
Rechnernetze und Telekommunikation

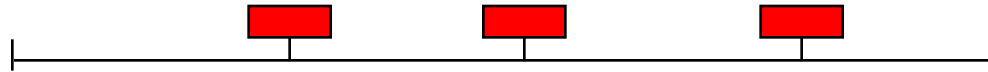
LAN/Ethernet

Übersicht

- ◆ LAN-Topologien
- ◆ LAN-Medien
- ◆ IEEE 802.3 Ethernet
 - Protokoll
 - Adressen
- ◆ ARP
- ◆ LAN-Struktur
- ◆ Switching
- ◆ VLANs
- ◆ LAN-Geräte

Topologien (1)

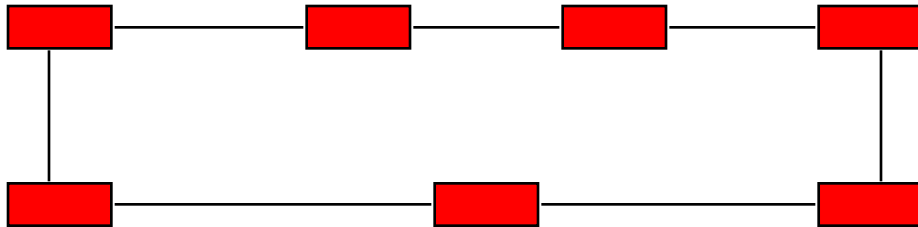
♦ Bus



- + einfach
- + 'wenig' Kabel
- speziell (nur für 10M-Ether)
- aufwendige Fehlersuche
- für große Entfernungen?

Topologien (2)

◆ Ring

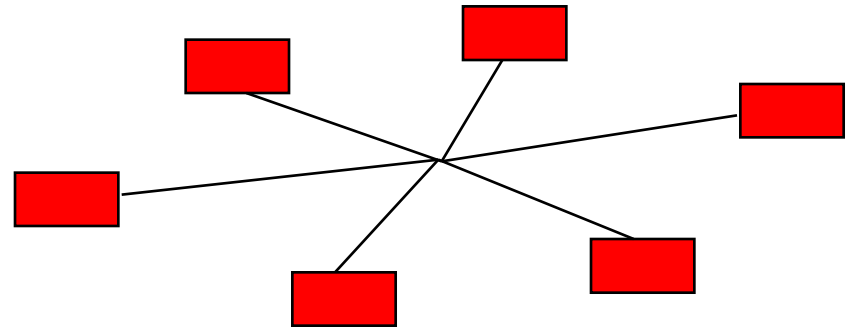


- + einfach
- + implizite Redundanz
- lange Kabelwege
(länger als Bus)
- Signal läuft durch alle Komponenten

Topologien (3)

◆ Stern

- + Standard
- + flexibel
- + gutes 'soft fail'
- + gute Datensicherheit
- + gute Problemeingrenzung
- aufwendig
- ‚viel‘ Kabel im Zentrum



Medien (1)

◆ Kupferkabel

- Twisted Pair („TP“)
 - Shielded (STP)
 - Unshielded (UTP)
- Selten heute Koaxialkabel

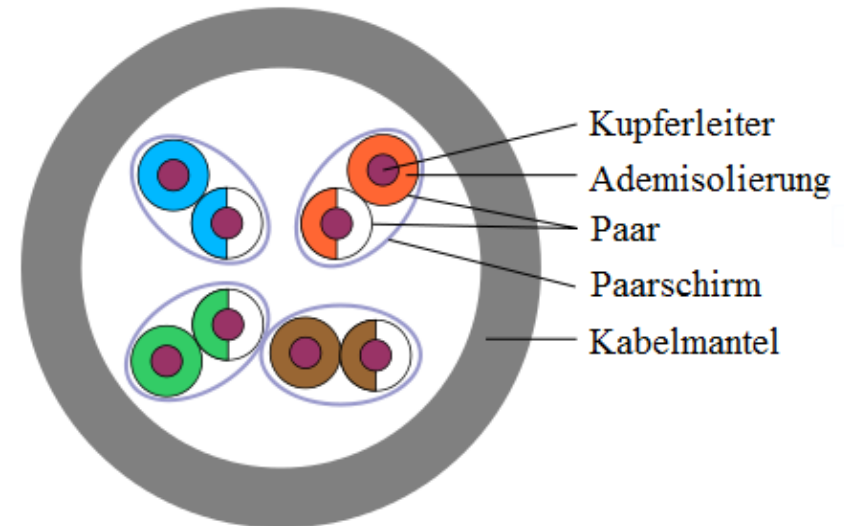
◆ I.d.R heute CAT5

- Spezifiziert bis 100 Mhz
- Verwendung
 - Telefon
 - Fast Ethernet/ GigabitEthernet („CAT5e“)

