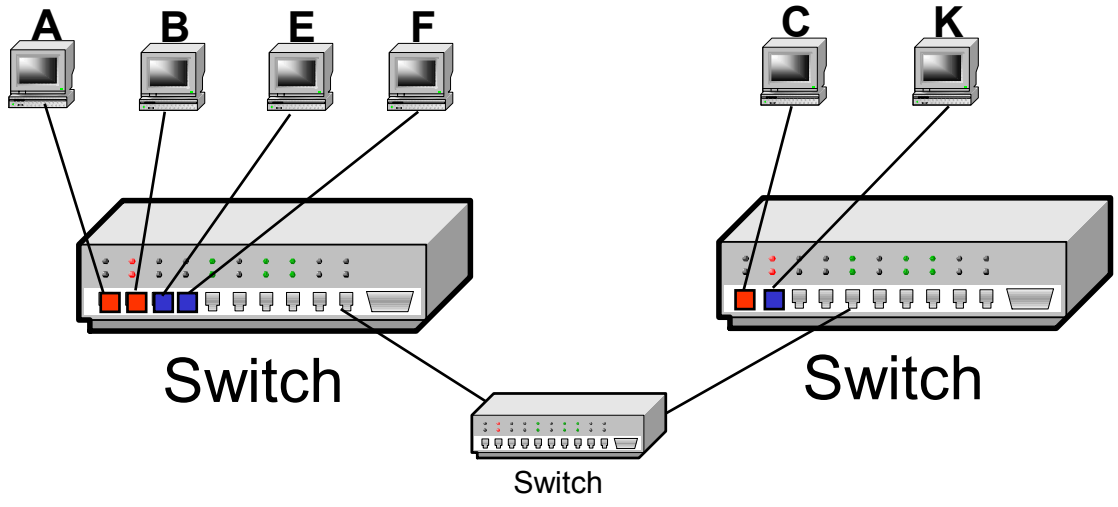


3.7.3 Angriffe

- **Problemstellung: MAC-Quelladressen, die über einen Port empfangen werden, werden ohne weitere Prüfung in die Adresstabelle eingetragen (-> es findet keine Authentifizierung statt)**
- **Es können mindestens zwei Angriffsarten unterschieden werden**
  - **MAC-Spoofing**: ein Angreifer versendet Rahmen mit der Source-MAC-Adresse eines anderen Hosts; Switch verwirft bisherige Zuordnung -> trägt den Port des Angreifers ein
  - **MAC-Flooding**: ein Angreifer versendet viele Rahmen mit verschiedenen, künstlich erzeugten Quelladressen, die die für das Netz gültigen MAC-Adressen aus der Adresstabelle des Switches verdrängen

3.7.4 Realisierungsalternativen von VLANs (1)

- **Layer-1-VLANs (Port-basierende VLANs)**
  - Einzelne Ports der Switches sind bestimmten VLANs zugeordnet
  - Sicherheit:
    - jeder Rechner, der an einem Port angeschlossen wird, gehört zu diesem VLAN (Portzuweisung zum VLAN)
    - Erweiterung -> Benutzer-Authentifizierung (802.1x)



VLAN1 Verwaltung
VLAN2 Entwicklung

3.7.4 Realisierungsalternativen von VLANs (2)

- **Das gleiche Prinzip der Gruppenzugehörigkeit wird auf verschiedenen Ebenen des OSI-Modells angewandt:**
  - Layer-2-VLANs: Zuordnung zu einem VLAN anhand der MAC-Adresse
  - Layer-3-VLANs: Zuordnung zu einem VLAN anhand der IP-Adresse
  - Policy-basierende VLANs: Zuordnung zu einem VLAN anhand von Policies (Kombination von Kriterien: Port, MAC-, IP-Adresse)
    Sicherheit: hoch
- **Portunabhängigkeit**
- **Gestufte Sicherheitskonfigurationen, die wegen der physischen Struktur anders nicht möglich wären**

3.7.4 Benutzerbezogene VLANs

- VLAN-ID des Benutzers wird auf dem RADIUS-Server gespeichert (Tunnel-Attribut)
- RADIUS-Server übermittelt VLAN-ID nach erfolgreicher Authentifizierung an Switch bzw. Accesspoint
- Benutzerport wird dynamisch in das entsprechende VLAN gelegt
- „Native˝ VLAN für RADIUS-Kennungen ohne VLAN-ID

3.7.4 Guest-VLAN

- **Authentifizierung erfolgreich**
  - Port kommt in benutzerspezifisches oder „native” VLAN
- **Authentifizierung nicht erfolgreich**
  - Kein 802.1X-fähiger Client
  - Keine gültige Kennung
  - Port wird freigeschaltet
  - Port kommt in das Guest-VLAN
- **Anwendungsgebiet**
  - Gastbenutzer ohne gültige Kennung (z.B. bei Tagung)
  - Weiche Migration nach 802.1X

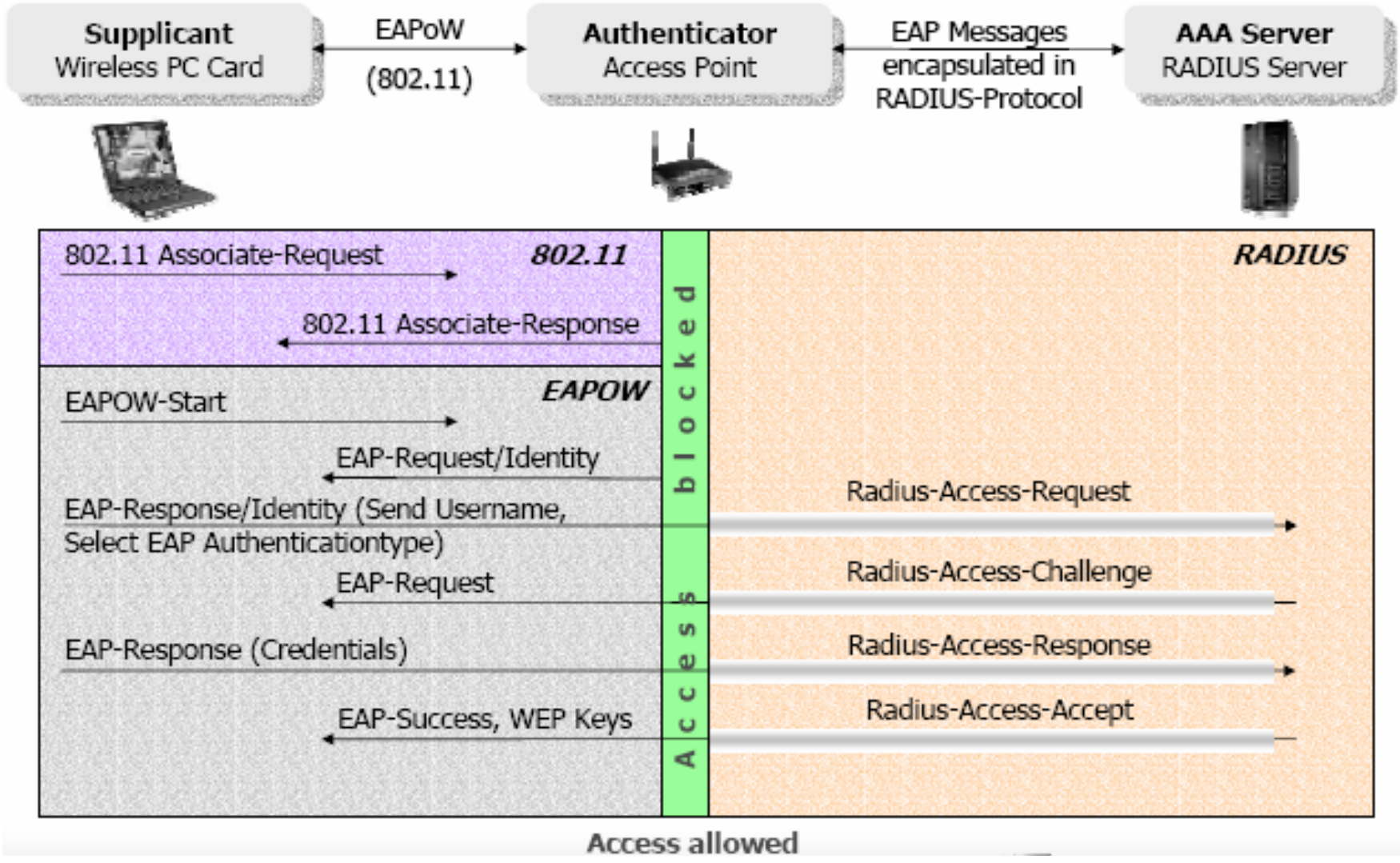
3.7.5 Was ist 802.1X?

- **Authentifizierung auf Layer 2**
- **Portbasierend (physischer Switchport oder logischer Port auf dem Accesspoint)**
- **Basiert auf Extensible Authentication Protocol (EAP)**
- **Authentifizierung durch RADIUS, LDAP usw.**
- **Verschlüsselung nur während der Authentifizierung**
- **Erweiterte Funktionen:**
  - Dynamische WEP-Keys (wired equivalent privacy)
  - Accounting
  - Benutzerbezogene VLANs
  - „Guest”-VLANs

3.7.5 Authentifizierung mit IEEE 802.1X

- **Layer 2**
  - MAC-Adress-Filter am Switch bzw. Access-Point
  - Zugang nur für „bekannte” MAC-Adressen
  - Authentifizierung des Rechners
  - Nachteile:
    - MAC-Adresse kann leicht gefälscht werden
    - Aufwändige Pflege der Adressen
- **Layer 3**
  - VPN-Server mit IPsec
  - Authentifizierung des Benutzers
  - Verschlüsselte Datenübertragung
  - Nachteile:
    - Authentifizierung erst auf Layer 3
    - Skalierbarkeit

3.7.5 Funktionsweise von 802.1X



3.7.5 IEEE 802.1X: EAP-Typen (1)

- EAP-MD5
  - Funktionsweise wie bei CHAP (challenge handshake authentication protocol)
  - Client sendet Kennung an den RADIUS-Server
  - RADIUS-Server sendet „Challenge”
  - Client generiert MD5-Hash mit Passwort als Key
  - Client sendet Hash an RADIUS-Server
  - Nachteile:
    - Kennung muss unverschlüsselt beim Server vorliegen
    - Keine Authentifizerung des Servers (Man-in-the-middle-Attacke möglich)

3.7.5 IEEE 802.1X: EAP-Typen (2)

- **EAP-TLS (Transport Layer Security)**
  - RADIUS-Server sendet Zertifikat an Client
  - Client überprüft Server-Zertifikat und sendet eigenes Zertifikat
  - RADIUS-Server überprüft Client-Zertifikat
  - Nachteile:
    - Zertifikat für jeden Client erforderlich
    - PKI muss vorhanden sein
    - Kennung des Clients wird unverschlüsselt im Zertifikat übertragen

3.7.5 IEEE 802.1X: EAP-Typen (3)

- **EAP-TTLS (Tunneled TLS)**
  - Authentifizierung erfolgt in 2 Phasen
  - Phase 1:
    - TLS-Tunnel wird zwischen Client und RADIUS-Server aufgebaut
    - Authentifizierung des RADIUS-Servers durch ein Zertifikat
  - Phase 2:
    - Authentifizierung mit Kennung und Passwort erfolgt verschlüsselt über den TLS-Tunnel durch PAP (password authentication protocol), CHAP oder MS-CHAP
  - Vorteile gegenüber EAP-TLS:
    - Kein Client-Zertifikat notwendig
    - Benutzerkennung wird verschlüsselt übertragen

3.7.5 IEEE 802.1X: EAP-Typen (4)

- **PEAP (Protected EAP)**
  - Entwicklung von Microsoft und Cisco
  - Funktionsweise fast identisch mit EAP-TTLS
  - Zweistufige Authentifizierung
    - Aufbau eines TLS-Tunnels
    - Benutzerauthentifizierung
  - Benutzerauthentifizierung z.Zt. nur mit MS-CHAP

3.7.5 IEEE 802.1X: EAP-Typen (5)

- **LEAP (Lightweight EAP)**
  - Proprietäres Protokoll von Cisco
  - Funktionsweise vergleichbar mit EAP-MD5
- **EAP-AKA, EAP-SIM**
  - Authentifizierung durch SIM-Karte des GSM- (EAP-SIM) bzw. UMTS-Handys (EAP-AKA)
  - Anwendung bei Hotspots (z.B. mit Smartphones)
  - Accounting über Mobilfunk-Betreiber

3.7.5 802.1X-Clients

	Windows 2000 SP3 oder XP	Mac OS X 10.3	Xsupplicant Linux, FreeBSD	Aegis-Client Meetinghouse	Odyssey-Client Funk Software
EAP-MD5	✓		✓	✓	✓
EAP-TLS	✓	✓	✓	✓	✓
EAP-TTLS		✓	✓	✓	✓
PEAP	✓	✓	✓	✓	✓
LEAP		✓		✓	✓

Aegis-Client: Windows 98/ME/NT/2000/XP, Mac OS X, Linux, Solaris, Pcket PC 2002, Windows Mobile 2003

Odyssey-Client: Windows 98/ME/2000/XP, Pocket PC 2002, Windows Mobile 2003

3.7.5 IEEE 802.1X: Dynamische WEP-Keys und Accounting

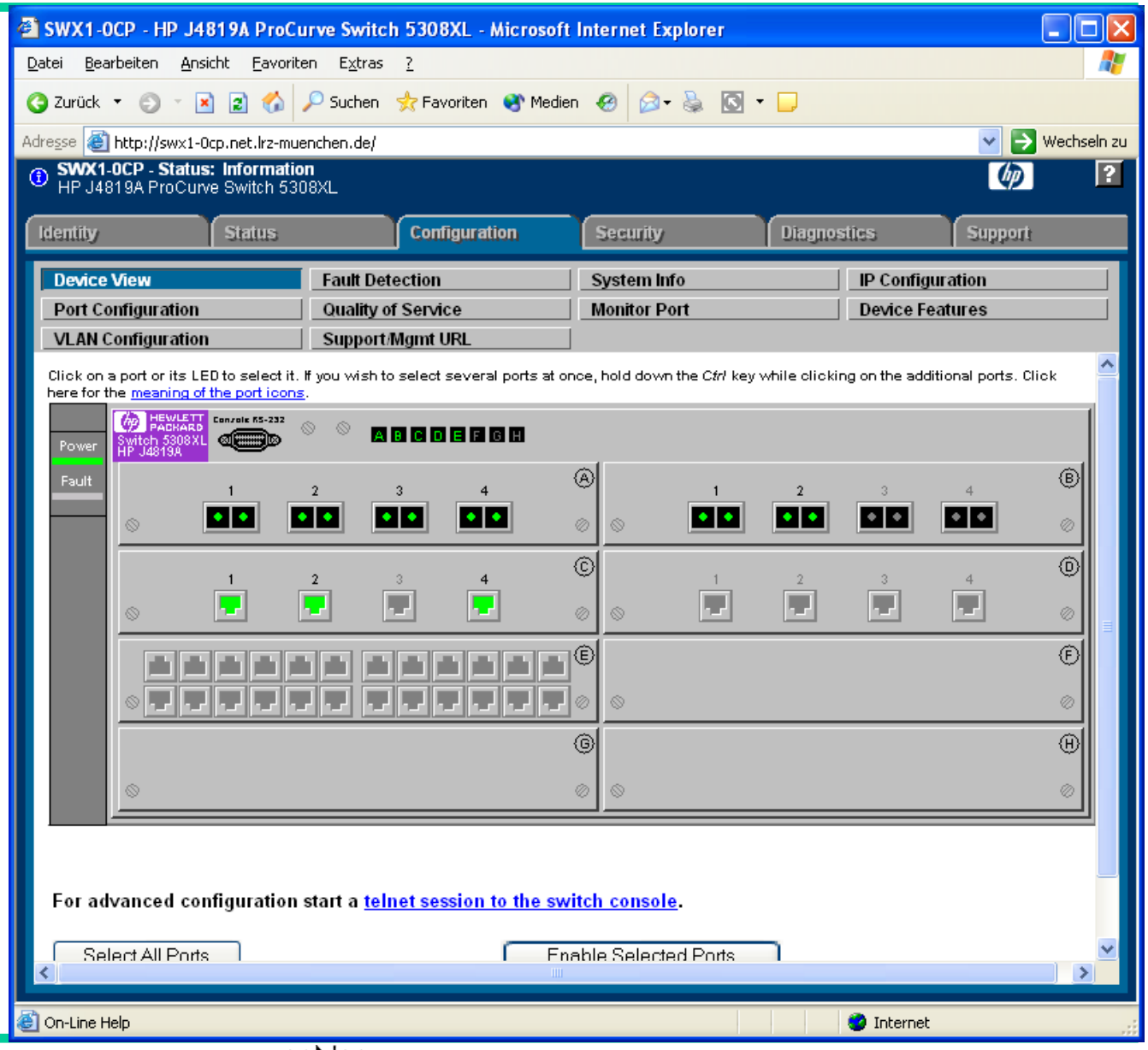
- **Dynamische WEP-Keys**
  - Voraussetzung: Verschlüsselte Verbindung zwischen Client und RADIUS-Server (nicht bei EAP-MD5)
  - Generierung der Session-Keys durch Client und Server
  - Gleichzeitige Verwendung von „Rapid Rekeying" erhöht Sicherheit
- **Accounting**
  - Switch bzw. Accesspoint führen Statistiken
    - Basis ist Interface (physikalischer oder logischer Port)
    - Übertragenes Datenvolumen
    - Uptime eines Interfaces
  - Daten werden bei Verbindungsende an RADIUS-Server geschickt

3.7.6 Produkte

- **Switches sind in unterschiedlichen Leistungsklassen verfügbar:**
  - **Workgroup-Switches**
    - Es wird davon ausgegangen, dass nur ein oder einige wenige Endgeräte an einen Port angeschlossen werden
  - **Enterprise-Switches**
    - Über einen Port können ganze LAN-Segmente erreichbar sein

3.7.7 Management-Werkzeuge

- **Komponenten-spezifische Werkzeuge**
  - Z.B. HP TopTools für das Management der HP-Switches

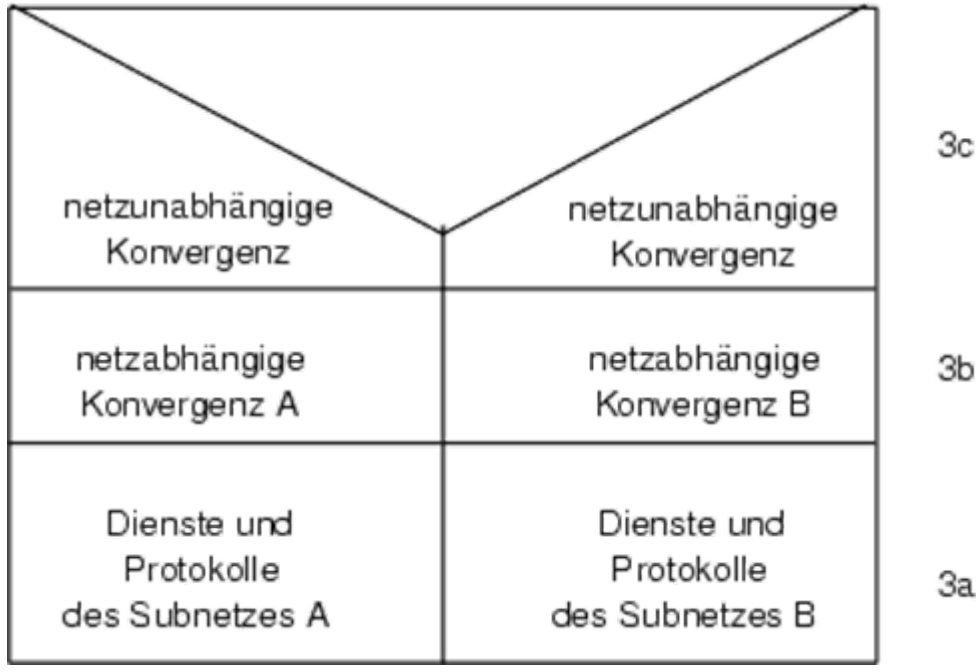


3.8 Router

- 3.8.1 Grundfunktionen eines Routers
- 3.8.2 Adressierungsschema
  - IPv4
  - IPv6
- 3.8.3 Routingverfahren
- 3.8.4 Protokolle in einem IP-Router
- 3.8.5 Funktionsweise eines Routers
- 3.8.6 Brouter
- 3.8.7 Router Management

3.8.1 Grundfunktionen eines Routers

- **Allgemeines**
  - Router sind Level-3-Gateways, d.h. sie verbinden Netze auf der Schicht 3 (genauer: das gemeinsame Protokoll des Verbundnetzes ist das Protokoll der Schicht 3c)

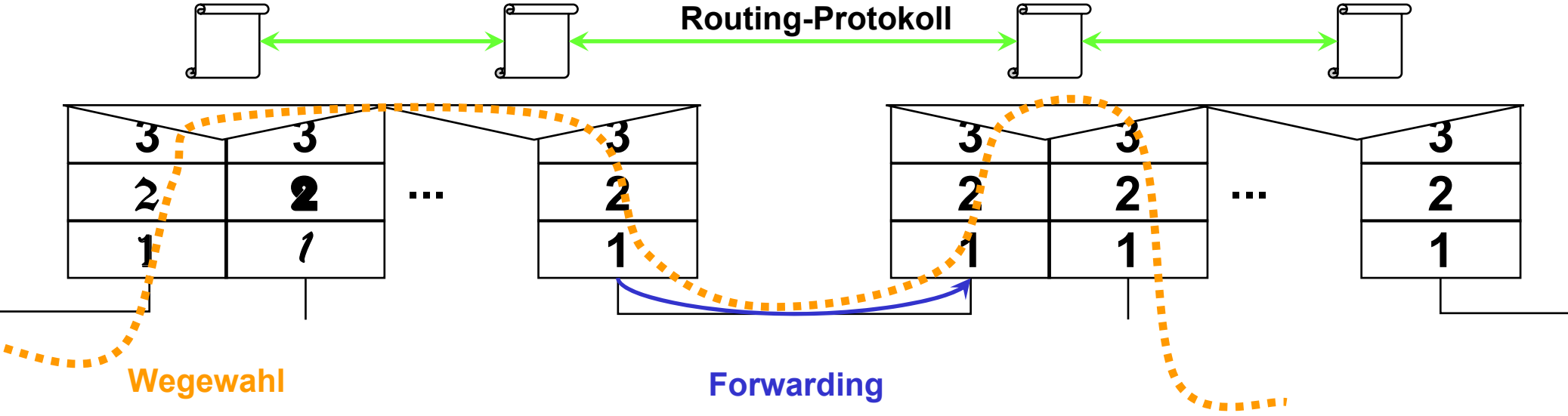


  - In LAN-Standards sind nur die Schichten 1, 2a und 2b festgelegt; alle Geräte, die auf Schicht 3 oder höher arbeiten, gehören zu protokoll-spezifischen Systemen
  - Router ermöglichen die *Strukturierung des Gesamtnetzes* (Verbundnetzes) in logische Subnetzhierarchien, in unterschiedlichen LAN-Technologien
  - Router sind *nicht transparent*