◆ CAT-6A/CAT-7

- Spezifiziert 600-1000 MHz
- Verwendung
 - 10 GBEthernet

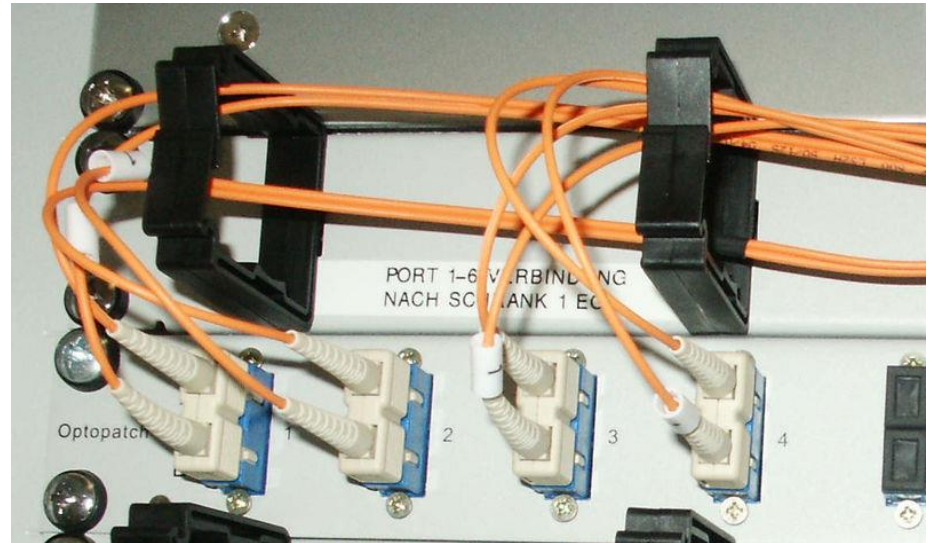
STP



Medien (2)

◆ Glasfaser („LWL“, „F“)

- Geeignet für Stern und Ring Topologie
- + Potentialtrennung
- + keine elektromagnetische Beeinflussung
- + hohe Bandbreite bei großen Längen
- + geringe Dämpfung
- + zukunftssicher
- passive, insbesondere aktive Komponenten teuer



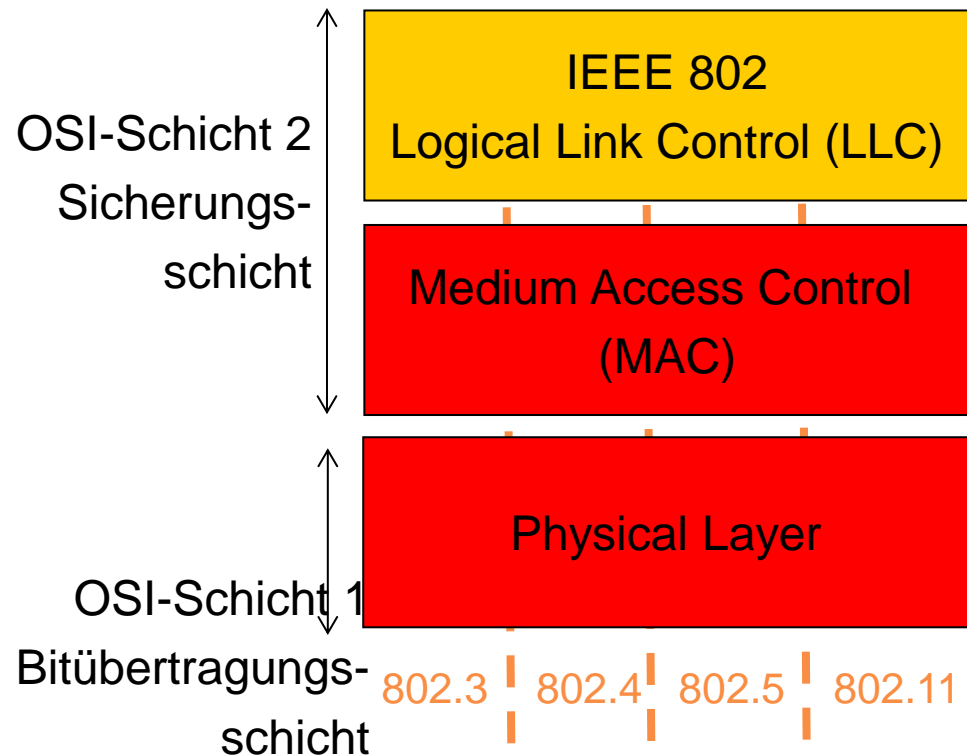
IEEE 802 Standards

◆ Standards für LANs (Local Area Networks)

◆ z.B.

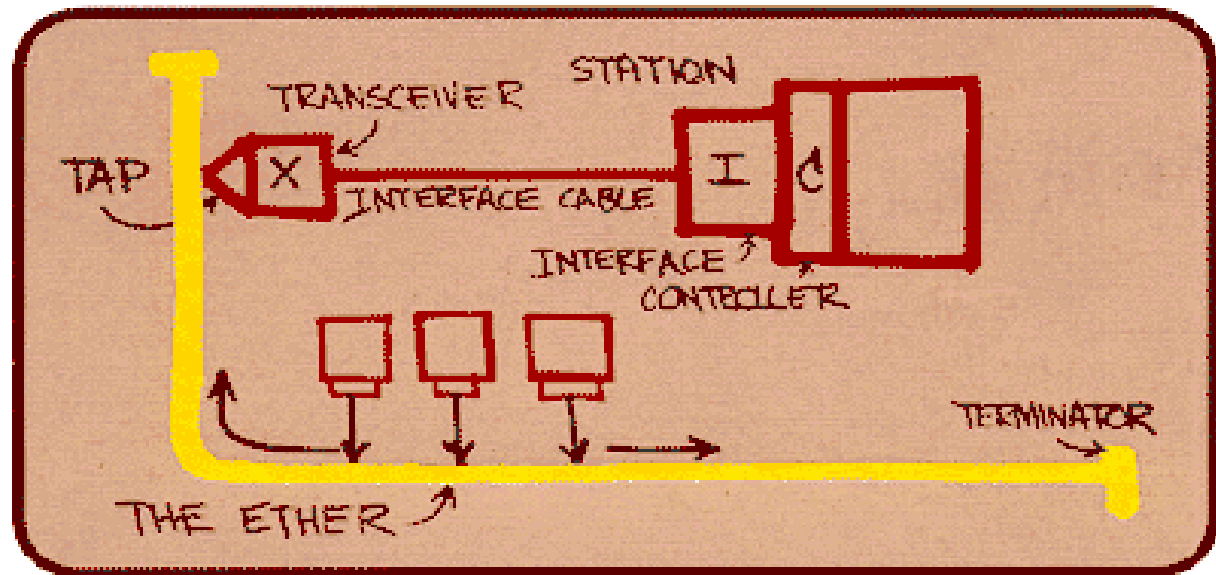
- 802.3 – Ethernet
- 802.4 – Tokenbus
- 802.5 – Tokenring
- 802.11 – WLAN
- 802.15 – Bluetooth

◆ Definiert OSI-Schicht 1 u. 2



Ethernet und IEEE 802.3

- ◆ Entwickelt Mitte der 70 Jahre am Xerox Palo Alto Research Center (Bob Metcalfe)
- ◆ Später überarbeitet von DEC, Intel and Xerox (DIX standard)
- ◆ Wurde 1985 mit leicht geändertem Frame-Format zu IEEE 802.3



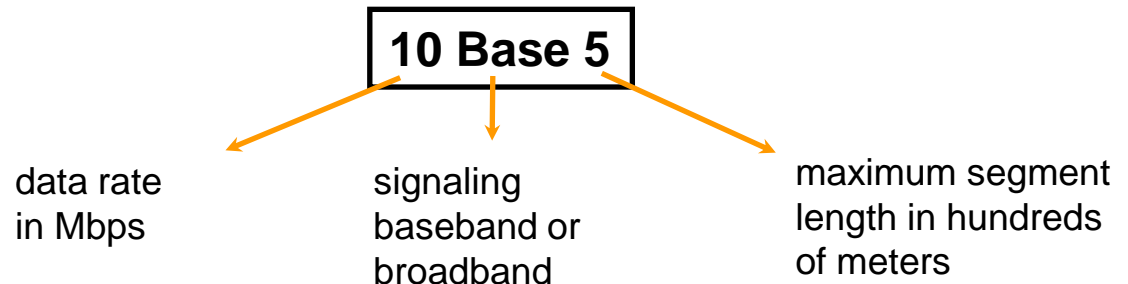
IEEE 802.3 Spezifikationen

♦ Verschiedene Standards für IEEE802.3

- 10Base5 -- thickwire coaxial
- 10Base2 -- thinwire coaxial oder cheapernet
- 10BaseT -- twisted pair
- 10BaseF -- fiber optics

♦ Fast Ethernet

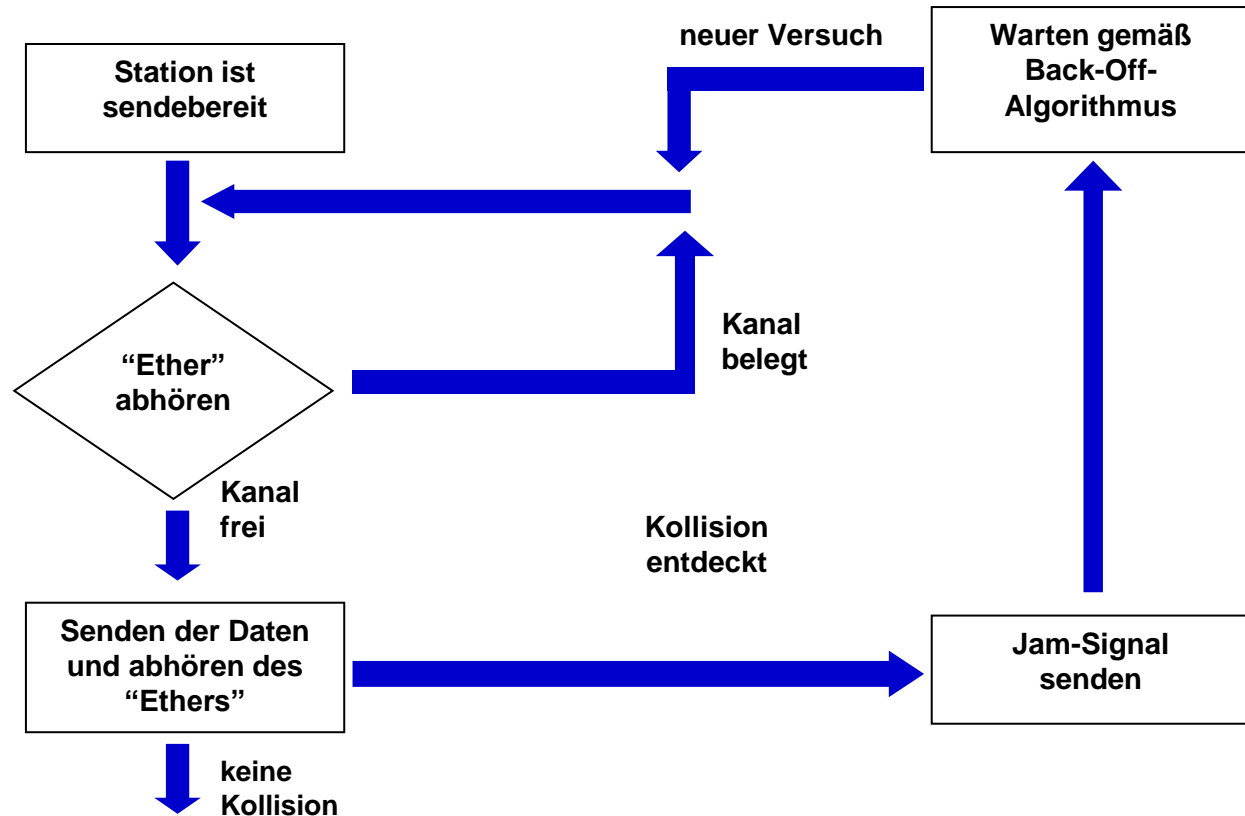
- 100BaseT
- 1GBaseT (Gigabit Ethernet)
- 10GBaseT
- 10GBaseFX
- und viele weitere...