3.8.1 Grundfunktionen eines Routers

- Routing := Wegewahl
- Forwarding := wörtlich „Weiterschieben der Daten“
- Häufig: Konvergenz unterschiedlicher Technologien

- Routing und Forwarding können zeitlich entkoppelt werden
- Verwendung von eigenen Schicht3-Adressen
- Wissen über Wege kann mit Routing-Protokollen „erworben“ werden



3.8.1 Grundfunktionen eines Routers -

- **Beispiele von Schicht-3-Protokollen**

		Routingprotokolle
X.25-PLP	Datex-P	
IP	Internet	RIP, OSPF
ISO-IP	ISO	IS-IS
IDP-XNS	Xerox	
IPX	Netware/Novel	RIP, NLSP
DECNet	Digital/Compaq	DRP
	Appletalk	RTMP

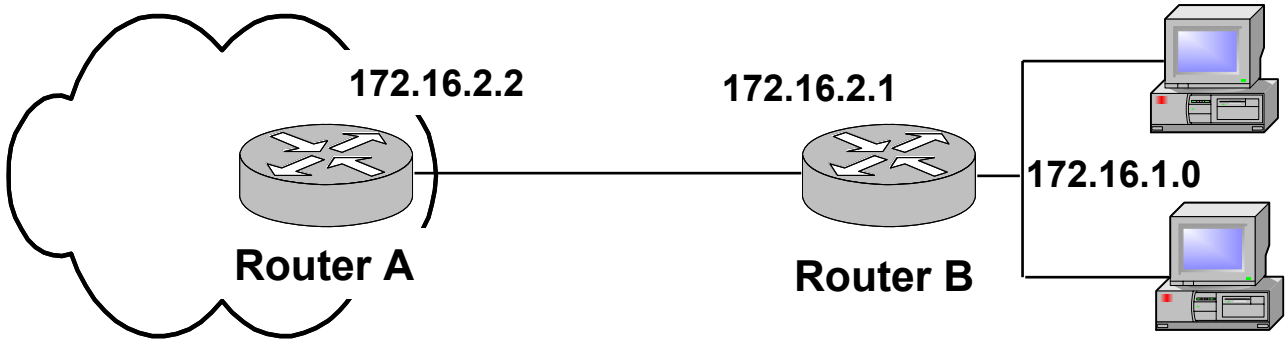
3.8.1 Grundfunktionen eines Routers

- **Statisches Routing**:
  - Basiert, wie der Name schon sagt, auf einer festen Vorgabe des Weges zwischen zwei beliebigen Endsystemen
  - Diese Vorgabe wird bei der Einrichtung, d.h. Installation des Netzes getroffen und in der Regel als feste Tabelle im Router abgespeichert
  - Routing-Tabellen werden explizit durch Netzadministrator verwaltet
  - Routing-Tabellen müssen bei jeder Topologieänderung (auch nach aufgetretenen Fehlern) aktualisiert werden
  - Statische Routen können wichtig sein, wenn das Routing-Protokoll keine Route zu einem bestimmten Ziel aufbauen kann -> „Gateway of Last Resort“

3.8.1 Grundfunktionen eines Routers

❑ Statische Routen

- Beispiel




```
routerA(config) # ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

Zielnetz

IP-Adresse des nächsten Router-Interfaces auf der Route zum Ziel

```
routerB(config) # ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

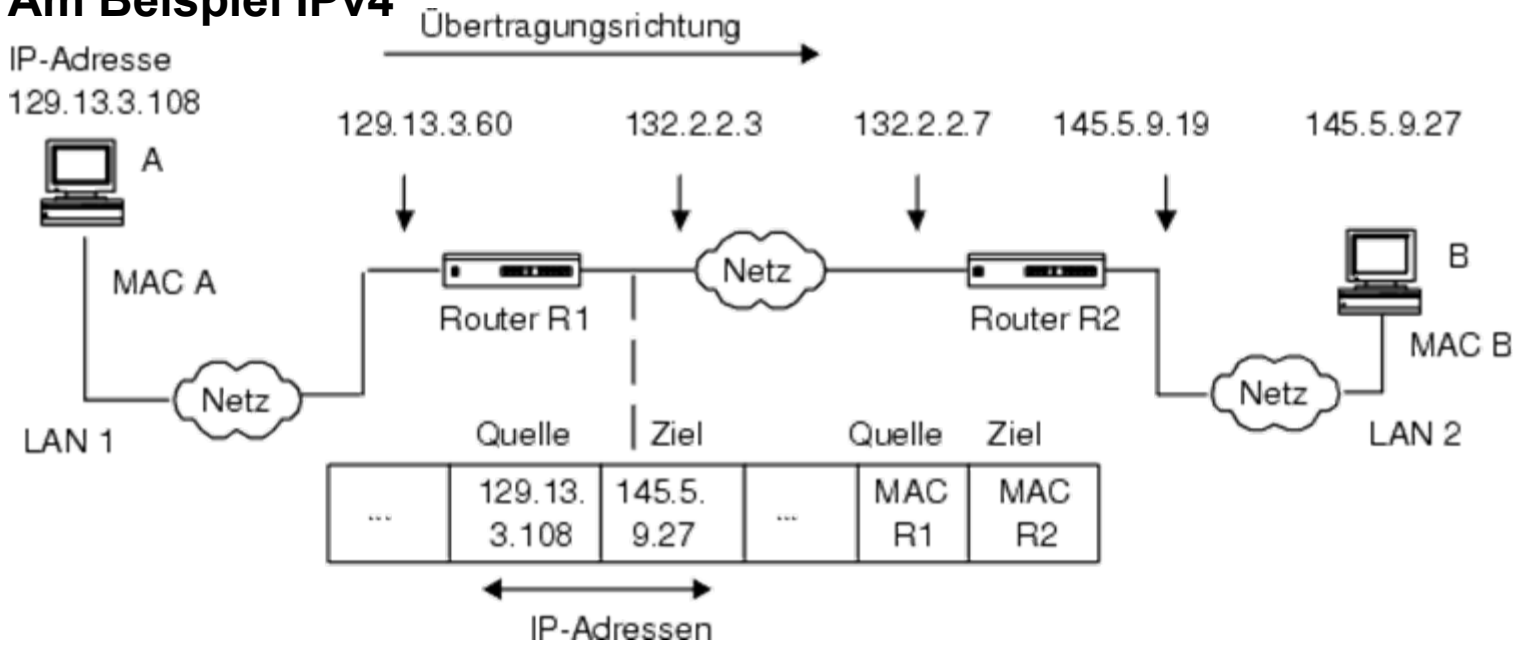
Route zu einem nicht existierenden Unternetz

3.8.1 Grundfunktionen eines Routers

- **Dynamisches Routing**:
  - Router informieren sich gegenseitig über Topologieänderungen mittels geeigneter Routing-Protokolle
  - Die optimale Wegewahl, die durch die so genannte Metrik gewichtet wird, wird nach einer anfänglichen Parametersetzung allein durch das Routing-Protokoll bestimmt und ist so für den Benutzer transparent.
- **Aufgaben in Routern:**
  - Relaying: Paketbezogene Wegewahlentscheidung häufig lastbezogen; Propagierung im allgemeinen nicht DTE-, sondern subnetzbezogen
  - Evtl. Fragmentierung
  - Evtl. Filterung
    (z.B. Broadcast-Unterdrückung oder für Firewall-Zwecke)
  - Router unterstützen multiple Wege;

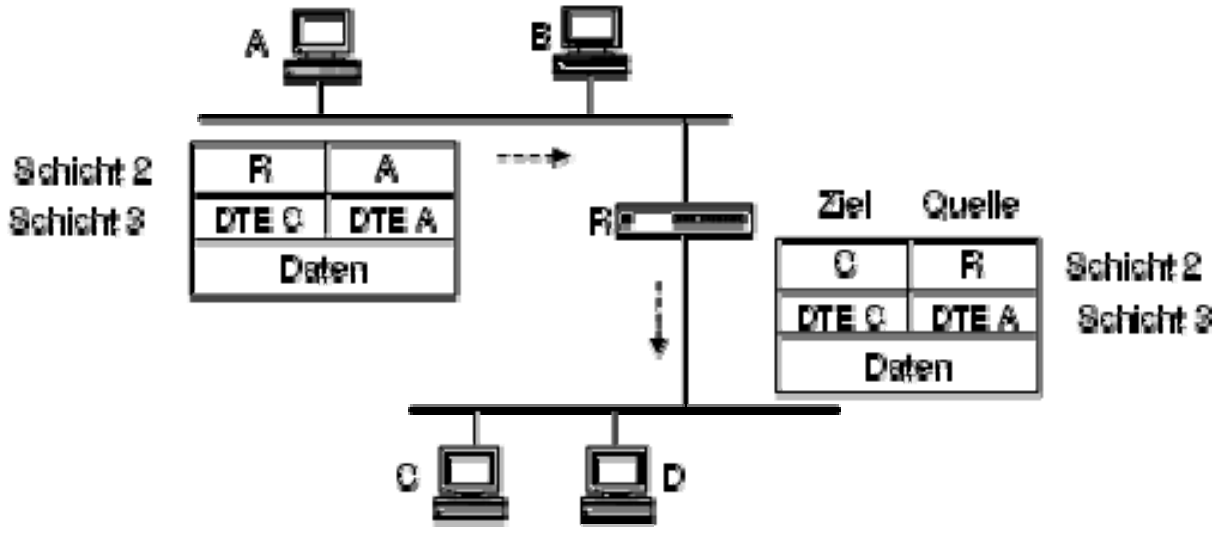
3.8.1 Grundfunktionen: Propagierung von Information

- **Am Beispiel IPv4**



- **Schicht 3: Netzadressen (IP) der Quell- und Zielsysteme**
- **In DTE (Sender) und Router: Einkapseln in MAC-Adressen (Schicht 2). Dies entspricht einem Link zweier benachbarter Systeme**
- **Jeder Router**
  - Ermitteln der IP-Adresse des nächsten Hops auf dem Weg (beispielsweise mittels einer Routing-Tabelle)
  - Abbilden dieser Adresse auf eine Anschlusspunkt (= MAC)-Adresse; Eventuell mittels Adressauflösungsprotokollen (ARP, RARP)

3.8.1 Beispiel: Propagierung von Nachrichten



- MAC-Adressen müssen nur im jeweiligen Subnetz eindeutig sein; A,B,C,D sind hier jeweils Netzadressen;
- neben der Adressumsetzung auf der MAC-Ebene muss Router gegebenenfalls auch die
- Prüfsumme neu bestimmen
- -> Verarbeitung aufwendiger als bei Bridge oder Hub

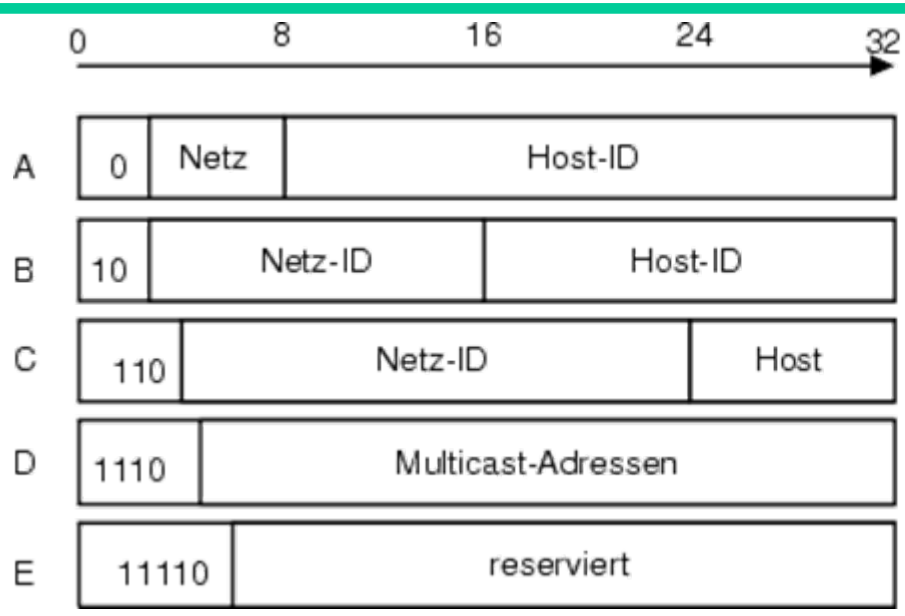
3.8.2 Adressierungsschema

- **Global eindeutige Adressierung auf Schicht 3c**
- **Adressierung mittels Router**
  - Router werden direkt adressiert
  - Router verarbeiten nur Pakete, die an sie direkt adressiert sind
  - Bridges puffern alle Frames eines angeschlossenen Subnetzes -> Entscheidung, ob Löschen oder Propagieren durch Bridge

Üblicherweise: hierarchisches Adressschema mit Unterscheidung der Adressen von Teilnehmerstationen und Netzkennungen

- **IP-Adresskonzept**
- **ISO-Netzadressen (NSAP-Adressen)**
- **IEEE-802-Adressen (flache Adressen)**

3.8.2 Adressierungsschema: IPv4



	Subnetze	Hosts
A	126	16.777.214
B	16.382	65.534
C	64.547	254

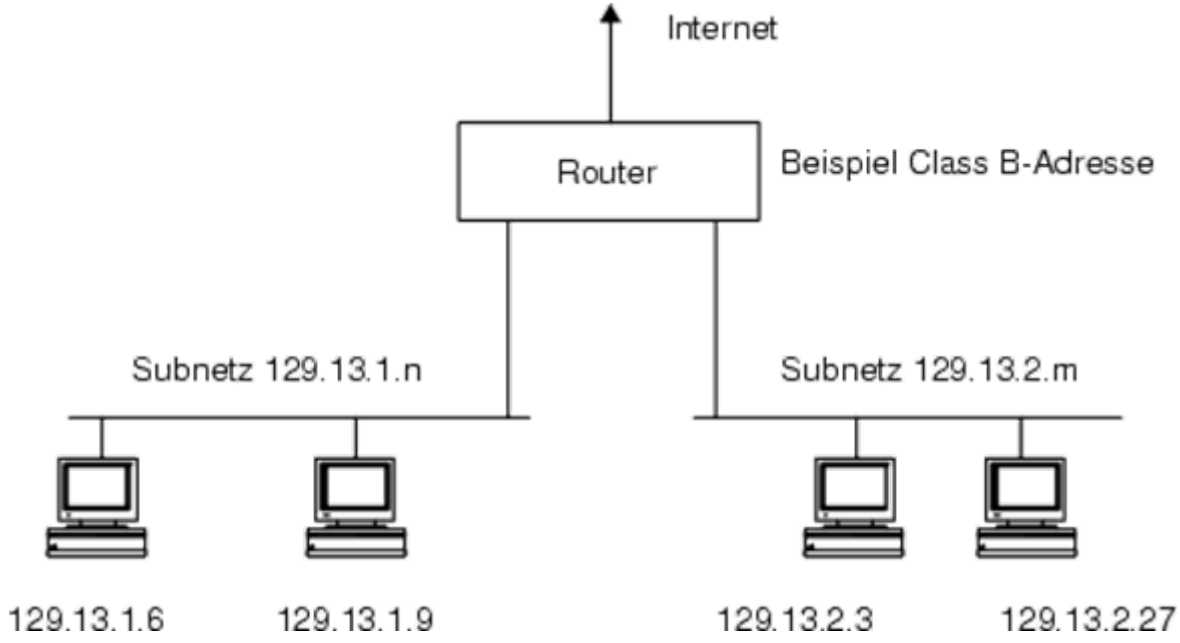
- **Die Adresse besteht aus Netz-IDs und Host-IDs. Nur die Netz-IDs werden zentral vom Network Information Center vergeben; die Klasse gibt an, wie groß der Byte-Anteil der Netz-IDs ist**
- **Adressklassen:**
  - **Klasse A: Adressbereich 1.0.0.0 – 127.255.255.255**
  - **Klasse B: Adressbereich 128.0.0.0 – 191.255.255.255**
  - **Klasse C: Adressbereich 192.0.0.0 – 223.255.255.255**
  - **Klasse D: Adressbereich 224.0.0.0 – 239.255.255.255 (verwendet durch Videokonferenzsysteme, z.B. durch Mbone-Werkzeuge)**
  - **Klasse E: Adressbereich 240.0.0.0 – 247.255.255.255**

3.8.2 Adressierungsschema: IPv4

- **Sondernummern: Es existieren eine Reihe von IP-Adressen mit einer speziellen Bedeutung**
  - Alles 0: dieser Host
  - Alles 1: Broadcast
  - Netz-ID = 0: dieses Netz
  - Host-ID = 1: Broadcast in Teilnetz
  - 127 * x * y * z: Schleifentest

3.8.2 Adressierungsschema: IPv4 - Subnetze

- **Subnetzadressen ermöglichen weitere Strukturierung innerhalb des Netzes**



1. Subnetz hat Adressen 129.13.1.n

2. Subnetz hat Adressen 129.13.2.m

Durch Subnetzmaske werden die ersten 3 Bytes als Netzkennung ausgewertet. Subnetzmaske lautet hier:

11111111 11111111 11111111 00000000

3.8.2 Adressierungsschema: IPv4 – Subnetze

- **Beispiele für Netz- und Broadcast-Adressen in den unterschiedlichen IPv4-Adressklassen**

Netzklasse	Adresse des Netzes	Subnetz-Maske	Broadcast-Adresse in diesem Netz
A	126.0.0.0	255.0.0.0	126.255.255.255
B	139.1.0.0	255.255.0.0	139.1.255.255
C	219.1.123.0	255.255.255.0	219.1.123.255

- **Subnetting: Aufteilung eines IP-Netzes in mehrere Teilnetze (-> Netzmaske)**
- **Supernetting: mehrere einzelne Netze zusammenzufassen**
  - Mehrere Netze können durch ein gemeinsamen IP-Präfix adressiert werden -> Verringerung der Komplexität der Routing-Tabellen

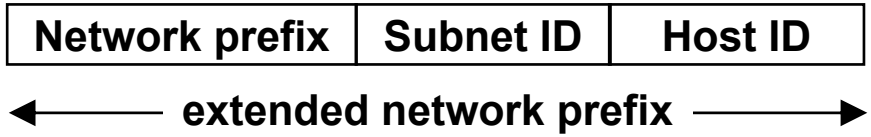
3.8.2 Adressierungsschema: IPv4 – CIDR

- Classless Interdomain Routing (CIDR)
  - Ursprünglich als Interimslösung bis zur Einführung von IPv6
  - Beschreibt ein Verfahren zur effektiveren Nutzung der bestehenden 32 Bit umfassenden IP-Adresse (RFC 1517 -1520)
  - Bei diesem Verfahren werden IP-Adressen zusammengefasst, wobei ein Block von aufeinander folgenden IP-Adressen der Klasse C als ein Netz behandelt werden kann
  - Das CIDR-Verfahren reduziert die in Routern gespeicherten Routing-Tabellen durch einen Präfix in der IP-Adresse
  - Mit diesem Präfix kann ein großer Internet Service Provider bzw. ein Betreiber eines großen Teils des Internets gekennzeichnet werden
  - Dadurch können auch darunter liegende Netze zusammengefasst werden; so genanntes Supernetting
  - Die Methode wird u.a. im BGP-Protokoll eingesetzt

3.8.2 Adressierungsschema: IPv4 – CIDR

❑ Classless Interdomain Routing (CIDR)

- Struktur:



- Notation: `<network>/<prefix length>`

- Beispiel: `192.168.121.0/26`
  Die 26 ersten Bits bilden Netz-ID

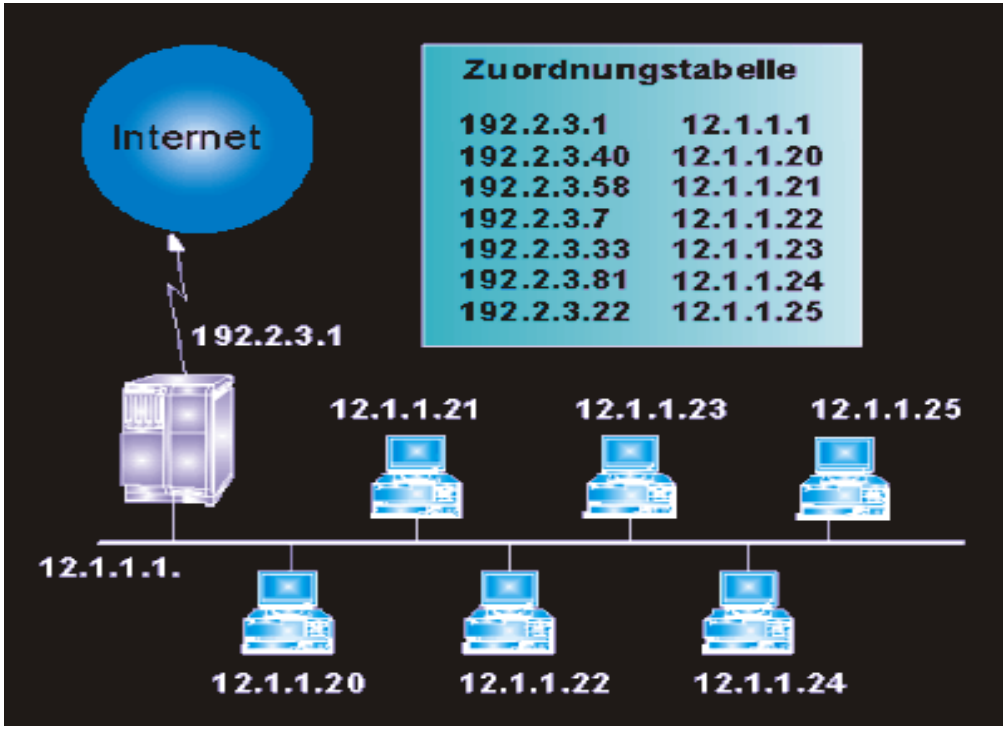
- Zweck: - Grenzen zwischen Netz-ID und Host-ID werden flexibel
  - „Vorwahl“ eines Netzes, repräsentiert IP-Adressblock