Zugriffsverfahren: CSMA/CD

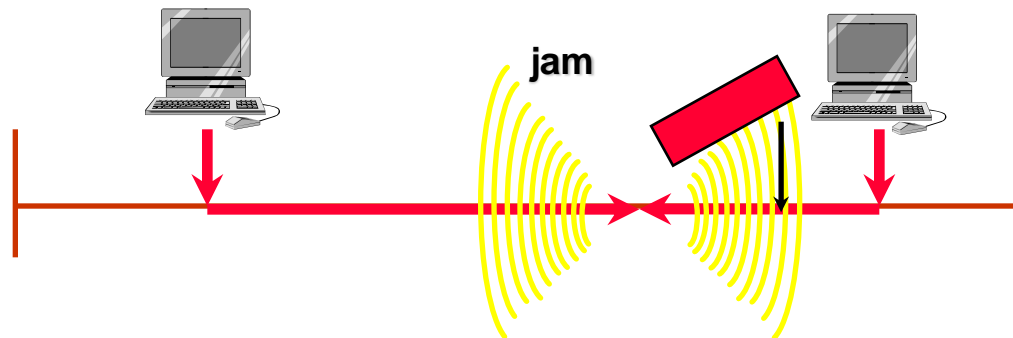
◆ Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- Erst Hören, dann Senden



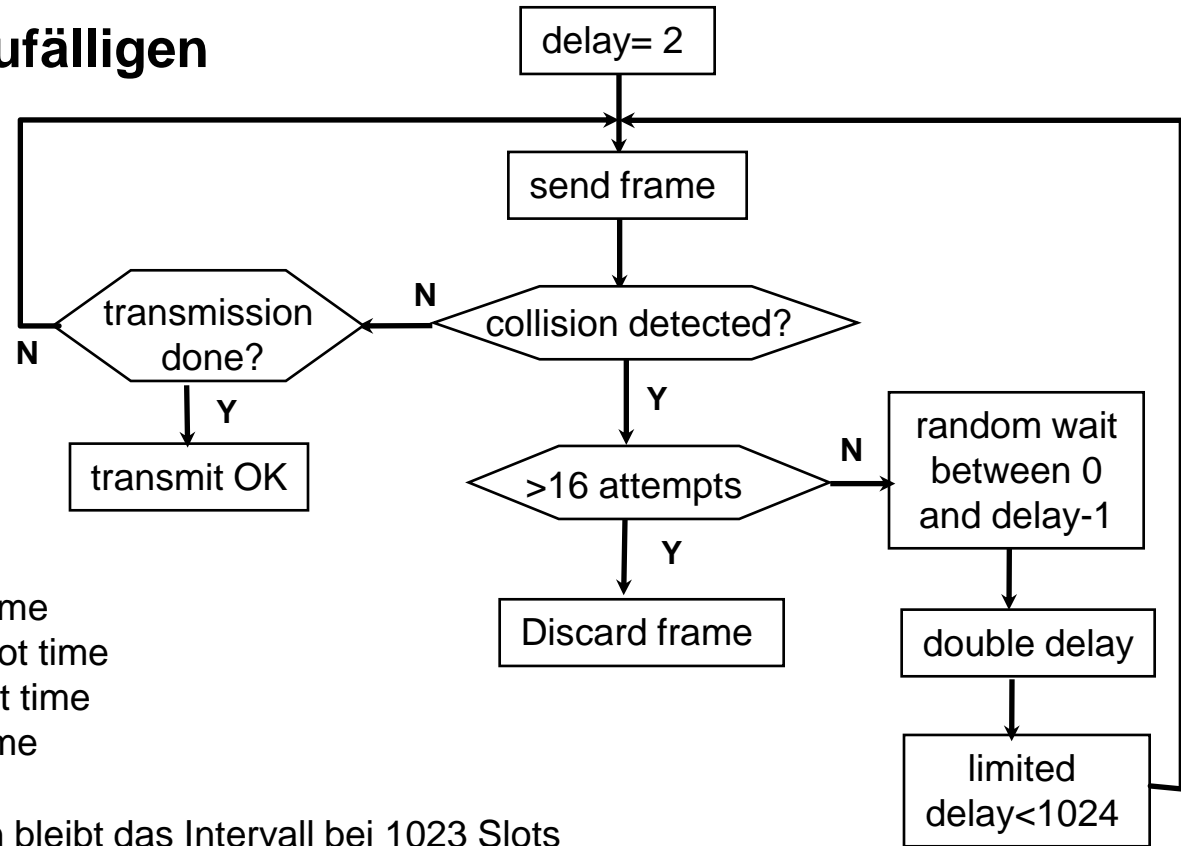
Kollision

- ◆ Mehr als eine Station sendet ein Frame zu einem Zeitpunkt
- ◆ Stationen überprüfen den Kanal bzgl. Kollisionen während sie senden
- ◆ Wenn der durchschnittliche Spannungspegel einen Schwellwert überschreitet, wird eine Kollision erkannt
- ◆ Sendende Stationen senden ein Jamming-Signal, wenn eine Kollision erkannt wird



Back-Off Algorithmus (1)

◆ Bestimmung der zufälligen Wartezeit nach der ersten Kollision



- 1st wait 0 or 1 slot time
- 2nd wait 0,1,2 or 3 slot time
- 3rd wait 0,1,2,..7 slot time
- kth wait 0.. 2^k slot time

Nach der 10. Kollision bleibt das Intervall bei 1023 Slots
Nach der 16. Kollision wird das Frame verworfen und ein Fehler gemeldet

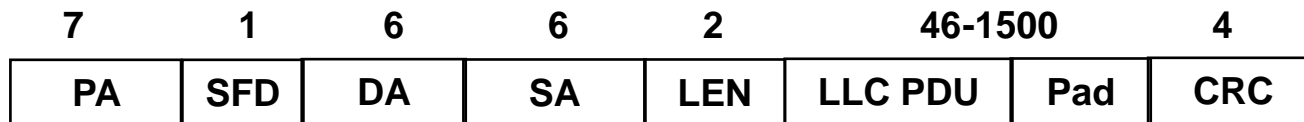
$$\begin{aligned} \text{max delay} &\leq \\ 1023 * 51.2 \text{ ms} &= 52.4 \text{ ms} \end{aligned}$$

Back-Off Algorithmus (2)

Anzahl der Wartezeiten, aus denen zufällig ausgewählt wird				
1	■ ■		2	50%
2	■ ■ ■ ■		4	75%
3	■ ■ ■ ■ ■ ■ ■ ■		8	87,5%
4	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		16	93,75%
5	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ...		32	96,88%
6	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		64	98,44
7	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		128	99,22%
8	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		256	99,61%
9	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		512	99,80%
10	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%
11	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%
12	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%
13	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%
14	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%
15	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%
16	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		1024	99,90%

IEEE 802.3 Frame Format

- ◆ **PA (Preamble):** Vorspann, besteht aus dem Bitmuster “0101010101...” und dient der Bit-Synchronisation des Empfängers
- ◆ **SFD (Start Frame Delimiter):** Startzeichen, besteht aus dem Bitmuster “10101011”
- ◆ **DA (Destination Address):** Empfängeradresse
- ◆ **SA (Source Address):** Absender Adresse
- ◆ **LEN (Length):** Gibt nach IEEE 802.3 die Länge des folgenden Datenfeldes in Bytes an
- ◆ **Data und Pad:** Datenfeld darf 46 bis 1500 Nutzdatenbytes enthalten
- ◆ **CRC/FCS (Frame Check Sequence):** Prüfzeichen, entspricht dem Polynom-Divisionsrest, der sich durch Anwendung des CRC-Verfahrens



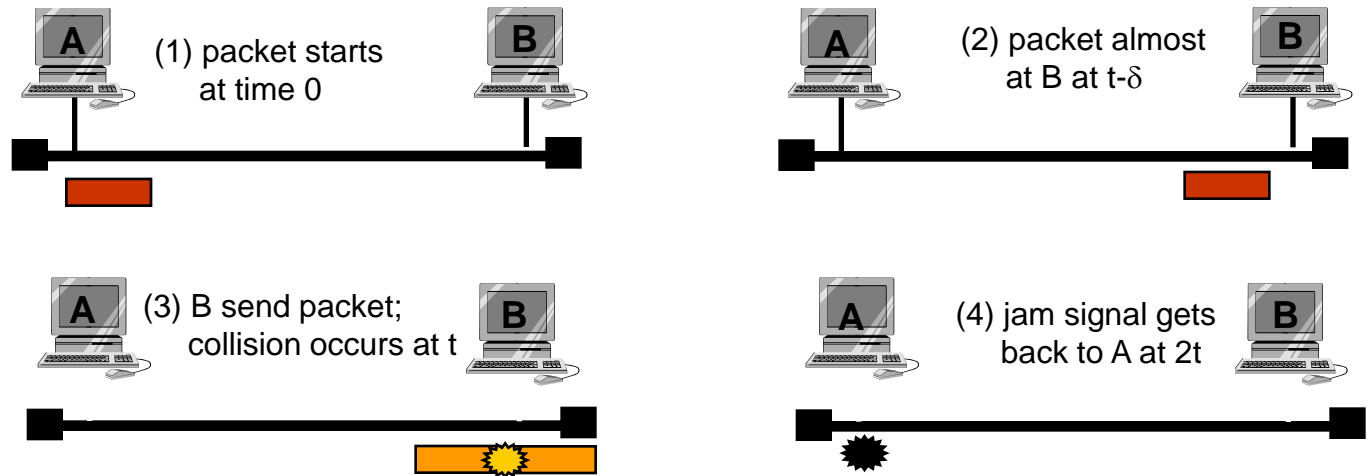
IEEE 802.3

calculation of the FCS

Minimale Frame-Größe

- ◆ Ein Signal braucht $2t$ um zum Empfänger und zurück zu kommen
 - Solange dauert es, bis ein Sender erfährt, ob ein Frame durch eine Kollision zerstört wurde
 - Hört er vorher auf zu senden, glaubt er alles sei okay gewesen!
- ◆ Zeit $\leq 51,2 \mu\text{s} = 512 \text{ Bit} = 64 \text{ Byte}$ (minimale Länge ohne Preamble)
- ◆ Mindestens 46 Byte Daten