3.8.2 Adressierungsschema: IPv4 – NAT

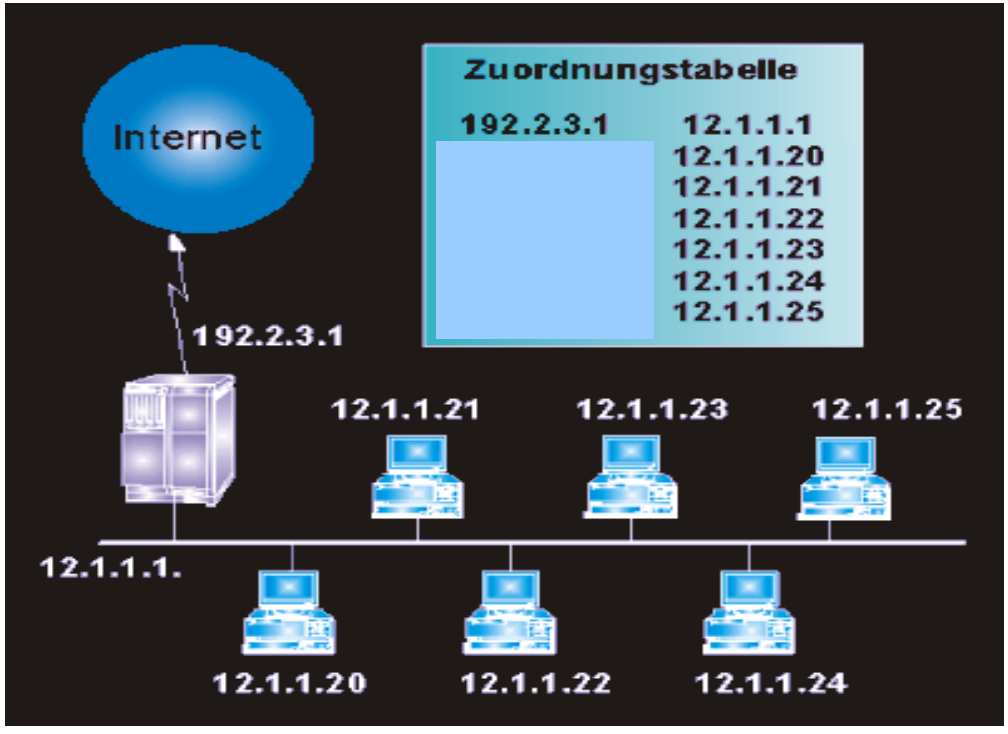
- **NAT (network address translation)**
  - Ein Verfahren, um eine IP-Adresse für mehrere Rechner innerhalb von Firmennetzen (Intranets) zur Kommunikation ins Internet zu verwenden, RFC 1918, RFC 2663
  - NAT kann nur an „Netzgrenzen“ verwendet werden
  - Das NAT-Verfahren registriert (nicht öffentliche) IP-Adressen eines Intranets und ordnet diese meist einer öffentlich registrierten IP-Adresse zu
  - Der Vorteil dieses Verfahrens liegt darin, dass Rechner innerhalb des Unternehmensnetzes keine öffentlichen IP-Adressen benötigen aber dennoch Kommunikationsrelationen ins Internet aufbauen können
  - Rechner, die Kommunikationsrelationen zu anderen, externen Rechnern aufbauen, erhalten beim Routing einen Tabelleneintrag

3.8.2 Adressierungsschema: IPv4 – NAT

- Adress-Zuordnung 1 zu 1



- Adress-Zuordnung 1 zu n



3.8.2 Adressierungsschema: IPv6

- **Internet-Protokoll IPv6 (RFC 2460, 2466) besteht aus 128 Bit statt bisher 32 Bit**
- **Eigenschaften**
  - Längere Adressen (128 Bit anstatt 32 Bit)
  - Im allgemeinen ist IPv6 nicht mit IPv4 kompatibel (aber mit anderen Protokollen wie z.B. TCP, ICMP, IGMP, OSPF, BGP, DNS)
  - Vereinfachung des Headers (7 anstatt 13 Felder)
  - Sicherheit
- **Notation**
  - 8 Gruppen von je vier hexadezimalen Ziffern, getrennt durch Doppelpunkte, z.B. 8000:0000:0000:0000:0123:4567:89AB:CDEF
  - IPv4-Adressen können wie folgt geschrieben werden ::192.31.20.46

3.8.2 Adressierungsschema: IPv6

- **IPv6 unterstützt 3 Adressierungsarten:**
  - Unicast
  - Multicast
  - Anycast (identifiziert eine Reihe von Komponenten; die Nachricht wird der „nächsten“ Komponente zugestellt („nächste“ wird durch das Routing-Protokoll definiert))
- **Bisher wird IPv6 nur sehr zögerlich unterstützt**

3.8.3 Routing-Verfahren

- **Kombination von Forwarding und Wegewahl**
- **Wesen eines Routing-Verfahrens:**
- **Korrektheit**
  - Einfachheit
  - Robustheit
  - Stabilität
  - Fairness
  - Optimalität
  - Art der Verbindung: verbindungslos (Datagrammdienst) oder verbindungsorientiert (virtuelle Verbindung)

	virtuelle Verbindung	Datagramm
Zieladresse	nur beim Verbindungsaufbau notwendig	in jedem Paket notwendig
Fehlerbehandlung	im Subnetzdienst	in höheren Schichten (End-DTE´s)
Flußkontrolle	durch Subnetz	durch höhere Schichten (End-DTE´s)
Reihenfolge	Ankunft wie Absenderzeitenfolge	willkürliche Ankunft möglich
expliziter Verbindungsauf-/abbau	ja	nein

3.8.3 Einteilung der Routing-Verfahren

- **Unterscheidung nach**
  - Statisch oder dynamisch (adaptive)
  - Zentral oder verteilt
- **Verteilte adaptive Routing-Algorithmen zur Bestimmung der Wegewahlinformation**
  - **Distanzvektoralgorithmus (DVA)**
    - Routing nach dem Entfernungsvektor
  - **Link State Algorithmen (LSA)**
    - Routing nach dem Verbindungszustand

3.8.3 Distanzvektoralgorithmen (DVA)

- **DVA wird auch Bellman-Ford Verfahren genannt**
- **Prinzip**
  - Jeder Router verwaltet eine Tabelle (einen Vektor), die für jedes Ziel die bestmöglich bekannte Entfernung und die zu verwendende Leitung enthält
  - Es wird angenommen, dass jeder Router die „Entfernung“ zu seinen Nachbarn kennt
  - **Metrik** ist der kürzeste Weg
    - Geringste Anzahl von Hops -> RIP
    - Geringste Übertragungszeit -> HELLO; Geringste Anzahl der auf dem Weg berührten Router
  - Algorithmus ist lokaladaptiv z.B. alle 30 sec komplette Routing-Information an alle Nachbarn
    -> Informationslast O(#Router, #Subnetze)

3.8.3 Distanzvektoralgorithmen (DVA)

- **Charakteristisch:**
  - Einfache Implementierung
  - Broadcast der Routing-Info (-> Netzlast)
  - Schrittweise Ausbreitung (-> Schleifengefahr). Bei 15 Hops: 15 x 30 sec = 7 min. Einträge in Routing-Tabelle des RIP werden alle 180 sec gelöscht, falls keine Änderung
  - Jeder Router berechnet aus allen Informationen seine Routing-Tabelle
  - Hat in der Praxis einen großen Nachteil (d.h. der Algorithmus führt zu richtigen Lösung, tut dies aber nur sehr langsam)
  - RIP definiert in RFC 1058, RIPv2 definiert in RFC 2453
  - Einsatz als Interior Gateway Protocol
  - Zunehmende Ablösung durch OSPF

3.8.3 Link State Algorithmen (LSA)

- **Prinzip:**
  - Netz wird als gerichteter Graph angesehen d.h. hierarchische Struktur
  - Propagierung der Routing-Info nur an Nachbar-Router innerhalb der eigenen Hierarchieebene
  - Basis ist der Dijkstra-Algorithmus; Quellensenken-Baum-Berechnung
  - Routing-Metrik = f (Übertragungs-Kapazität, aktuelle Warteschlangenlänge an Ports, Verzögerung etc.)
  - Routing Propagation i.a. schneller als bei DVA
  - Beispiel: OSPF („Open Shortest Path First“)

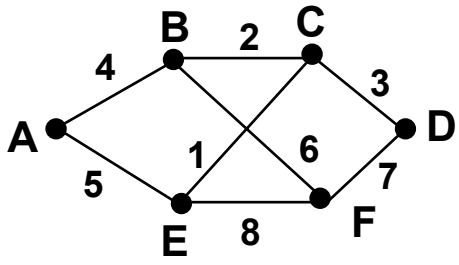
3.8.3 Link State Algorithmen (LSA)

- **Ermittlung der Nachbar-Router**
  - Jeder Router sendet ein spezielles HELLO-Paket auf jeder Punkt-zu-Punkt-Leitung
  - Der Router am anderen Ende muss eine Antwort zurücksenden, durch die er seine Identität bekannt gibt
- **Ermittlung der Leitungskosten**
  - Übertragungszeit zu ermitteln mit Aussenden eines speziellen ECHO-Pakets; die andere Seite muss es sofort wieder zurücksenden
  - Durch Messen der Hin- und Rückreisezeit (geteilt durch zwei) kann der sendende Router die Übertragungszeit vernünftig abschätzen

3.8.3 Link State Algorithmen (LSA)

❑ Link-State-Pakete erstellen

- Beispiel



Link-State-Pakete

A	
Folge-Nr.	
Alter	
B	4
E	5

B	
Folge-Nr.	
Alter	
A	4
C	2
F	6

C	
Folge-Nr.	
Alter	
B	2
D	3
E	1

D	
Folge-Nr.	
Alter	
C	3
F	7

E	
Folge-Nr.	
Alter	
A	5
C	1
F	8

F	
Folge-Nr.	
Alter	
B	6
D	7
E	8

❑ Link-State-Pakete verteilen

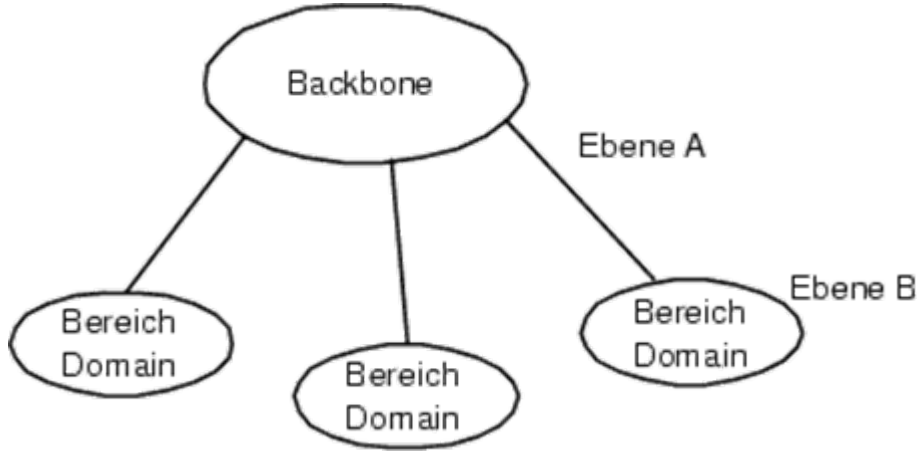
- Anwendung von Flooding
- Jedes Paket enthält eine Folgenummer, die bei jedem neu ausgesendeten Paket erhöht wird
- Router vermerken alle Paare (Quell-Router, Folgenummer)
  Ein neues Link-State-Paket wird mit der Paketliste verglichen; ist es neu, wird es an alle Leitungen außer derjenigen, auf der es eingegangen ist, ausgegeben

3.8.3 Link State Algorithmen (LSA)

- **Charakteristisch:**
  - Propagierung nur bei Topologieänderung, Berechnung ziemlich aufwendig
  - Angemessen für regelbasiertes Routing, Unterstützung von Dienstqualitäten
  - Keine Schleifengefahr
  - Schnelle Propagierung, deshalb mehr Hops (z.B. OSPF:1024)
  - Beispiele von Protokollen: OSPF, IS-IS (Intermediate System – Intermediate System)

3.8.3 Routing-Bereiche – Hierarchisches Routing

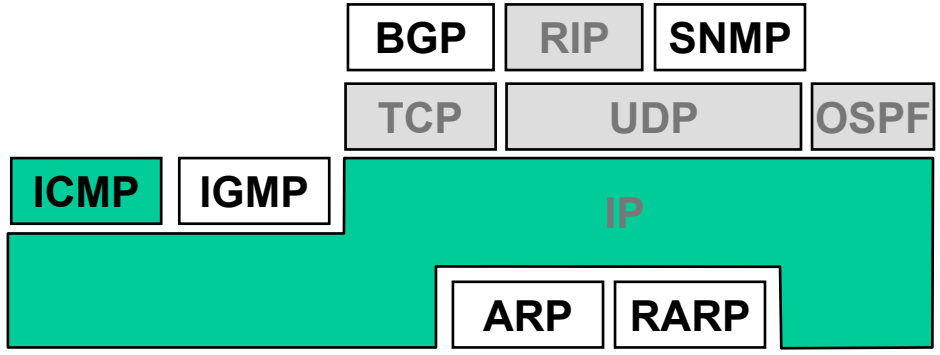
- **Problemstellung:**
  - Anwachsen der Routing-Tabellen
- **Einsatzbereich im Internet:**
  - Ebene A (EGP): („Exterior Gateway Protocol“), domänen-übergreifend
    - Internet: BGP
  - Ebene B (IGP): innerhalb der Domäne
    - Internet: RIP, OSPF
    - ISO: IS-IS, ES-IS



Autonomes System (AS): mehrere Netze, die unter einer gemeinsamen technischen Administration stehen sowie ein internes Routing-Protokoll und einheitliche Metriken verwenden

3.8.4 Protokolle in einem IP-Router

- **IP ist ein Schicht 3c-Protokoll, Datagramm-orientiert; IP-Protokoll unterstützt:**
  - Fragmentierung
  - Diensttypkennung
  - Zeitstempel, Hop Count

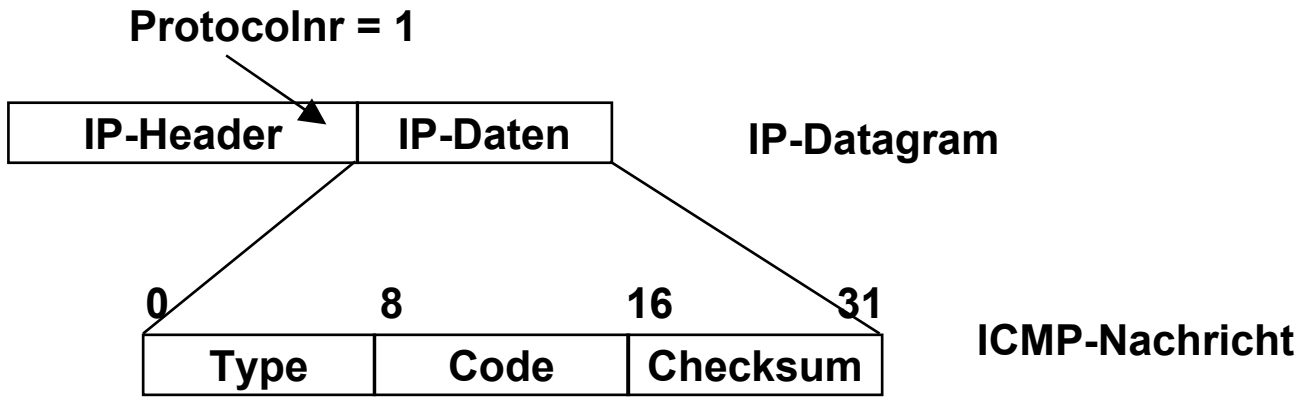


- **ICMP: Internet Control Message Protocol (RFC 792, 1256)**
  - Fehlermeldemechanismus, mit dem ein Router anderen Routern oder auch DTEs Fehlermeldungen oder Steuernachrichten schicken kann
  - Die Meldungen des ICMP-Protokolls sind in zwei Klassen definiert:

Fehlermeldungen	Informationsmeldungen
- DEE nicht erreichbar,	- DEE nicht erreichbar
- Wegumleitung,	- Zeitmessung
- Ressourcen nicht mehr nutzbar	- Adressmaske
- Zeit abgelaufen	- Router-Findung
- Parameterproblem	- Echo (Erreichbarkeit prüfen)

3.8.4 Protokolle in einem IP-Router

ICMP



- Type: Unterscheidung von Nachrichten (Beispiele)

3 Destination unreachable + Code	8/0 Echo Request / Reply
4 Source Quench	9/10 Router Discovery (Advertisement / Solicitation)
5 Redirect Message	13/14 Time Stamp Request / Reply
11 Time Exceeded	15/16 Information Request / Reply
12 Parameter Type Problem	17/18 Adress Mask Request / Reply

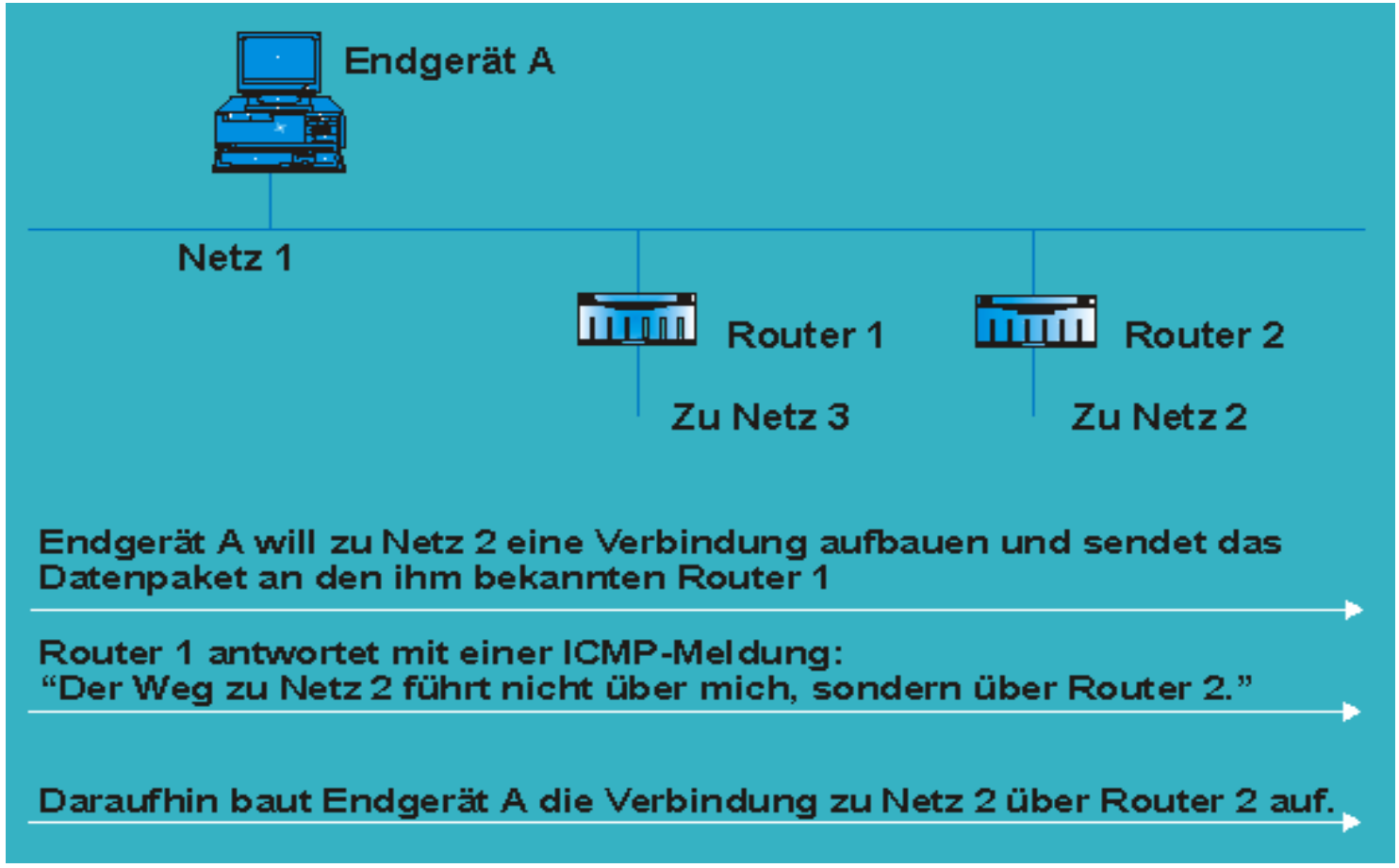
- Code für Type 3 Nachrichten (Auswahl):

0 Net Unreachable	4 Fragmentation Needed and Don't Fragment was Set
1 Host Unreachable	5 Source Route Failed
2 Protocol Unreachable	6 Destination Network Unknown
3 Port Unreachable	7 Destination Host Unknown