A und B liegen am äußersten Ende des Kabels



MAC Adressen

♦ I/G

- =0 Individual address
- =1 Group address

I/G	U/L	46-bit address
-----	-----	----------------

♦ U/L

- =0 Global administered address
- =1 Local administered address

♦ **Unicast** : Ein Empfänger

♦ **Broadcast** : FFFFFFFF Jede Station

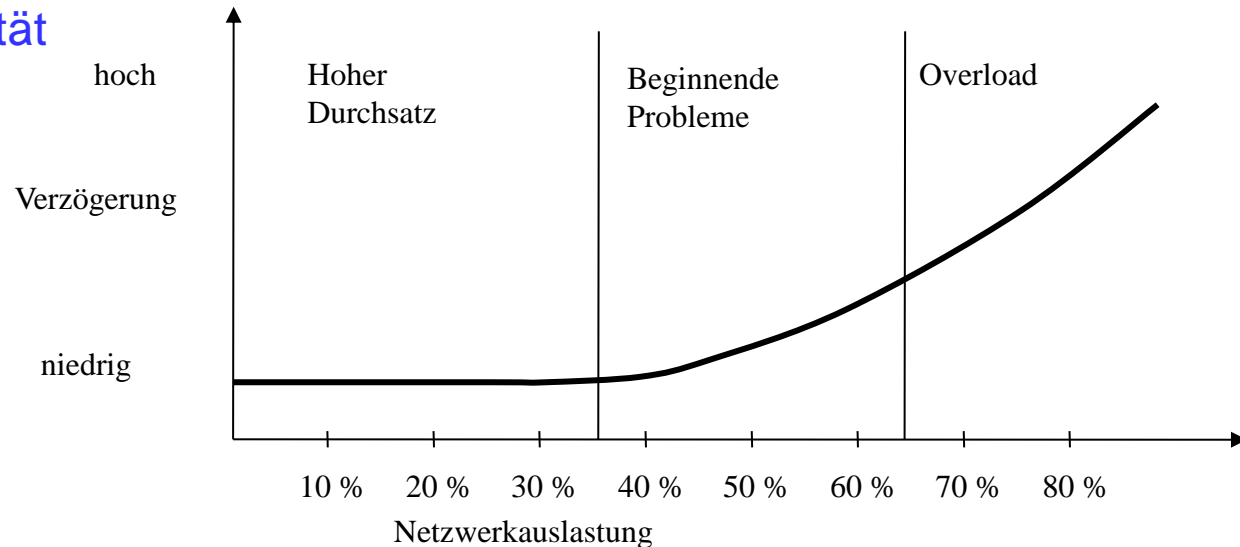
♦ **Multicast** : Mehrere Empfänger in einer definierten Gruppe

Erfahrungen mit Ethernet

◆ Ethernet funktioniert am besten unter leichter Last

- Auslastung über 30% kann als stark angenommen werden

- Netzwerkkapazität wird durch Kollisionen verschwendet



◆ Die meisten Netzwerke sind auf ca. 200 Hosts beschränkt

◆ Die meisten Netzwerke sind kürzer als die Spezifikation erlaubt

- 5 to 10 μ s RTT

◆ Ethernet ist billig, schnell und einfach zu administrieren

Fast and Gigabit Ethernet

- ◆ **Fast Ethernet (100Mbps) nutzt im Vergleich zu 10Mbps Ethernet ähnliche Technologie**
 - Andere Codierung auf der physikalischen Schicht
 - Die meisten Adapter unterstützen wahlweise 10 und 100 Mbps
- ◆ **Gigabit (1.000Mbps) und 10 Gigabit (10.000Mbps) Ethernet**
 - Kompatibel mit den geringeren Geschwindigkeiten
 - Benutzt Standard Frames und CSMA/CD Algorithmus
 - Typischerweise im Backbone benutzt
- ◆ **Heute üblich: Punkt-zu-Punkt Vollduplex-Verbindungen!**
 - Keine Kollisionen mehr
 - Trotzdem rückwärtskompatibel
 - CSMA/CD implementiert
 - Mindestlänge 64 Byte

ARP/RARP

- ◆ **Address Resolution Protocol (ARP):**
- ◆ **Verbindung der logischen Netz(IP)adresse mit der von LAN- bzw. WAN-Infrastruktur abhängigen Hardwareadresse (MAC-Adresse)**
- ◆ **Address Resolution Protocol (ARP), RFC 826: Übersetzung der IP-Adresse in die entsprechende Hardwareadresse**
 - **Wird für die normale Kommunikation benötigt**
- ◆ **ARP arbeitet vollständig automatisch (dyn. ARP-Cache)**

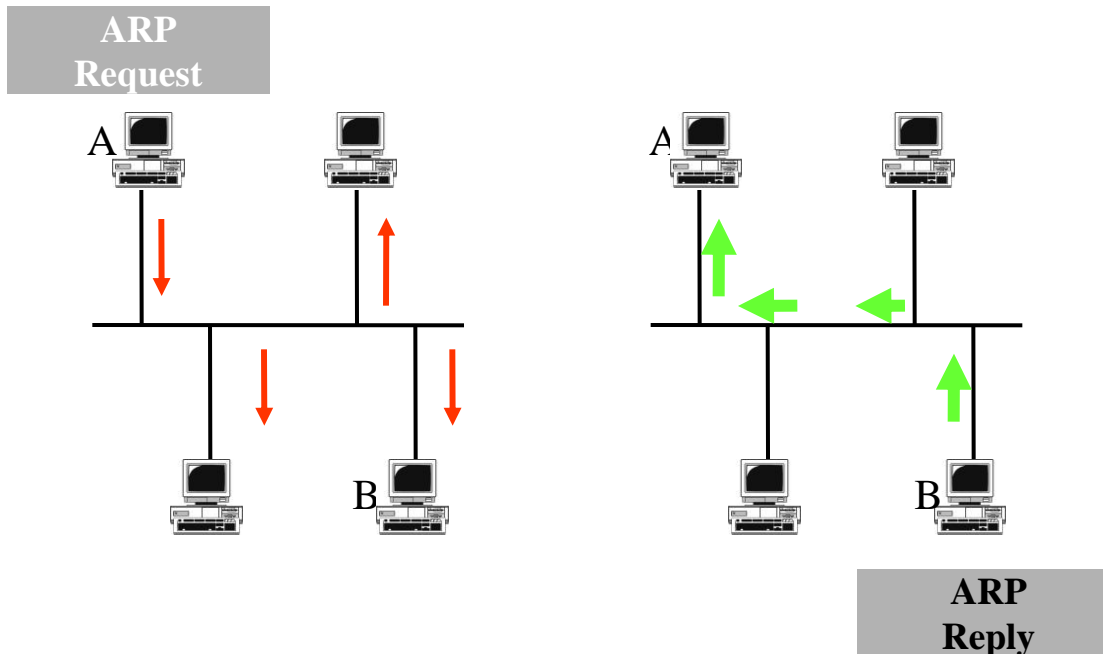
ARP Request / Reply

◆ ARP Request

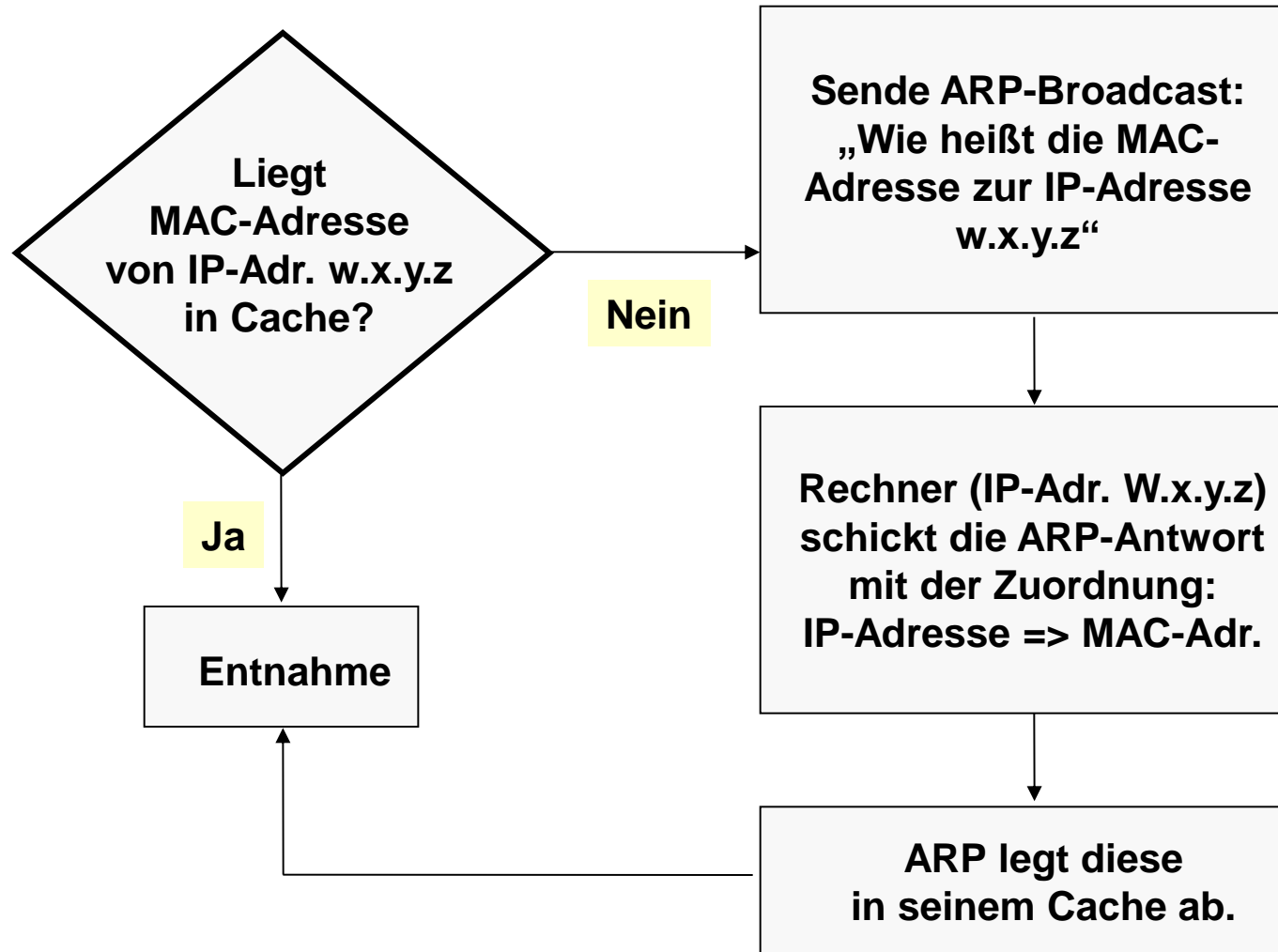
- MAC-Broadcast an alle Endsysteme des LANs
- Gesuchte Adresszuordnung : IP-Adresse B => MAC-Adresse B