3.8.4 Protokolle in einem IP-Router

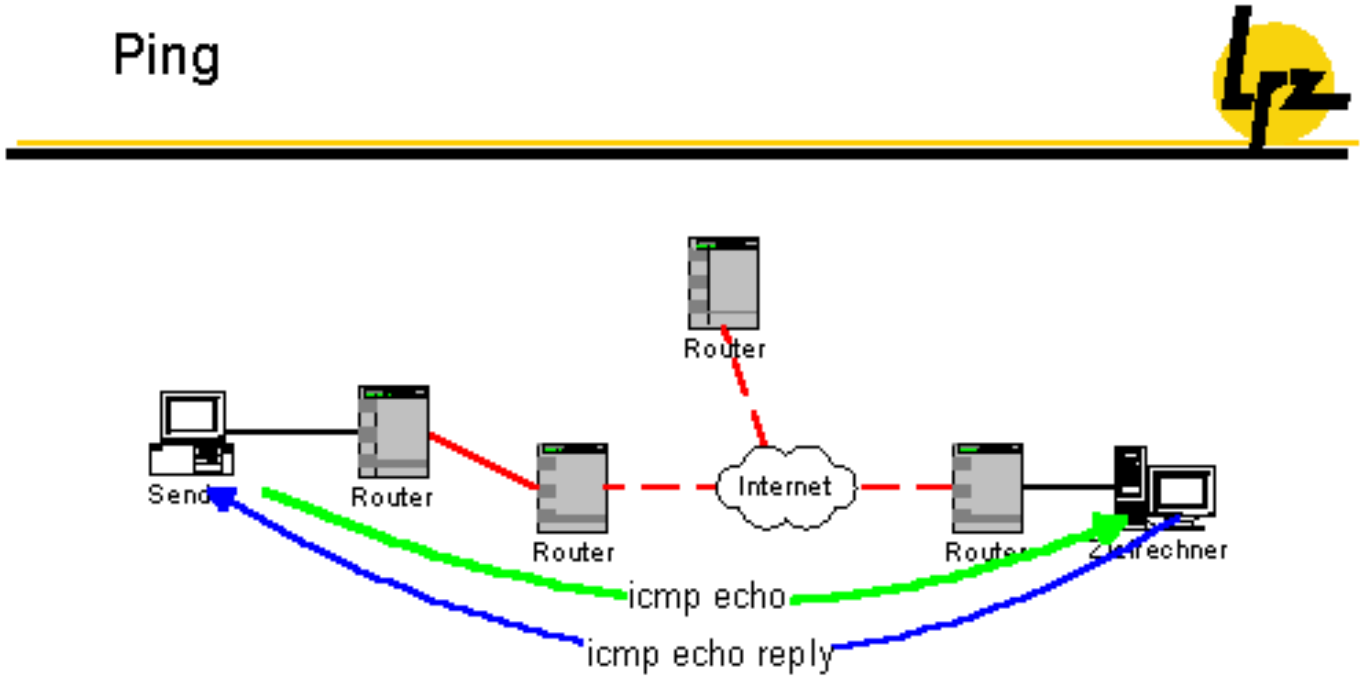
ICMP: Internet Control Message Protocol

- Funktionsablauf



3.8.4 Protokolle in einem IP-Router

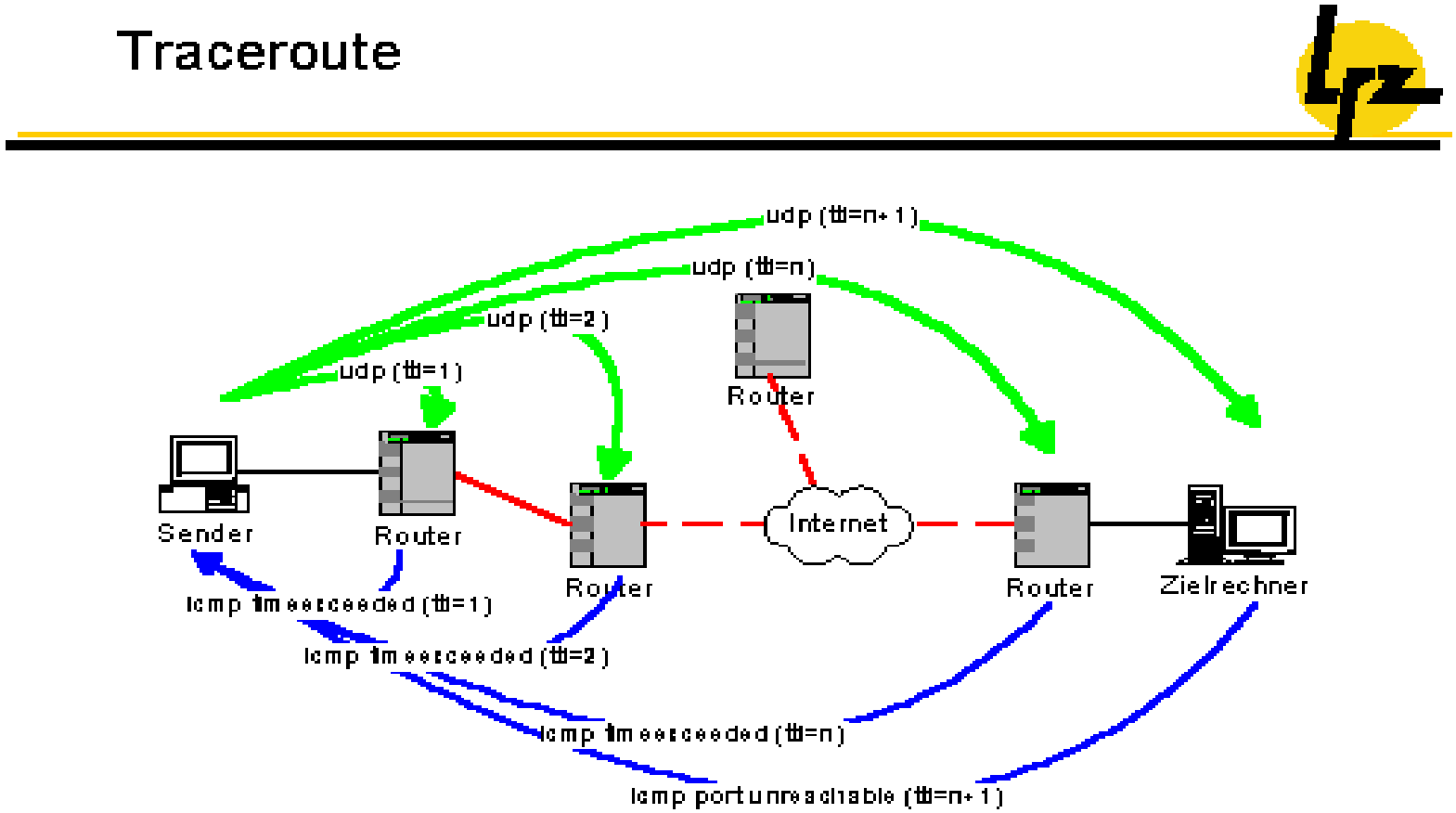
- ICMP: Internet Control Message Protocol: Basis für ping
  -



Verbindungsprobleme

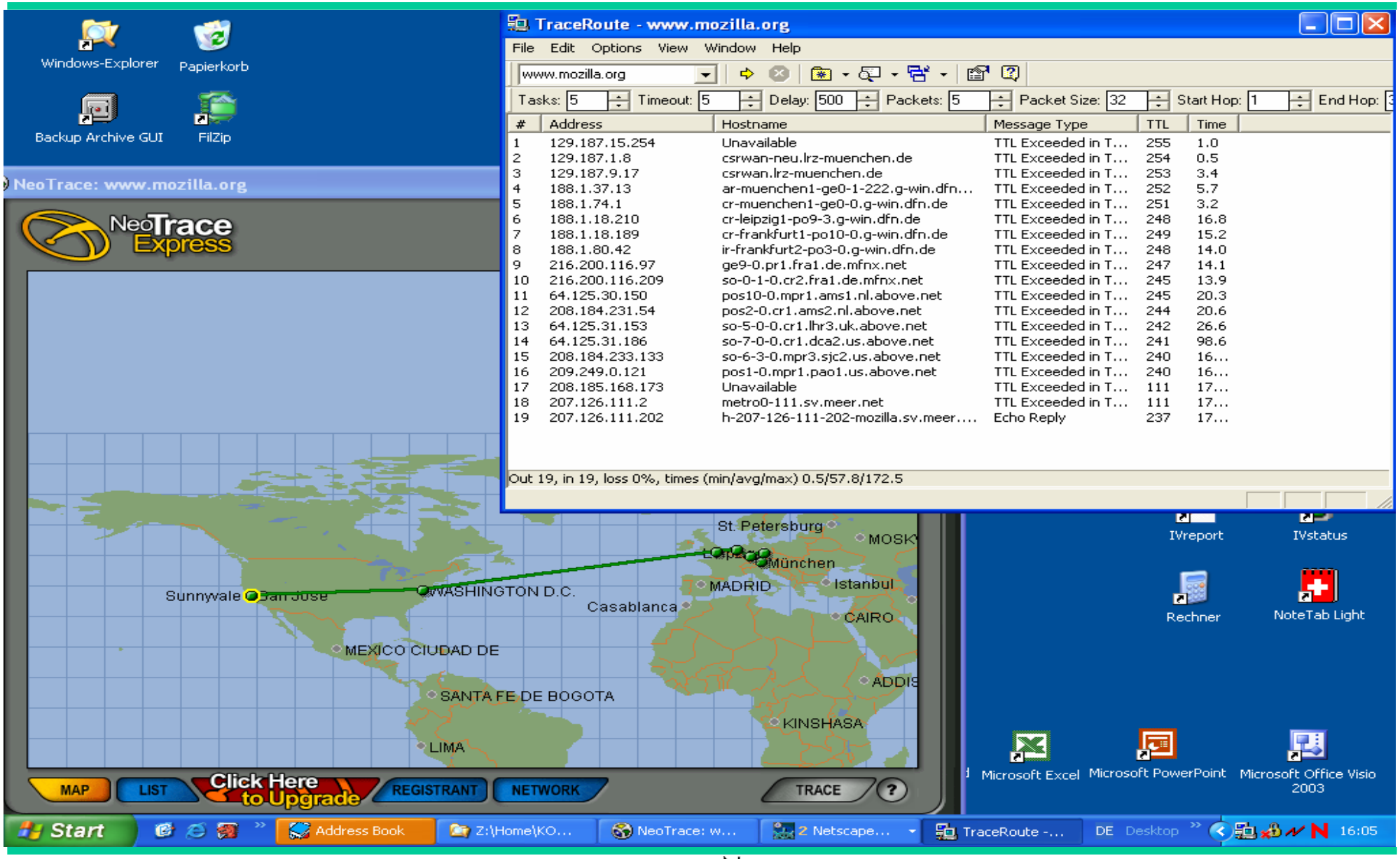
3.8.4 Protokolle in einem IP-Router

- ICMP: Internet Control Message Protocol: Basis für traceroute

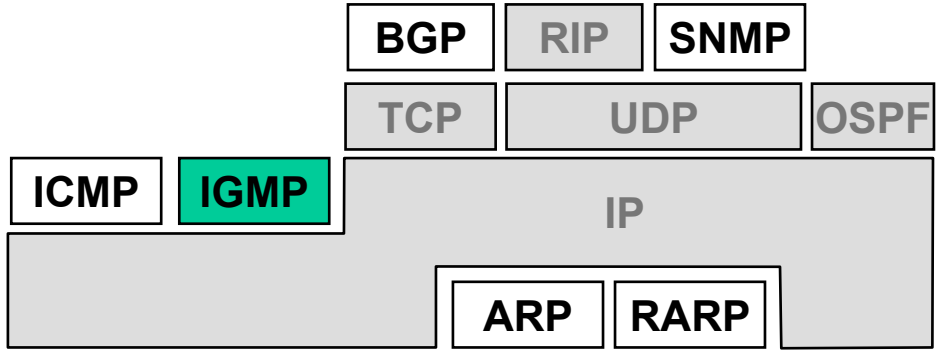


Verbindungsprobleme

3.8.4 Protokolle in einem IP-Router



3.8.4 Protokolle in einem IP-Router



- **IGMP: Internet Group Management Protocol**
  - Dient zur Verwaltung von Gruppen (im Zusammenhang mit Class D-Adressen)
  - Das IGMP-Protokoll wird für IP-Multicast, also für die Gruppenkommunikation eingesetzt
  - Das IGMP-Protokoll baut auf dem IP-Protokoll auf, d.h. es wird von IP behandelt, als sei es ein Protokoll einer höheren Schicht
  - IGMP-Daten werden immer mit einem vollständigen IP-Header verschickt, die eigentlichen IGMP-Meldungen befinden sich im anschließenden IP-Datenteil

3.8.4 Protokolle in einem IP-Router

❑ IGMP – Problemfelder im Zusammenhang mit IP-Multicast (MC)

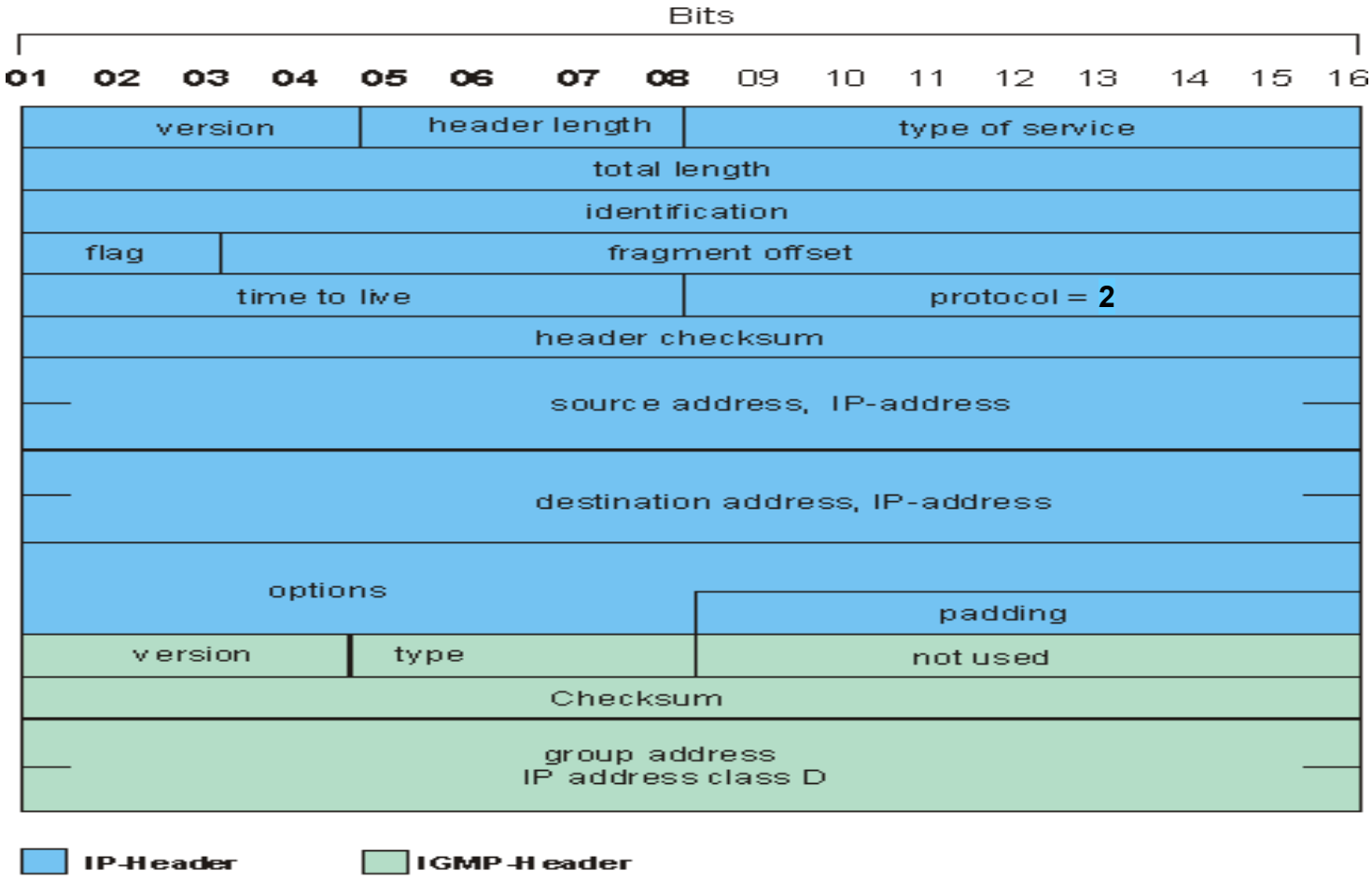
- Endsystemregistrierung: Empfänger eines IP-MC-Paketes muss Mitglied einer MC-Gruppe sein. Gruppenverwaltung mit IGMP
- Adress-Mapping: Abbildung von IP-MC auf IP-Adressen bzw. MAC (MC)-Adressen
- Multicast-Routing: Infos über MC-Gruppen verteilen und pflegen (spezielle Protokolle: PIM, MOSPF, DVMRP)

- Nicht jeder Router ist auch MC-Router
- IP-MC-Adressen sind Class-D-Adressen
  Reservierte Bereiche (All-Hosts, All-Routers, locale – RFC 1700)

3.8.4 Protokolle in einem IP-Router

❑ IGMP: Internet Group Management Protocol

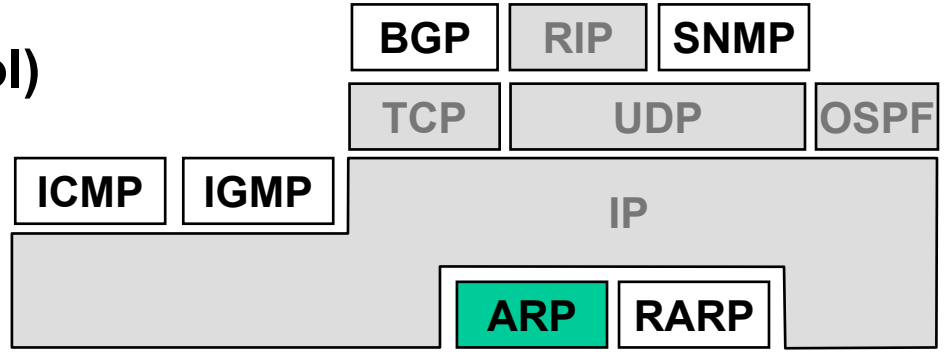
- Datenrahmen



3.8.4 Protokolle in einem IP-Router

- **IGMP – Version 2 in RFC 2236**
  - IGMP-Nachricht als Payload in IP, Protocol Type = 2
  - Type-Felder für Host / MCRouter Kommunikation
    - MembershipQuery (0x11): Welche Gruppen, welche Mitglieder
    - Version1 MembershipRequest (0x12)
    - Version2 Mebership Report (0x16)
    - LeaveGroup (0x17)
    - DVMP-Nachricht
    - Maximum Response Time
    - Gruppenadresse
  - Ein MC-Router sendet alle 100 sec eine MembershipQuery an alle Endsysteme im LAN und führt Buch über Gruppen und Mitglieder

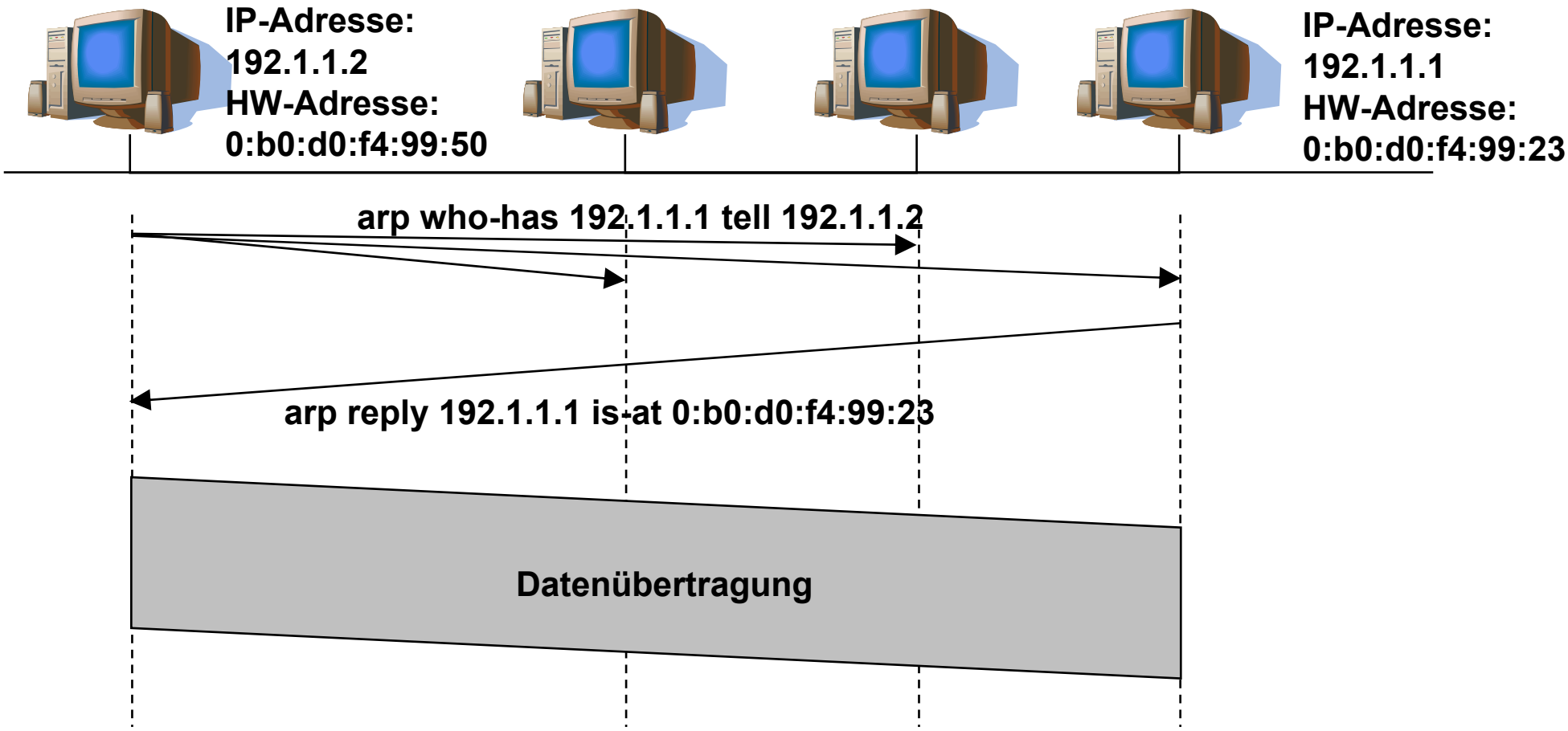
3.8.4 Protokolle in einem IP-Router (Fortsetzung)



- **ARP (Address Resolution Protocol)**
  - ARP ist ein typisches ES-IS-Protokoll, das dazu dient, die MAC-Adressen in die zugehörigen IP-Adressen umzuwandeln, damit überhaupt eine Kommunikation auf der Vermittlungsschicht mittels des IP-Protokolls stattfinden kann
  - Das ARP-Protokoll legt zu diesem Zweck Mapping-Tabellen an, die die MAC-Adressen den Netzwerkadressen zuordnen

3.8.4 Protokolle in einem IP-Router (Fortsetzung)

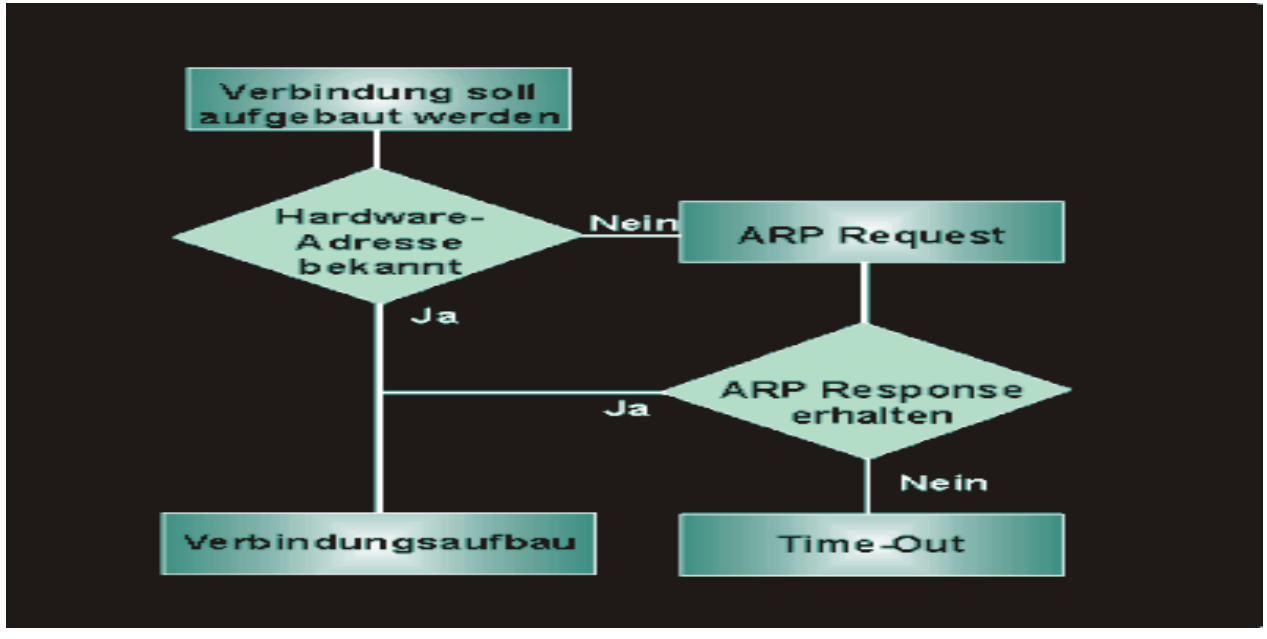
- **ARP (Address Resolution Protocol)**
  - Funktionsablauf



3.8.4 Protokolle in einem IP-Router (Fortsetzung)

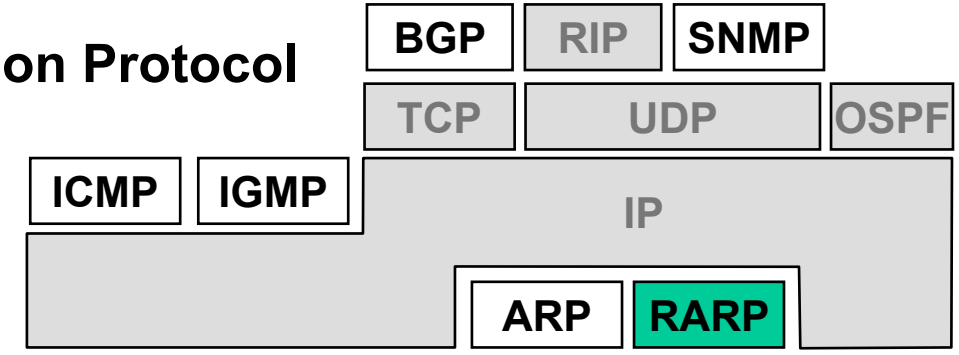
ARP (Address Resolution Protocol)

- Hat ARP keinen Eintrag in seiner Tabelle, so wird über eine Anfrage an alle Netzknoten (Broadcast) die Ethernet-Adresse der zugehörigen Internet-Adresse erfragt
- Nur Netzknoten mit einem Eintrag zu dieser IP-Adresse antworten auf die Anfrage
- Die Antwort auf den ARP-Broadcast wird in der ARP-Adresstabelle gespeichert
- Flussdiagram



3.8.4 Protokolle in einem IP-Router (Fortsetzung)

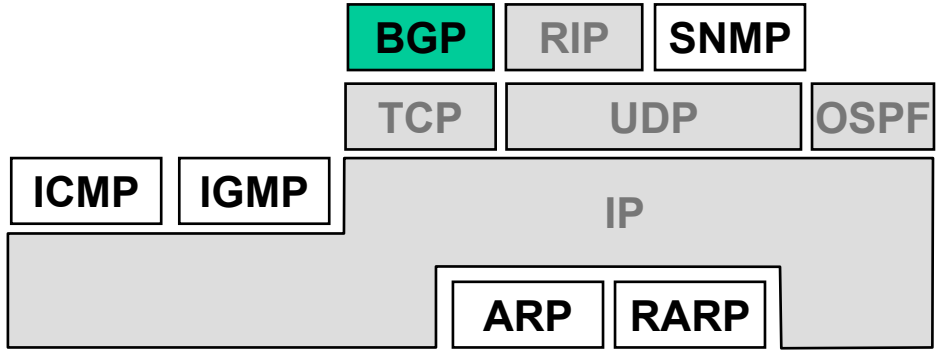
❑ RARP: Reverse Address Resolution Protocol



- Station kann eine IP-Adresse zu ihrer MAC-Adresse anfordern
- Anfrage als Broadcast
- Der RARP-Server (beliebiger Rechner) beantwortet Anfrage und liefert IP-Adresse zur MAC-Adresse des Anfragenden
- RARP arbeitet auf Schicht 2, ist aus dem Address-Resolution-Protokoll (ARP) abgeleitet und benutzt ähnliches Datenformat
- Adressverwaltung durch einen Server ermöglicht zentrale Adrerssvergabe

3.8.4 Protokolle in einem IP-Router (Fortsetzung)

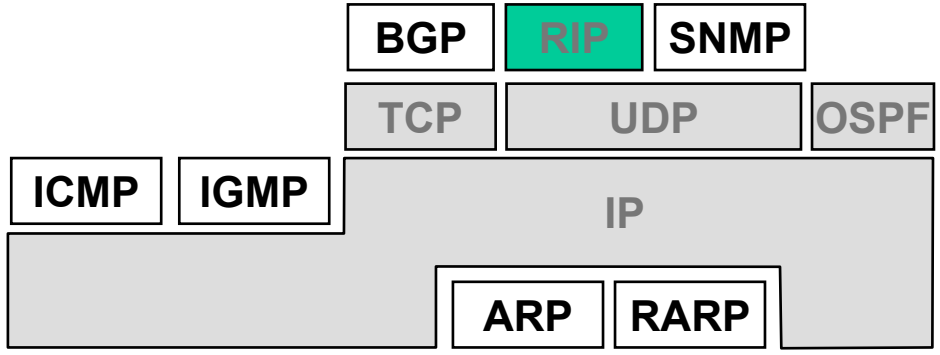
- **BGP (border gateway protocol)**
  (Implementierung eines EGP
  (exterior gateway protocol)
  nach RFC 827)



  - Kommunikation
    zwischen Routern im Verbund komplexer Netze, sog. autonomer Systeme (AS; selbständige Routing Domänen)
  - Externes Routingprotokoll (ERP)
  - Erkennt einen Nachbar-Gateway
    und dessen Aktivierung; es kann Nachbar-Gateways testen, ob sie antworten, und periodisch »Routing Update Messages« zwischen Nachbar-Gateways austauschen
  - RFC 904, 1771 – 1774, 1863, 1930, 2283

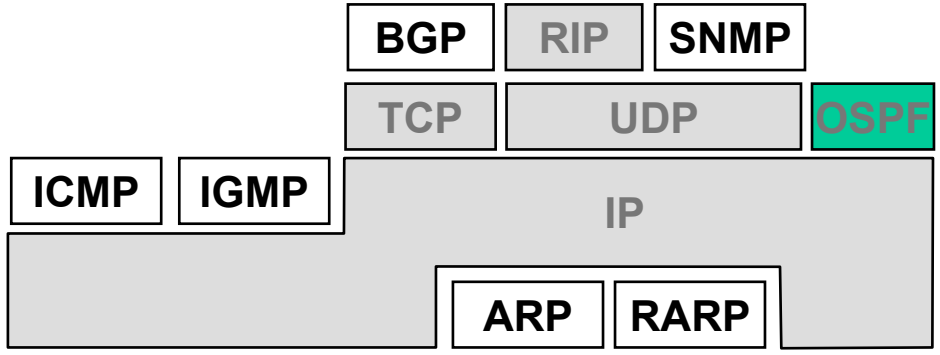
3.8.4 Protokolle in einem IP-Router (Fortsetzung)

- **RIP (routing information protocol)**
  - Meist verwendetes IGP (Interior Gateway Protocol)



  - Alle Router verteilen in Intervallen ihre eigenen Routing-Tabellen per Broadcast an Nachbarn
  - Routing-Tabelle wird auf Basis der gewonnen Informationen in jedem Router neu berechnet
  - Maximale Routenlänge für Berechnung: 14 Hops
  - RIPv2, baut auf Distance-Vector-Algorithmus auf und benutzt wie RIPv1 UDP für den Transport der Routing-Tabellen
  - RIPv1 im RFC 1058 beschrieben,
    RIPv2 in den RFCs 1387 bis 1389,
    extended Version in RFCs 1721 bis 1724

3.8.4 Protokolle in einem IP-Router (Fortsetzung)



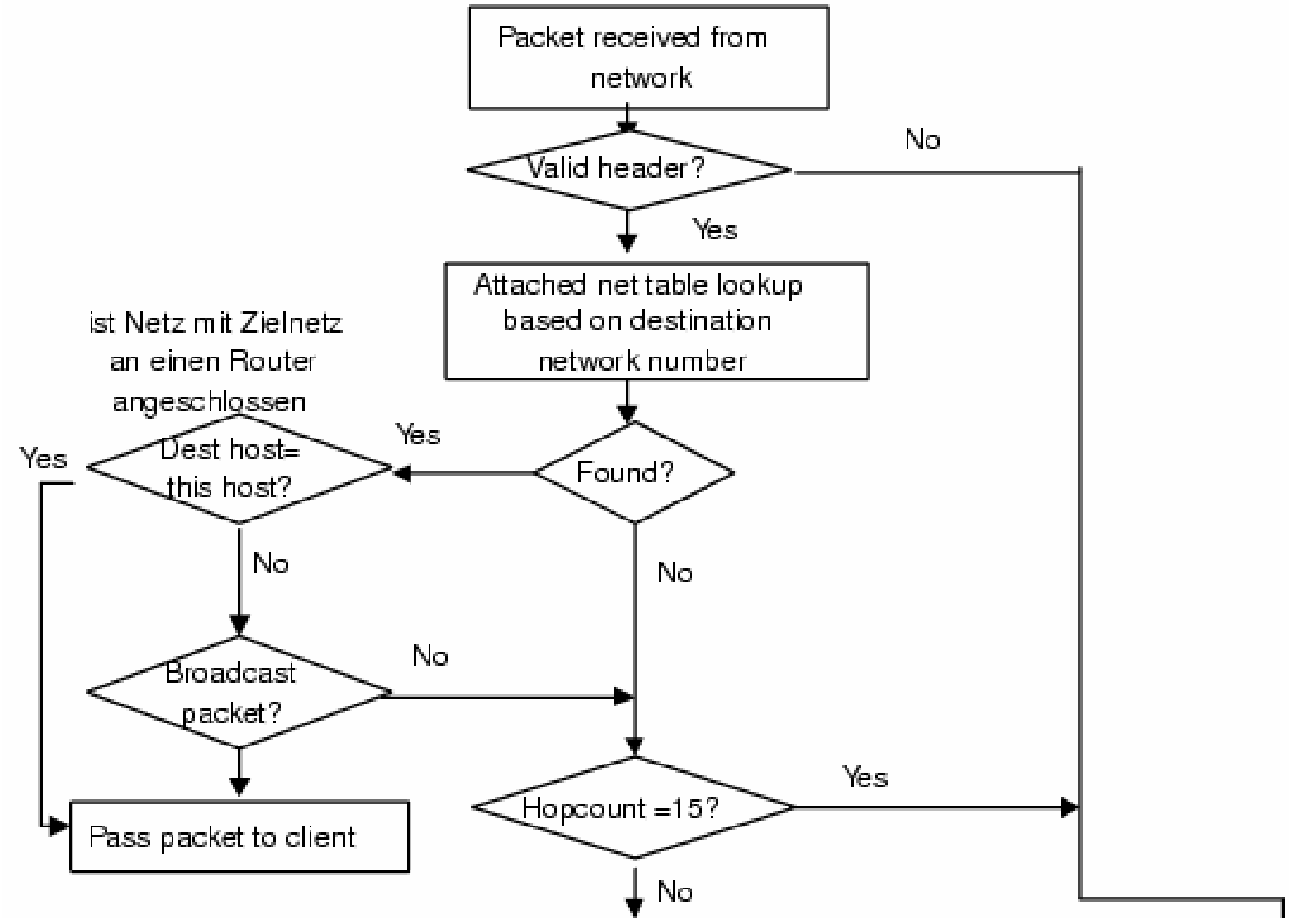
- **OSPF (open shortest path first)**
  - IGP (Interior Gateway Protocol)
  - Propagierung der Verfügbarkeit von Verbindungswegen zwischen Routern
  - Unterstützt hierarchische Netzstrukturen
  - Schnelles, dynamisches Verhalten in Bezug auf die Änderungen in der Netztopologie
  - Dynamische Lastverteilung
  - Geringer Overhead
  - Berücksichtigung der Dienstleistungsmerkmale (TOS) im Routing
  - Arbeitet nach Link-State-Algorithmus (LSA)
    - Lange Routen mit (max. 65.000) Zwischensystemen möglich
    - Subnetze lassen sich in Gruppen zusammenfassen
  - RFC 2178

3.8.4 Protokolle in einem IP-Router (Fortsetzung)

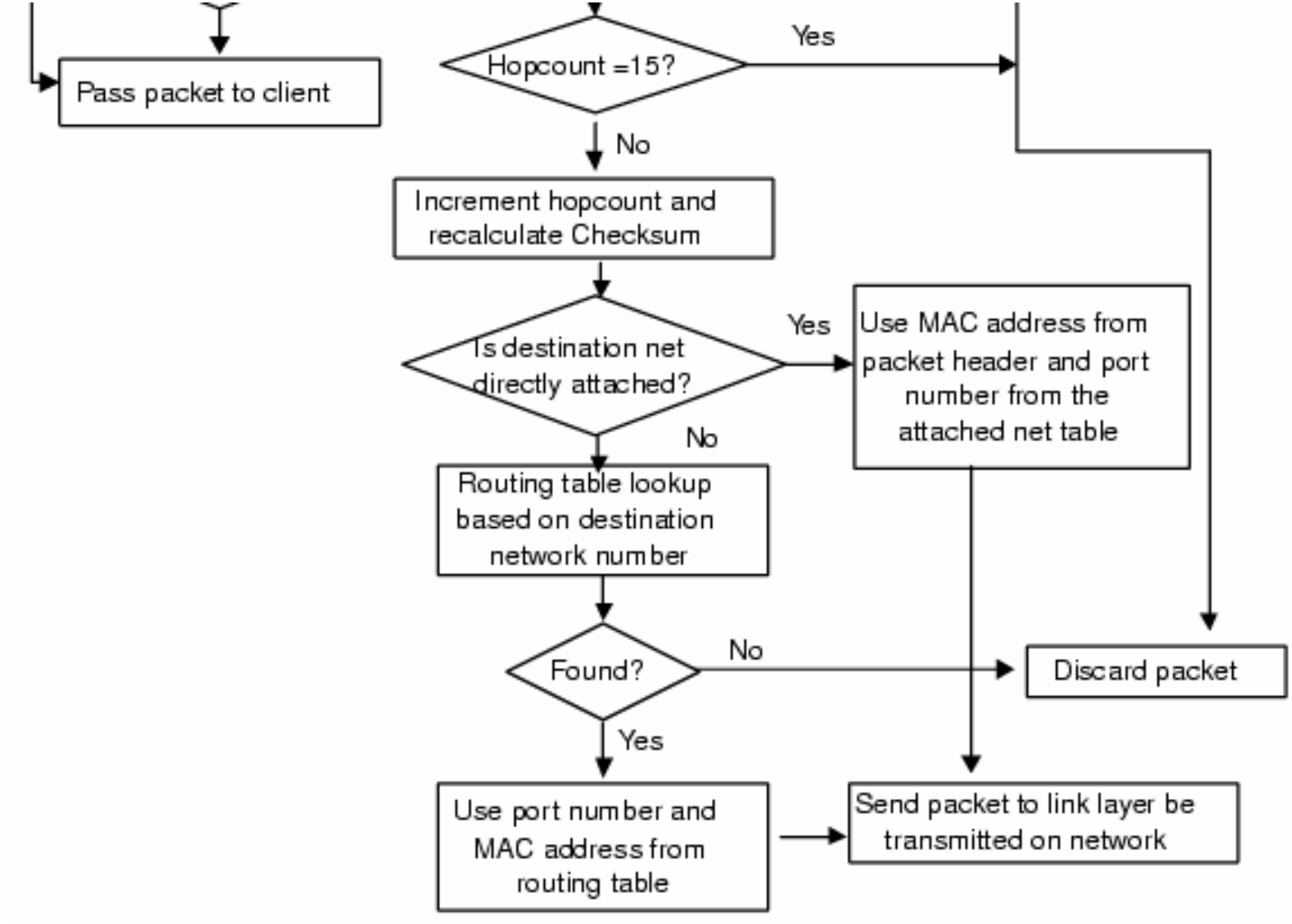
- **OSPF (open shortest path first)**
  - Unterscheidet vier Router-Klassen
    - Interne Router, die sich vollständig in einem Bereich befinden
    - Grenz-Router, die zwei oder mehrere Bereiche verbinden
    - Backbone-Router, die sich im Backbone befinden
    - AS-Grenz-Router, die zwischen mehreren AS vermitteln
  - Nachrichtentypen

Hello	Dient zur Feststellung, wer die Nachbarn sind
Link State Update	Gibt die Kosten des Senders an seine Nachbarn aus
Link State Ack	Bestätigt eine Link-State-Aktualisierung
Database Description	Gibt die neuesten Daten des Senders bekannt
Link State Request	Fordert Informationen vom Partner an

3.8.5 Funktionsweise eines Routers (oberer Teil)

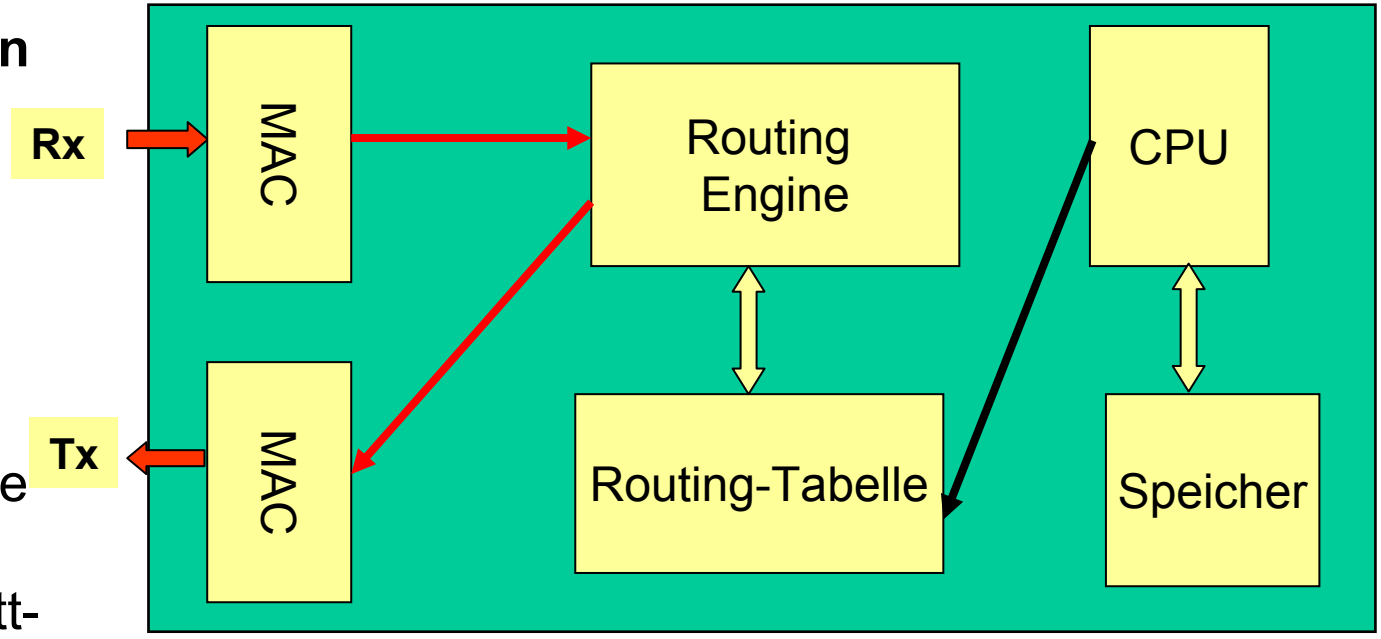


3.8.5 Funktionsweise eines Routers (unterer Teil)



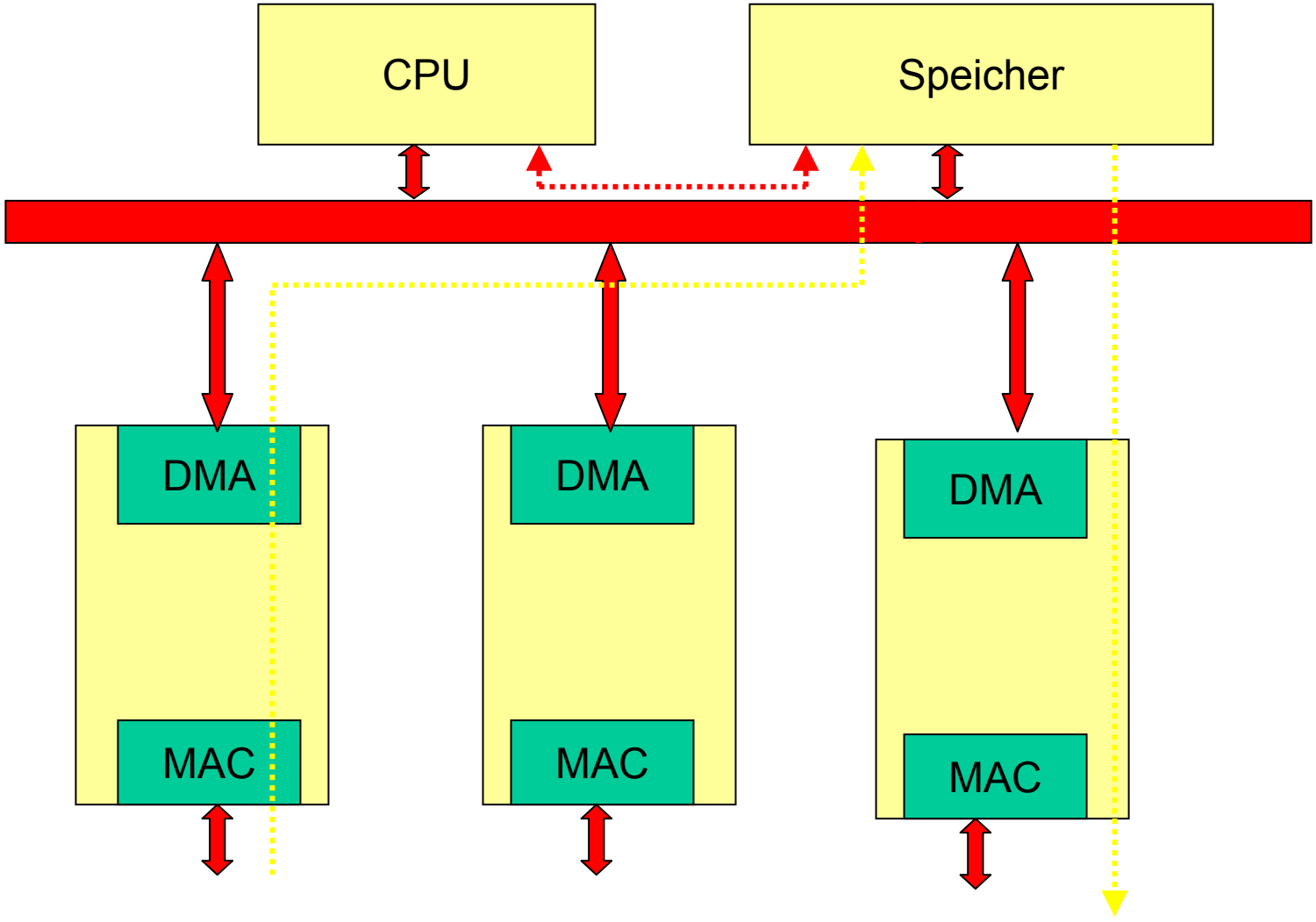
3.8.5 Funktionsweise eines Routers: Aufbau

- **Netzschnittstellen**
- **Routing Engine**
  - Führt das Routing aus
- **Routing-Tabelle**
  - Enthält Regeln welche Pakete über welche Schnitt-stellen weitergeleitet werden müssen

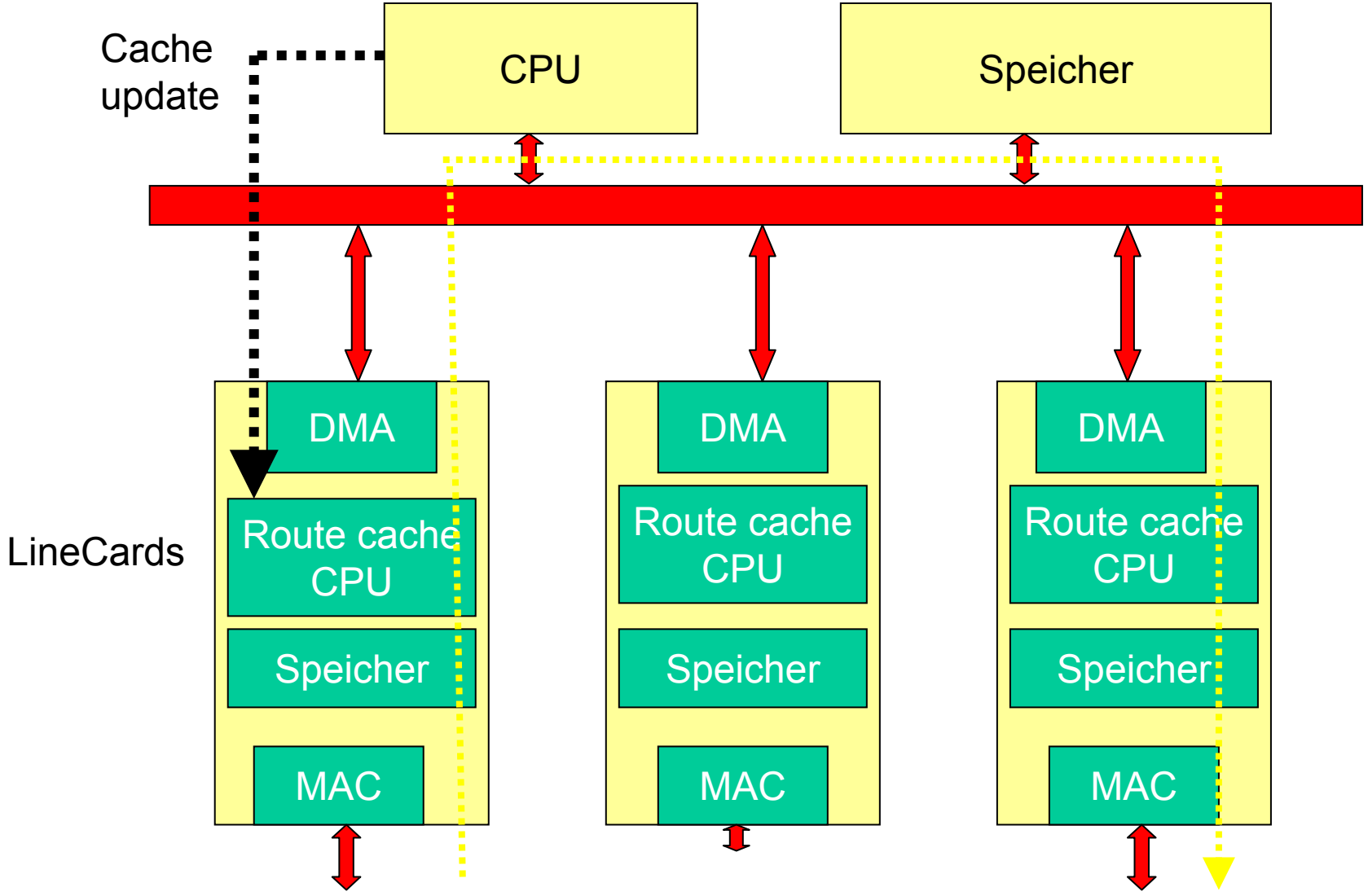


- **I.d.R. wird die Funktionalität der Sicherungsschicht in Hardware (Interface Karten) ausgeführt**
- **Realisierung der Vermittlungsschicht oft (aber nicht notwendigerweise) in Software**

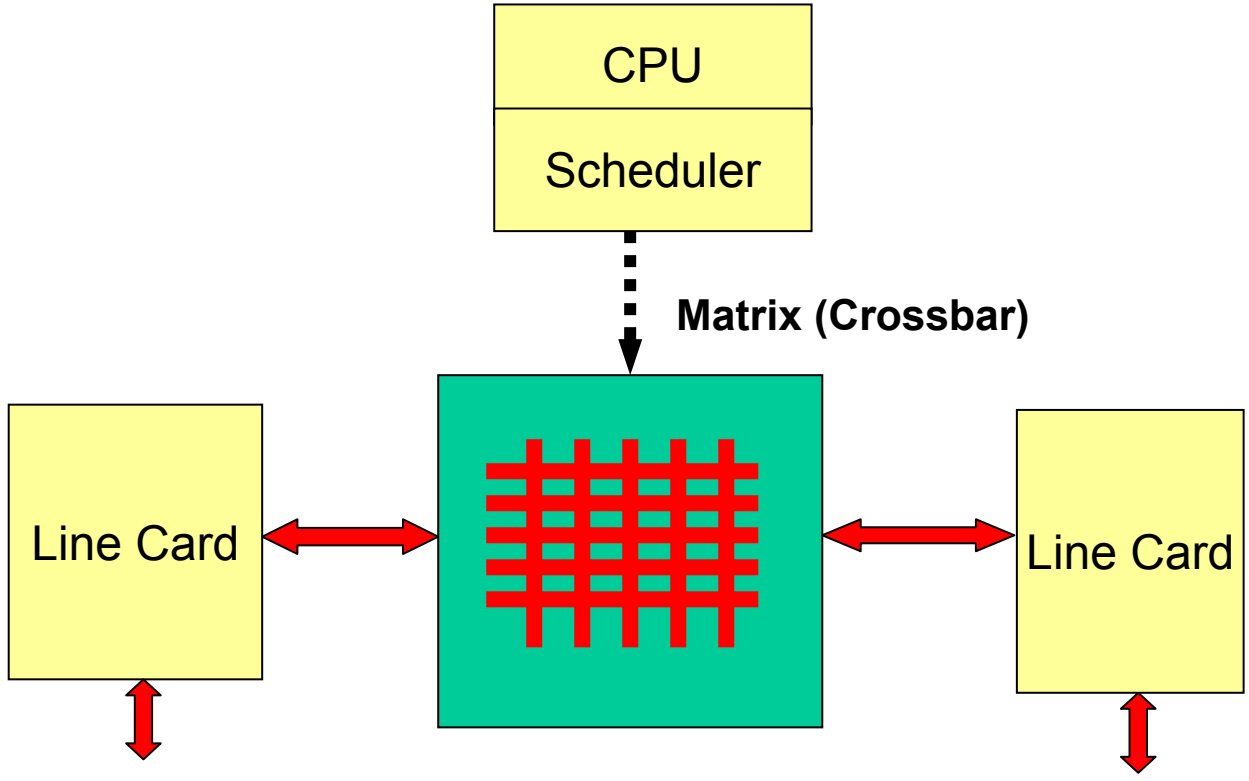
3.8.5 Funktionsweise eines Routers: Erste Generation



3.8.5 Funktionsweise eines Routers: Zweite Generation

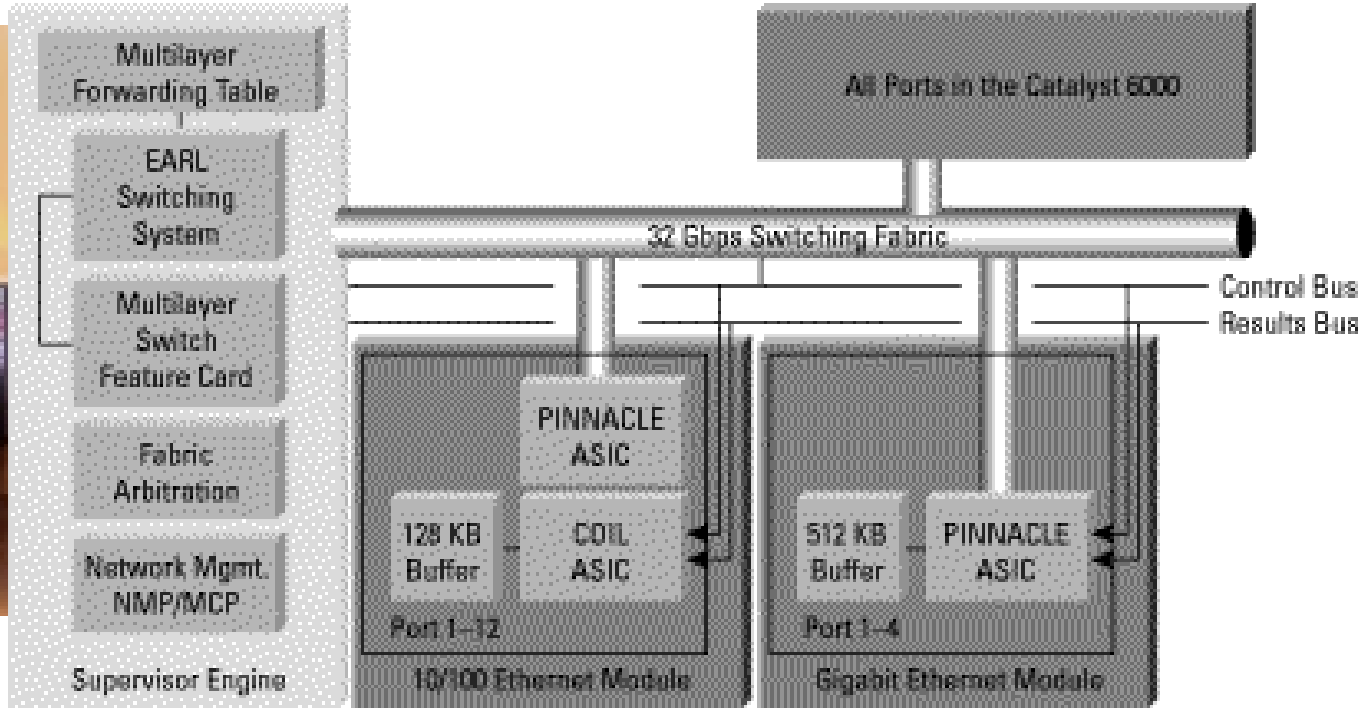


3.8.5 Funktionsweise eines Routers: Dritte Generation



3.8.5 Funktionsweise eines Routers: Beispiel Cisco Catalyst 6500

Architektur



- Supervisor Engines
- Switch fabric modules
- Fast Ethernet modules
- Gigabit Ethernet modules
- 10 Gigabit Ethernet modules
- Voice Modules
- WAN Modules
- ATM Modules
- Multi Gigabit systems (content services, firewall, intrusion detection, IPSec/VPN, network analysis)
- Betriebssystem IOS (propriäter, aktuelle Version 12.3)

3.8.6 Brouter

- **„Routing Bridge“ oder „Bridging Router“ (nicht klar definiert):**
  - Kombination aus Router und Bridge
  - Bridge, angereichert um Routing-Funktionen wie Routing und Flussregelung
  - Transparent für höhere Protokolle
  - Verletzen reine OSI Architektur Philosophie
  - Beispiel
    - Pakete, die nicht geroutet werden können (z.B. Interpretation der Protokollfamilie nicht möglich), werden nach Bridge-Methode propagiert
    - Andere Möglichkeit: Alle Datenpakete werden nach Bridge-Methode propagiert; Brouter kommunizieren untereinander über ein Routingprotokoll zur besseren dynamischen Lastverteilung

3.8.7 Router-Management

- **Managementrelevante Informationen sind**
  - Grundkonfiguration der Komponente (Gerätebestückung, Karten, Portcharakteristik, etc.)
  - Adresstabellen (Netzadressen, MAC-Adresse)
  - Mapping-Adressen (Netzadresse <-> MAC-Adresse)
  - Routing Tabellen
  - Filtereinträge (z.B. für Firewall-Filter)
  - Protokoll-Tabellen (welche werden unterstützt, welche sind aktiv)
  - Subnetzmasken
  - Protokollparameter (z.B. Hallo-Timer, Dead-Timer, Metriken für Routing-Protokolle, Packet-Discard Policy, Retransmission Policy)
  - Statistiken (z.B. IP Broadcasts, ICMP (Redirects, Unreachable Meldungen), IP-Fragmente, IP-Lastanteil, fehlerhafte Pakete, Filterverletzungen, Router-Auslastung)

3.9 Aufbau von Netzkomponenten

- 3.9.1 Hubs
- 3.9.2 Smart Hubs
- 3.9.3 Kategorien von Hubs
- 3.9.4 Hubsystemaufbau
- 3.9.5 Grundaufbau einer Netzkomponente

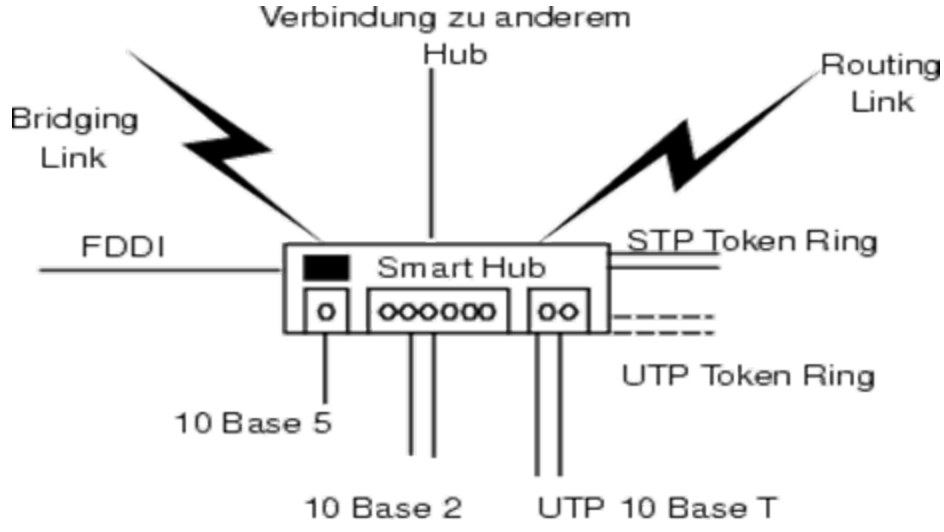
3.9.1 Hubs

Hubs

- Hubs (der Ebene 1) sind Multiport-Repeater
- Signalverstärkerfunktion und Frame-Propagation
- Signalumsetzung und Medienanpassung
- Natürlicher Zusammenhang mit strukturierter Verkabelung
- Bilden Aufpunkt für sternförmige bzw. baumartige Topologien (Wiring Concentrator, Cable Concentrator)
- Begriff ist nicht scharf definiert
  - Reicht von ursprünglich rein homogenen Sternkopplern („Wiring Junction“)
  - Über allgemeine Level-1-Hubs mit unterschiedlichen Medien (Multimedia Access Centers, „Dump Hubs“)
  - Bis zu „Intelligent Hubs“ und „Smart Hubs“ als Knotenpunkt verschiedenster LAN-Technologien (ein solcher Hub ist funktionell auch höheren Ebenen zuzuordnen)

3.9.2 Smart Hubs

- **Knotenpunkt verschiedenster LAN-Technologien mit Repeater-, Bridge-, und/oder Router-Funktion**
- **Smart Hubs sind Kombi-Geräte**
- **Vorteile:**
  - Gemeinsames Gehäuse, Stromzuführung
  - Vereinfachte Verkabelung
  - ein Hersteller für mehrere Funktionen
  - Konsistente Schnittstelle zum Funktionsaufruf
  - Integriertes Netzmanagement
- **Nachteile:**
  - Singuläre Fehlerquelle
  - Herstellerabhängigkeit (keine generelle Interoperabilität von Hubs)



Firewire IEEE-1394 DV 6-Port Switchable Router/ Distributor Hub

3.9.3 Kategorien von Hubs (1)

- **Hubs sitzen in Schnittpunkten von Verkabelungshierarchien. Drei verschiedene Kategorien:**
  - Stackable Hubs:
    - Einfache Single-LAN-Konzentration, kaskadierte Dump Hubs
    - Üblich: 10-24 Anschlussports und wenige LWL-Ports für Backbone-Anschluss
    - Anschlussports üblicherweise über RJ45 (Twisted Pair Ports), aber auch BNC-Ports für 10Base2 und AUI für 10Base5
    - Produkte unterscheiden sich nach
      - Anzahl der Hubs pro Stackcable
      - Ports
      - Kaskadiertiefe
      - Wirkung als Repeater (pro Hub oder Stack)

3.9.3 Kategorien von Hubs (2)

- Modular Hubs:
  - Smart Hubs, unterstützen mehrere parallele LANs (üblich Ethernet, Token Ring, FDDI)
  - Aufbau der Backplane ermöglicht es, die Einschubmodule an mehrere voneinander unabhängige Bussysteme anzuschließen
  - Smart Hubs haben Bridgefunktionalität
  - Mehrere physikalisch getrennte Netze werden über eine Backplane verbunden
  - Enterprise Hubs sind verfügbar für
    - Ethernet [AUI (10Base5), BNC (10Base2), RJ45 (10BaseT), ST (10BaseF) – verschiedenste Fasern, Brücken- und Routermodule (local, remote), Terminal-Server-Module]
    - Token-Ring [UTP, STP, Glasfaser 802.5 J, 53 Ohm-Koaxial, Lobe Ports (RI,R0), Brücken- und Routermodule, SDLC/LLC Konvertierer]
    - FDDI
    - Sie unterstützen SNMP-Management

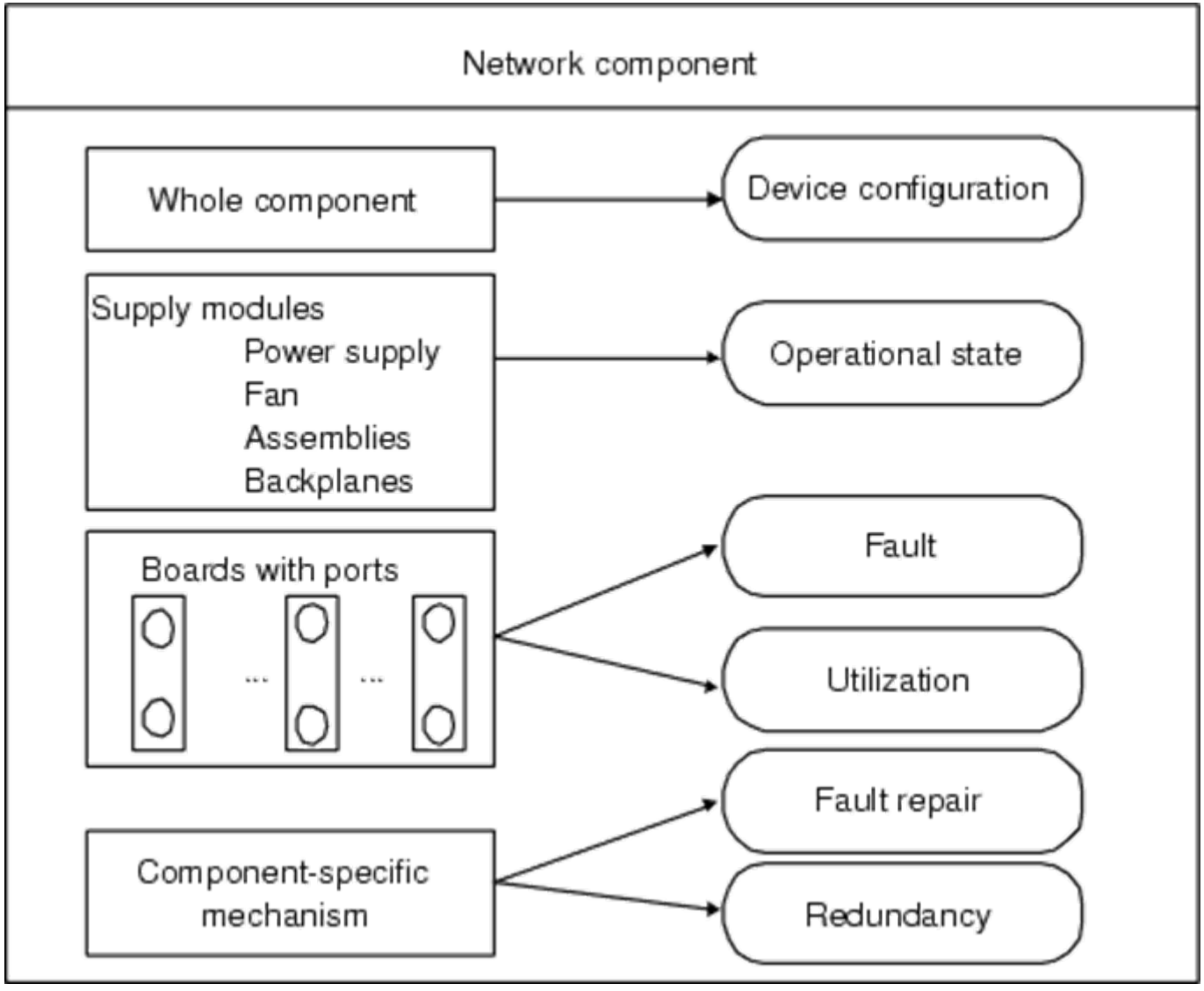
3.9.3 Kategorien von Hubs (3)

- Highend Hubs:
  - 100 Mbps Ethernet, ATM
  - „Collapsed Backbone Hubs“ – nicht für den Anschluss von Endgeräten konzipiert

3.9.4 Hubsystemaufbau

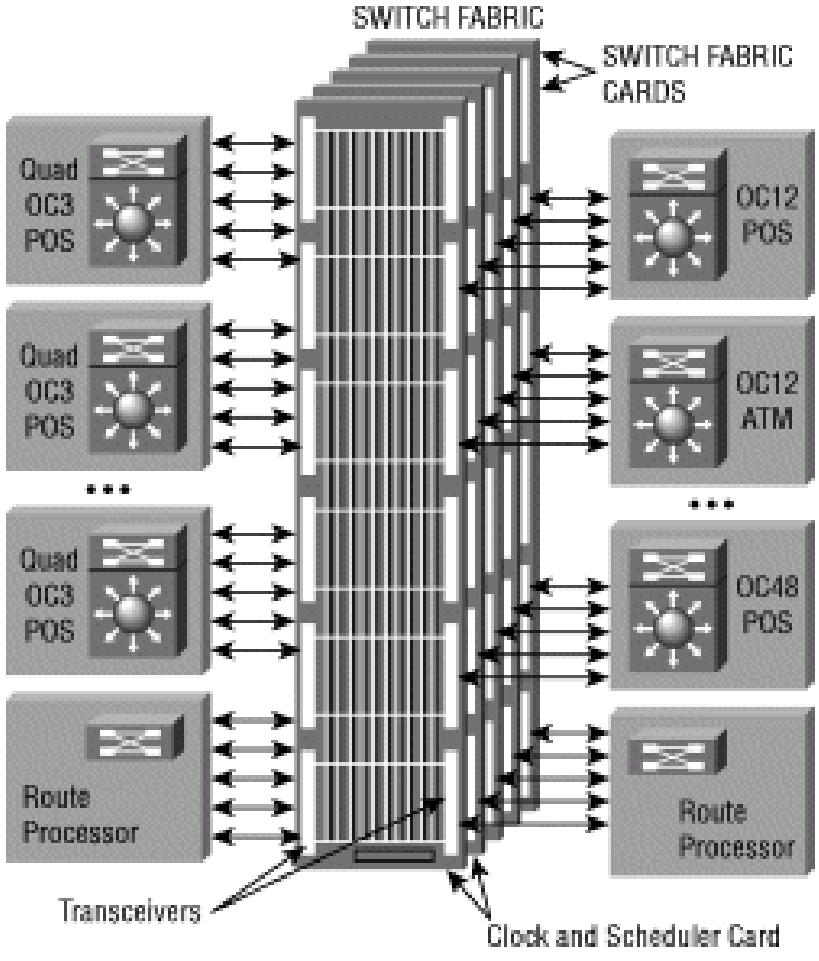
- **Einschubkarten („Link Modules“)**
- **Bus/Backplane („Processor Interconnect“)**
  - Mehrere unterschiedliche Datenbusse für verschiedene Netztypen (Ethernet, FDDI, Token Ring, ATM)
  - Management-Busse. Automatisches Erkennen aller Einschubmodule; Überwachung Verkehr und Modulstatus; Konfigurierung und Überprüfung Modulparameter.
  - Passive Backplane (keine aktiven Komponenten)
  - Aktive Backplane. Backplane hat Controllerfunktionen wie Taktgebung, Buszugriffssteuerung
- **Systemcontroller (Takt, Redundanz, Busmaster, Steuerung der Backplane, zentrale Verwaltung). Oft existiert Multiprozessorarchitektur; Fast Routing Engine**
- **Netzteil**
- **Lüfter. Redundanz kann sich beziehen auf Controller-Modul, Bus, Karten, Ports, Netzteil**

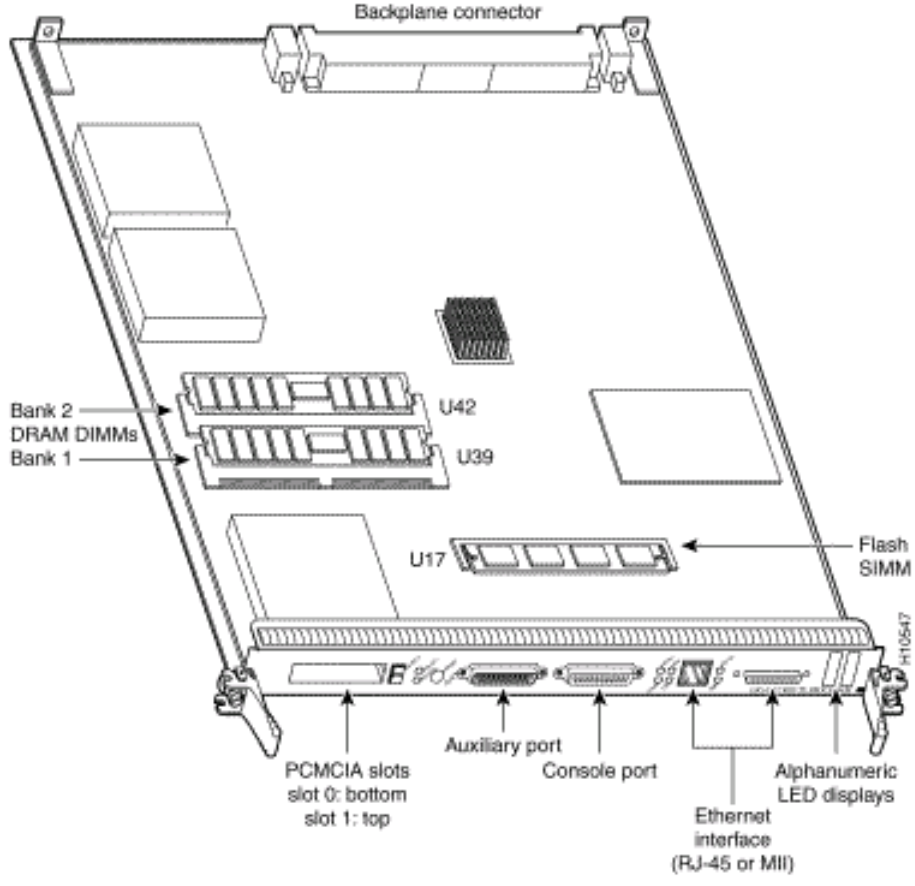
3.9.5 Grundaufbau einer Netzkomponente



3.9.5 Grundaufbau einer Netzkomponente

Beispiel Cisco 12000 Series





3.10 Management von LAN-Komponenten

- 3.10.1 Management Architektur
- 3.10.2 Beispiel einer Architektur: Internet Management
- 3.10.3 Implementierungen in LAN-Komponenten
- 3.10.4 Anforderungen an Komponentenmanagement
- 3.10.5 Gesamtkonfiguration
- 3.10.6 Managementaspekte einer Bridge
- 3.10.7 Managementaspekte eines Routers
- 3.10.8 Protokolle zur automatisierten Konfiguration

3.10 Management von LAN-Komponenten

Zielsetzung: Integriertes Management

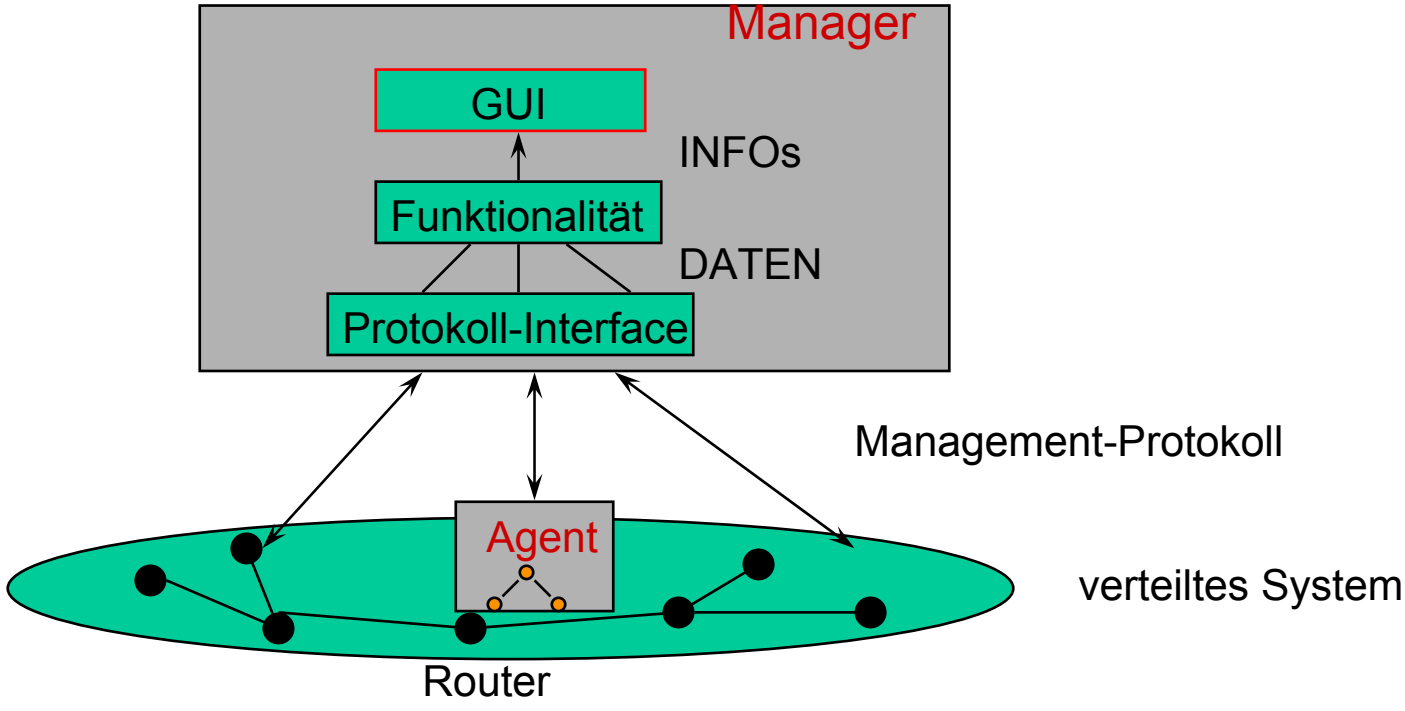
- **Heterogenität und Anzahl der Netze, der Endsysteme (PCs. Workstations, Hosts)**
- **Heterogenität von System-Hardware und -Software (Firewalls, WWW-Server, Mail-Server, aFTP-Server, Web-Browser, etc.)**
- **Verteilung von Informationen und Funktionalität auf verschiedene Komponenten**

→ Management einer verteilten, heterogenen, komplexen Umgebung

- **Integriertes Management**
  - "Das Netz ist der Rechner", d.h. Zusammenwachsen von Netz-, System- und Anwendungsmanagement

3.10 Status-quo: Zentralisiertes Management

- **Überwachung des verteilten Systems zentral vom Manager (Polling, Traps)**



3.10.1 Einführung einer Management-Architektur

- **Komplexität erfordert eine integrierende Struktur für Lösungskonzepte und Implementierungen**

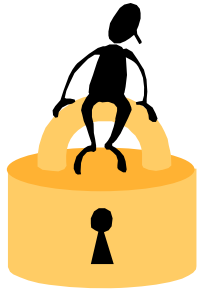
  → *Notwendigkeit einer Architektur für das Management*

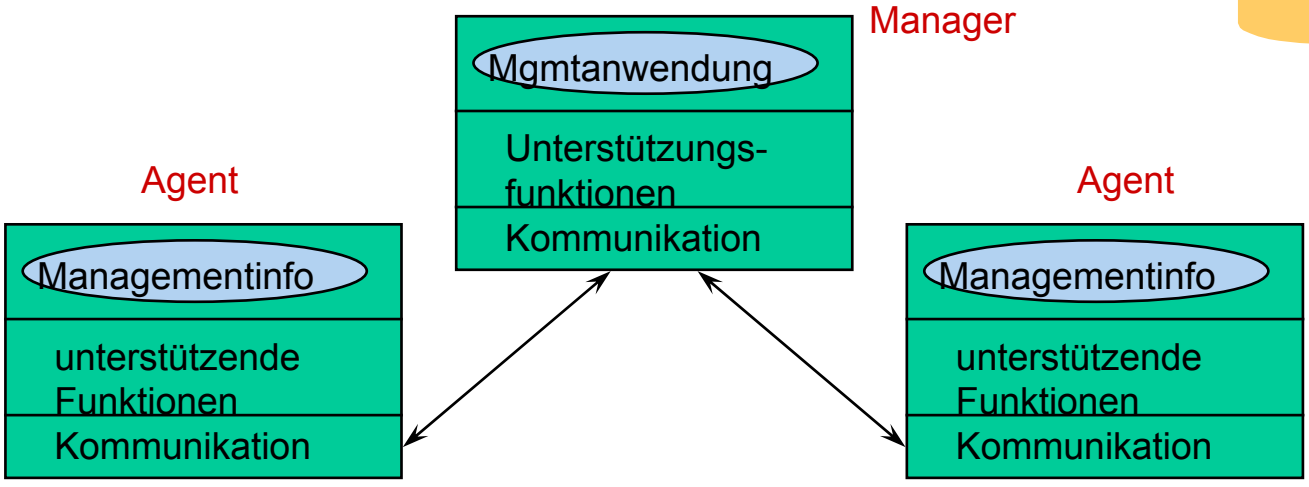
- **Prinzipiell sind zwei Klassen von Architekturen zu unterscheiden:**
  - Herstellerspezifisch
  - Herstellerübergreifend

  → *integrierte, offene Architektur*

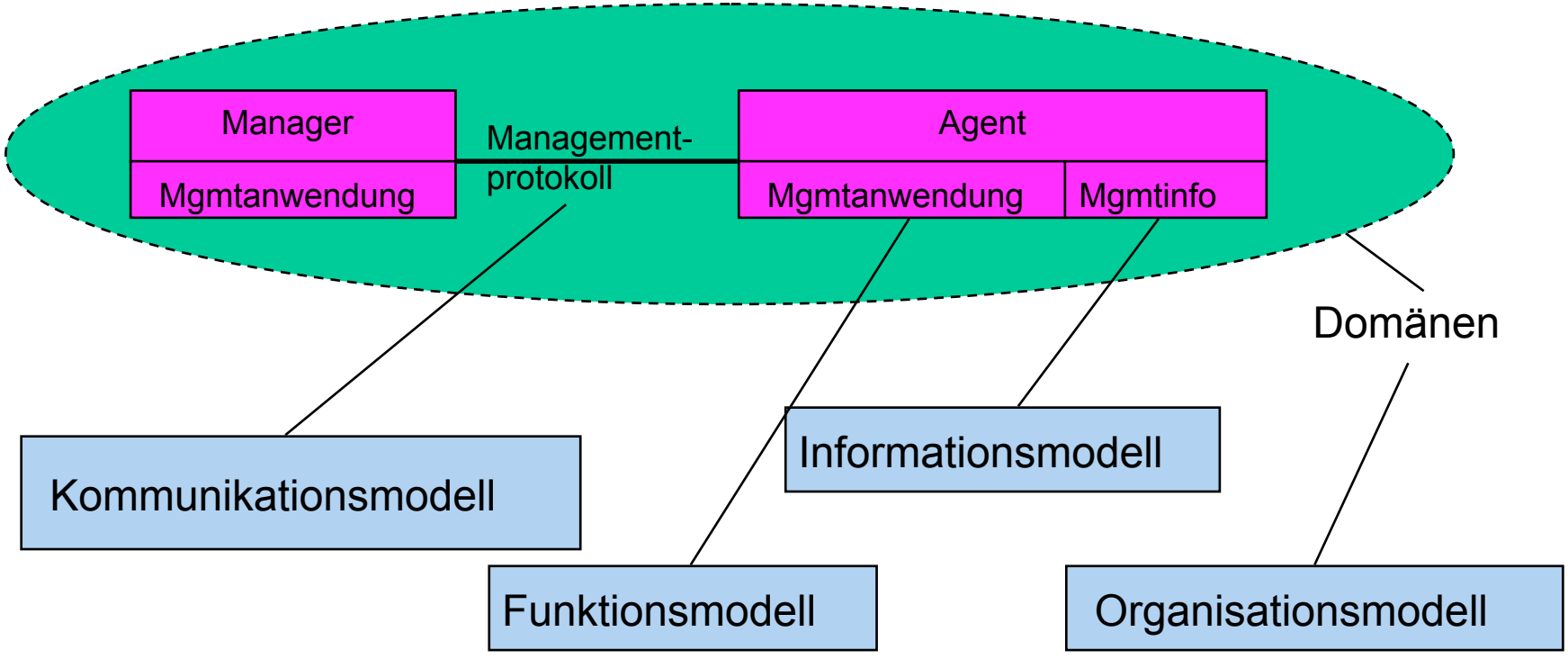
3.10.1 Managementarchitektur

- **Elementare Eigenschaften einer integrierten Managementarchitektur**
  - Standardisierte Managementinformation, Managementprotokollen, Managementfunktionen
  - Häufigstes Organisations-Prinzip:
    Manager-Agent-Model



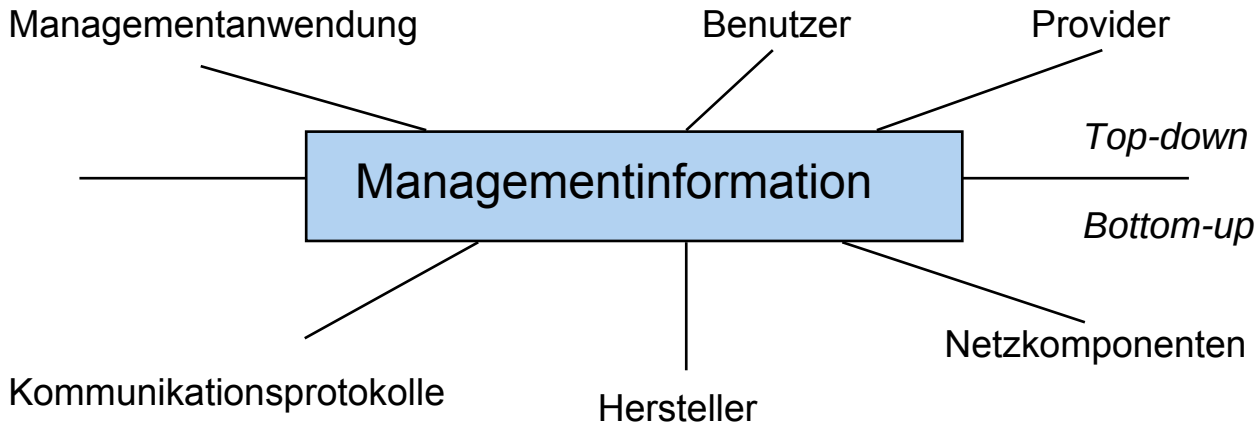


3.10.1 Teilmodelle der Architektur



3.10.1 Informationsmodell: Managementinformation

❑ Definition von konkreter Managementinformation



Managementinformationsbasen (MIBs)
-- konzeptionelles Repository für Managementinformation

3.10.1 Funktionsmodell

- Gliederung des Gesamtkomplexes Management in Funktionsbereiche (z.B. Fehlermanagement, Sicherheitsmgmt)
- Festlegung der Funktionalität der Bereiche
- Dienste zur Erbringung der Funktionalität
- Bereitstellung generischer, gemeinsam benutzbarer Funktionalität für Managementanwendungen

3.10.1 Kommunikationsmodell

- **Management-Kommunikation erfolgt durch**
  - Statusabfragen
  - Austausch von Steuerinformation
  - (asynchrone) Ereignismeldungen
- **Aspekte des Kommunikationsmodells folglich:**
  - Festlegung der kommunizierenden Partner
  - Mechanismen für die genannten Kommunikationszwecke
  - Syntax und Semantik der Austauschformate

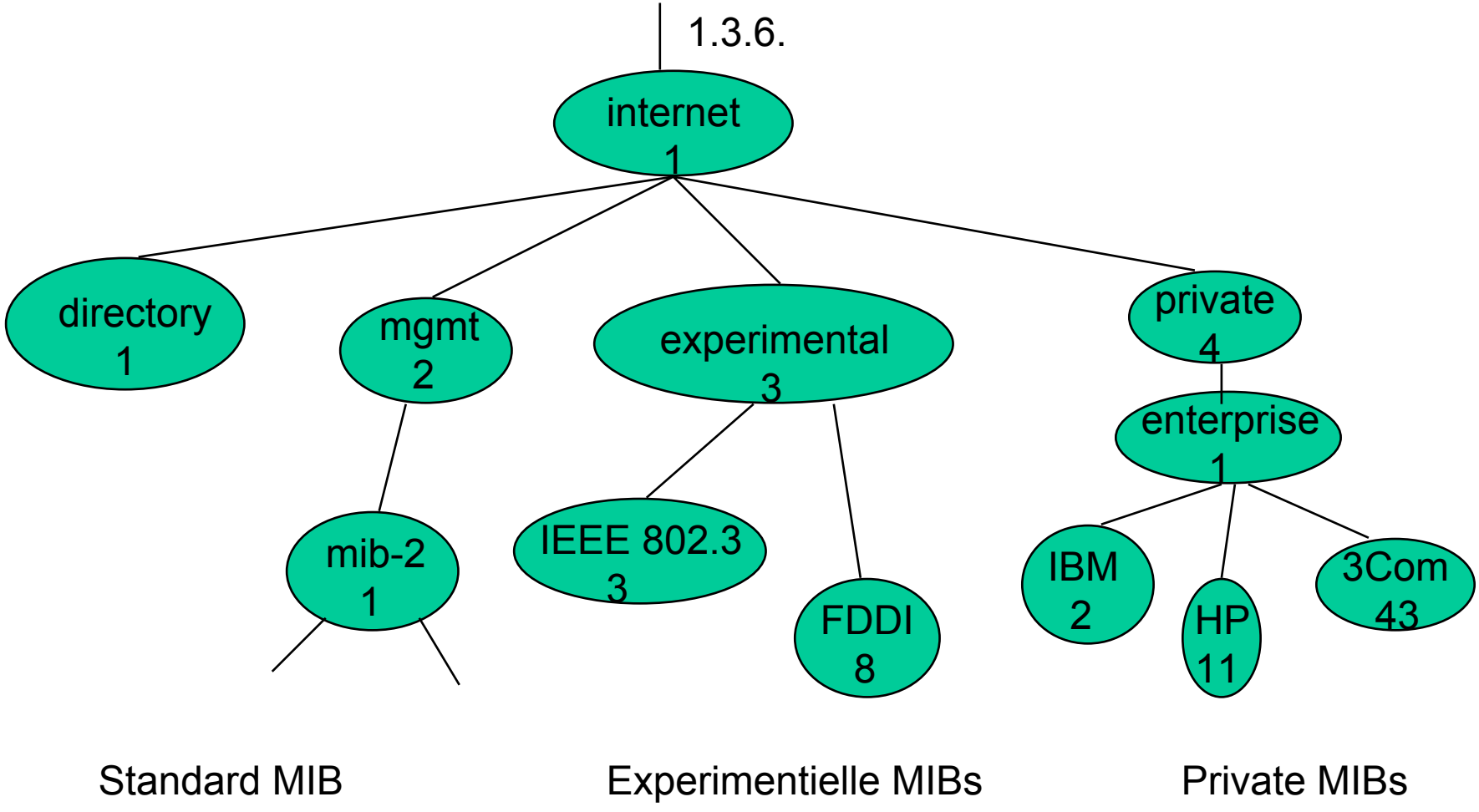
3.10.1 Organisationsmodell

- **Anpassung des Managements an die Aufbau- und Ablauf-Organisation des Betreibers**
- **Domänenbildung:**
  - Gruppenbildung auf Ressourcen aus organ. Gründen
  - Management Policies
- **Festlegung von Rollen und Beziehungen der beteiligten Einheiten (z.B. Manager, Agent)**

3.10.2 Beispiele von Architekturen: Internet-Management

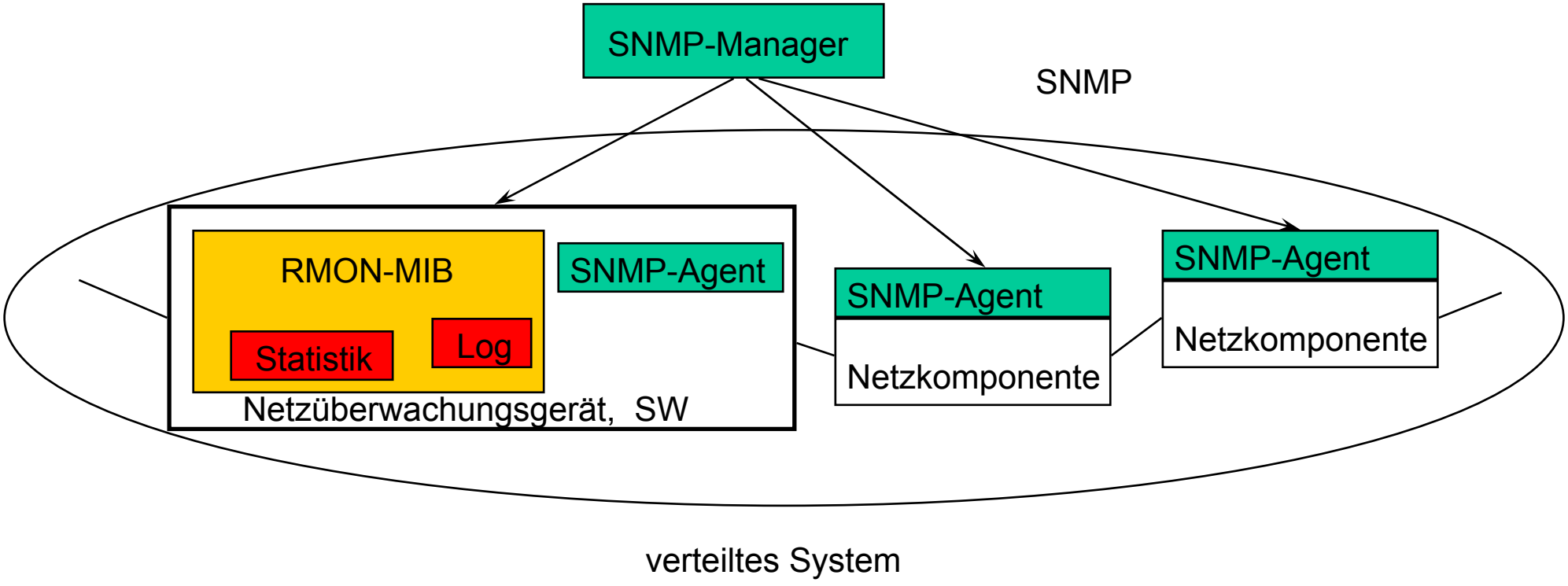
- **Ansatz: pragmatischer, einfacher als der universelle aber komplexe ISO-Ansatz**
- **Informationsmodell**
  - Modellansatz: Datentypansatz, Informationseinheiten: einfache und zusammengesetzte Variablen, RFC 1155 bzw. 1442 “Structure of Management Information”, MIB II (RFC 1213) - Basis Objektkatalog im Internet-Management
- **Funktionsmodell**
  - bisher kaum ausgeprägt, Ausnahme: RMON (Remote MONitoring), größter Teil der Funktionalität im Manager
- **Kommunikationsmodell**
  - Simple Network Management Protocol (SNMP), verbindungslos

3.10.2 Teile des Internet Registrierungsbaum



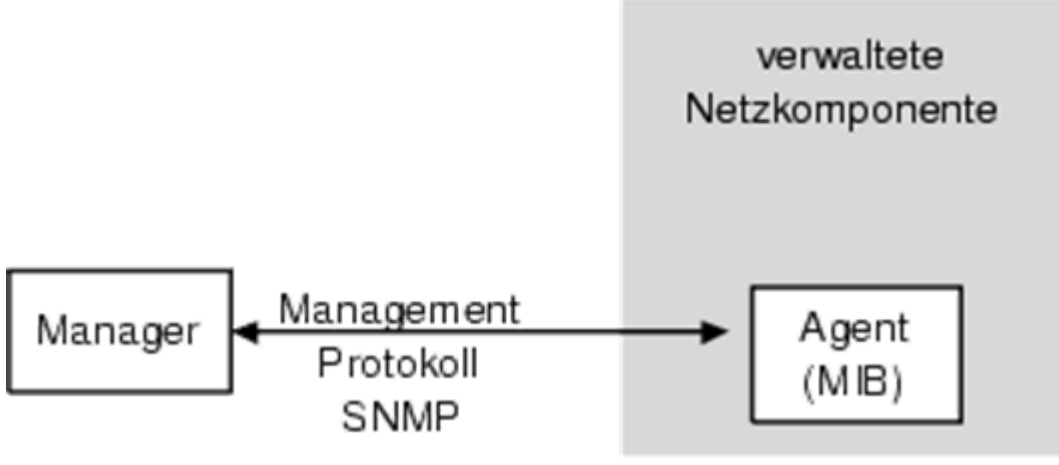
3.10.2 Internet-Management: RMON

- **Remote MONitoring (RMON) - Performance-Informationen**



3.10.3 Implementierungen in LAN-Komponenten (1)

- **Im Umfeld von Netzkomponenten (LAN und Router) meist Internet-Managementarchitektur**
- **Internet-Architekturmodell:**
  - Es existieren Manager, Agenten und zu verwaltende Netzkomponenten („Managed Nodes“)
  - Jeder zu verwaltenden Netzkomponente ist ein Agent zugeordnet, der mit einem oder mehreren Managern kommuniziert.
  - Agent läuft auf der Netzkomponente
  - Manager übernimmt die eigentlichen Managementaufgaben abhängig von den Informationen, die von Agenten über die zu verwaltenden Komponenten bereitgestellt werden



3.10.3 Implementierungen LAN-Komponenten (2)

- In LAN-Umgebung wird häufig das Internet-Management verwendet, d.h. als Agent-Protokoll kommt SNMP zum Einsatz
- Von der Netzkomponente bereitgestellte Managementinformation ist durch die MIB (Management Information Base) gegeben.
- Für Bridges gibt es standardisierte Internet-MIBs, für die meisten Komponenten kommen jedoch herstellerabhängige MIBs zur Anwendung.
- Solche MIBs können sehr umfangreich sein (mehrere hundert Variablen!)
- MIBs sind management-relevante Abstraktionen von realen Ressourcen, z.B. kann ein „Lüfter“ durch ein Boolean („ein“, „aus“) moduliert werden mit Operationen get und set.

3.10.4 Anforderungen an Komponentenmanagement

- **Konfiguration. Darunter ist die Konfiguration der Komponente zu verstehen, so dass sie in den Betrieb des Netzes mitintegriert wird.**
  - Allgemeine Parameter (z.B. IP-Adresse), Leistungsparameter, Sicherheitsparameter, Abrechnungsparameter
- **Überwachung während des Betriebs der Komponente im Netz, Fehlverhalten, Engpässe, Ressourcennutzung, Angriffe**
- **Gerätetypunabhängige Aufgaben**
  - Gesamtkonfiguration
  - Betriebszustandsüberwachung
  - Portüberwachung
- **Gerätetypabhängige Aufgaben**
  - Berücksichtigen die komponentenspezifischen Mechanismen; hier sind auch die FCAPS-Funktionen zu berücksichtigen

3.10.5 Gesamtkonfiguration (1)

- Komponente wird als gesamte Einheit betrachtet
- Zuordnung der IP-Adresse
- Festlegung des Zugriffs auf Bridge-Funktionalität, z.B. Schutz von Administratorfunktionen durch Paßwörter
- Booten von Bridges

3.10.5 Gesamtkonfiguration (2)

- Physische Installation
- Grundkonfiguration (Basisinitialisierung, Boot-Diskette)
- Zuteilung von Namen, Adressen, Domänen
- Konfiguration der gerätespezifischen Funktion
- Konfiguration der Baugruppen
- Konfiguration der Ports. Aktivieren/Deaktivieren von Ports, Setzen von Port-Geschwindigkeiten, Setzen der maximalen Framegröße für Empfang/Senden über Port
- Konfiguration der Sicherheitsparameter
- Setzen von Grundparametern für das Monitoring (Timer, Poll-Router, Traps)
- Darstellung der Konfiguration der Komponente
- Überwachung des Betriebszustandes. Stromversorgung, Temperatur und Durchführung von Selbsttests

3.10.6 Managementaspekte einer Bridge

- **Steuerung des Schleifenunterdrückungsmechanismus**
- **Steuerung des Verkehrsseparierungsmechanismus:**
  - Aktivieren/Deaktivieren und Steuerung des Lernmechanismus
  - Aktivieren/Deaktivieren der gelernten Adresstabelle. Im Zustand inaktiv werden nur manuell eingetragene MAC-Adressen berücksichtigt. Aufbau einer Filtertabelle zum Ausfiltern von Frames entsprechend ihrer Adressen; Festlegung des Zeitintervalls, wie lange MAC-Adressen in Adresstabelle bleiben, ohne gesendet zu haben
  - Aktivieren Spanning Tree-Verfahren (übliches Verfahren zur Schleifenunterdrückung)
  - Spezifikation von Bridge-Prioritäten zur Festlegung der Root-Bridge (Bridge in zentraler Lage im Netz hat höchste Priorität); Festlegung der Wegekosten
- **Lastüberwachung: CPU- und Pufferauslastung; verarbeitete Frames (Standard-, Multicast-, Broadcast-Frames)**
- **Fehlerüberwachung: Kollisionszähler; Auswertung von Fehlern, die durch Empfangen/Senden von MAC-Frames entstanden sind**

3.10.7 Managementaspekte eines Routers

- **Hier treten wie beim Bridge-Management die Aspekte Gesamtkonfiguration, Überwachung des Betriebszustands, Kommunikationsfehler-Analyse und Auslastungs-Ermittlung**
  - Konfiguration der verschiedenen Tabellen (Adresstabelle, Mapping-Tabelle, Routing-Tabelle). Router muss seinen angeschlossenen DTEs bekannt gemacht werden -> Eintragung der Netzadresse bei DTEs. Eintrag der Adressen der angeschlossenen DTEs in Routingtabelle
  - Routingverfahren: Festlegung der Parameter zur Durchführung des Wegewahlverfahrens (statisch oder dynamisch), z.B. Metriken bei Entscheidungsfindung (Hop-Anzahl, Leitungskapazität, Fehlerrate)
  - Protokollverarbeitung der Ebene 3
  - Eventuell Abbildung Ebene 3a auf 3c
  - Firewall-Management
  - Statistiken. Statistiken über Fehler bei der Verarbeitung von Paketen eines Protokolltyps; Einstellen von Zugangsfiltern für den weiteren Transport von Paketen

3.10.8 Protokolle zur automatisierten Konfiguration (1)

❑ BOOTP (bootstrap protocol)

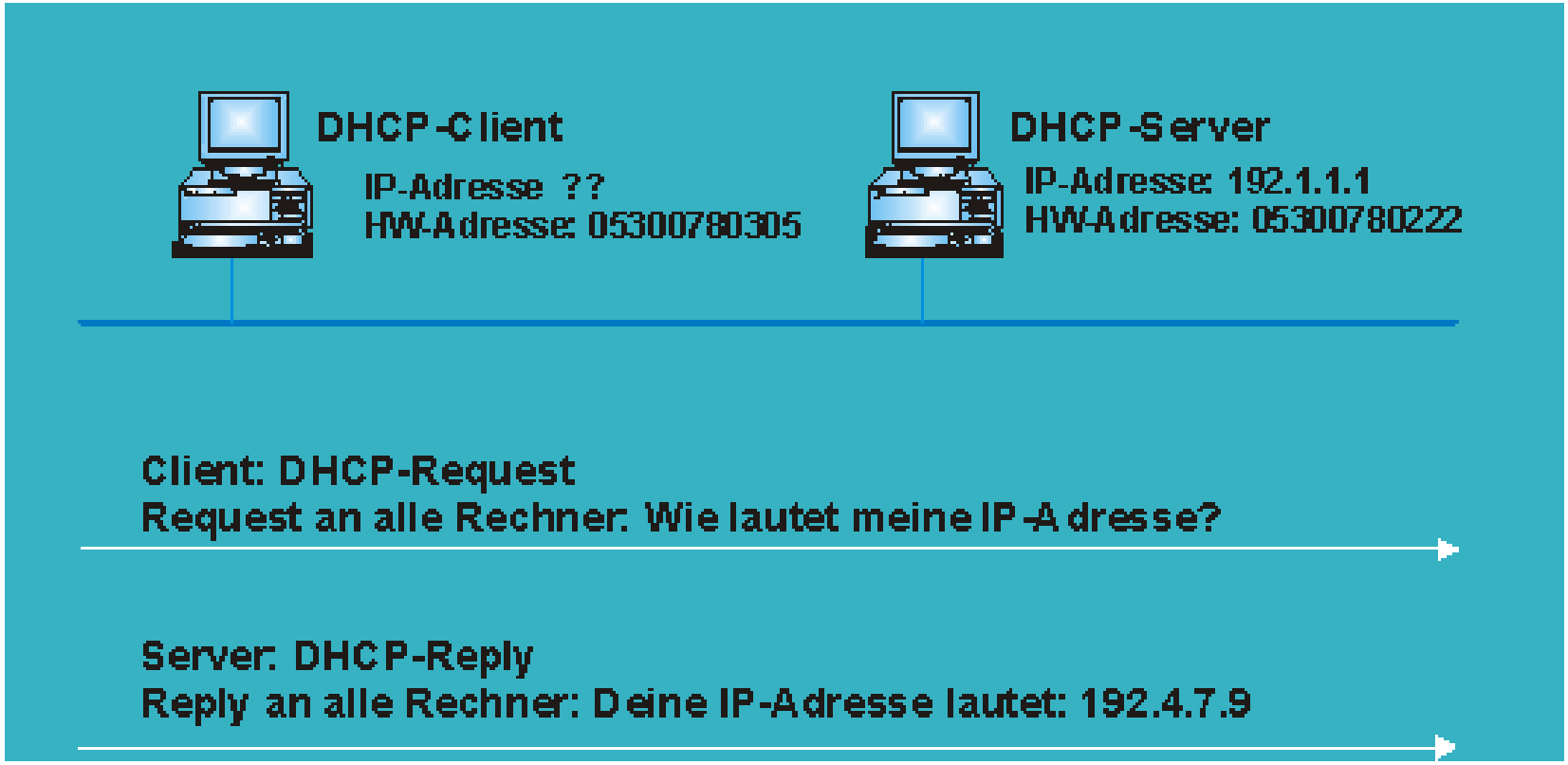
- Das Bootstrap-Protokoll ist ein Client-Server-Protokoll, das der Vergabe von IP-Adressen dient
- Es kann überall dort eingesetzt werden, wo die Adressvergabe über das Netz erfolgen muss
- Beim BootP-Protokoll benutzen BootP-Client und -Server das UDP-Protokoll zur Kommunikation
- Dabei geht es im Wesentlichen um den Austausch eines Datenpaketes, in dem der BootP-Server dem Client wesentliche Informationen übermittelt
- Funktionsablauf

3.10.8 Protokolle zur automatisierten Konfiguration (2)

- **DHCP (dynamic host configuration protocol)**
  - Das DHCP-Protokoll ist ein Client-Server-Protokoll, das den Aufwand für die Vergabe von IP-Adressen und sonstigen Parametern reduziert
  - Mittels DHCP kann ein Netz-Administrator alle TCP/IP-Konfigurations-Parameter zentral verwalten und warten
  - Das DHCP-Protokoll dient der dynamischen und automatischen Endgeräte-Konfiguration z.B. der Vergabe von IP-Adressen unter IPv4 und IPv6
  - Die entsprechenden IP-Adressen werden von den angeschlossenen DHCP-Clients beim DHCP-Server angefordert
  - Die Adressen werden einem Adresspool entnommen, der in einem DHCP-Server residiert
  - Die Zuweisung der IP-Adresse kann automatisch, dynamisch oder manuell erfolgen

3.10.8 Protokolle zur automatisierten Konfiguration (3)

- **DHCP (dynamic host configuration protocol)**
  - Funktionsablauf



3.10.8 Protokolle zur automatisierten Konfiguration (4)

- Einordnung ins OSI-Modell