◆ ARP-Reply

- MAC-Unicast des Endsystems B mit Adresszuordnung



Adressierung mit dem Protokoll ARP



ARP-Spoofing

- ◆ **Angriffs-Methode: Man-in-the-Middle-Attack**
- ◆ **Vorgehen:**
 - Um den Datenverkehr zwischen A und B abzuhören, sendet der Angreifer an A eine manipulierte ARP-Nachricht.
 - A wird erzählt, dass die IP-Adresse von B zur MAC-Adresse des Angreifers gehört
 - A sendet alle Nachrichten statt an B an den Angreifer, der leitet ggf. dann erst an B weiter
- ◆ **In LANs mit Switches klappt das auch**
 - Der Switch wird mit ARP-Nachrichten so überlastet, dass er aufgibt und alles weiter leitet
- ◆ **Tools:**
 - Cain & Abel – ARP-Spoofing unter Windows
 - Ettercap – Sniffer für Switched LANs

LAN-Strukturelemente

Übersicht

◆ Ebene 1

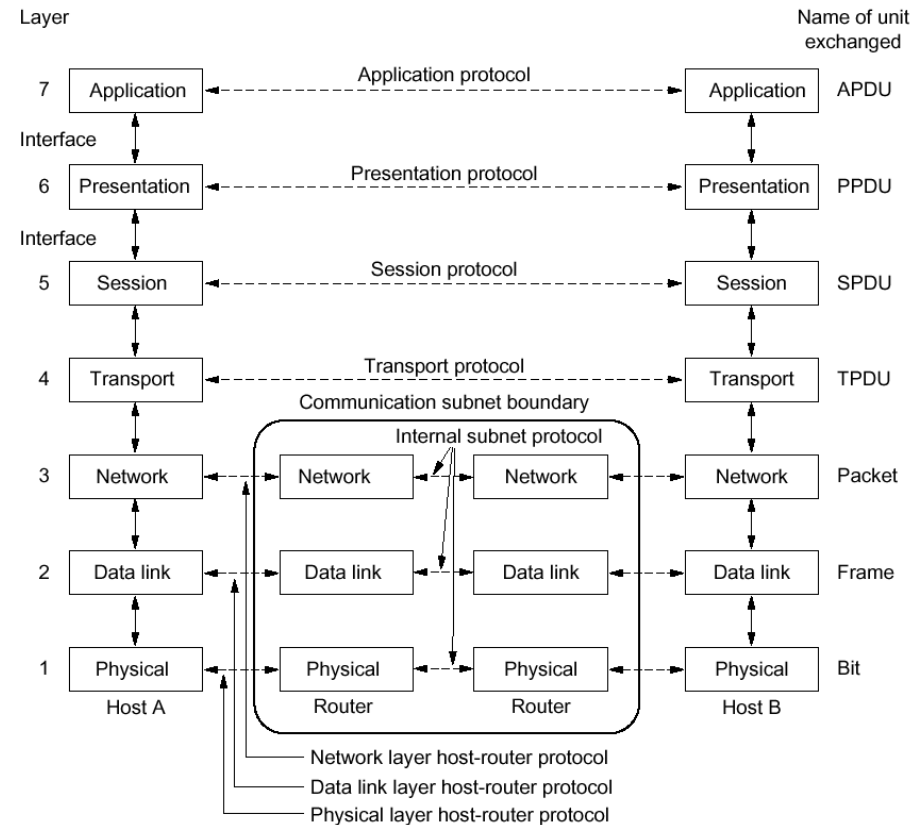
- Medien-Verbund (z.B. gemeinsamer Ethernet-Kollisionsbereich)
 - unabhängig von Ebene 2/3 - Info
- ⇒ Repeater / Hubs

◆ Ebene 2

- Frame-Verbund
 - unabhängig von Ebene 3 - Info
- ⇒ Bridges / Switches

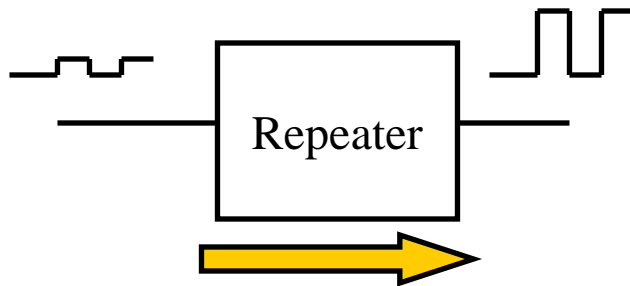
◆ Ebene 3

- (IP-)Paket-Verbund
- ⇒ Router

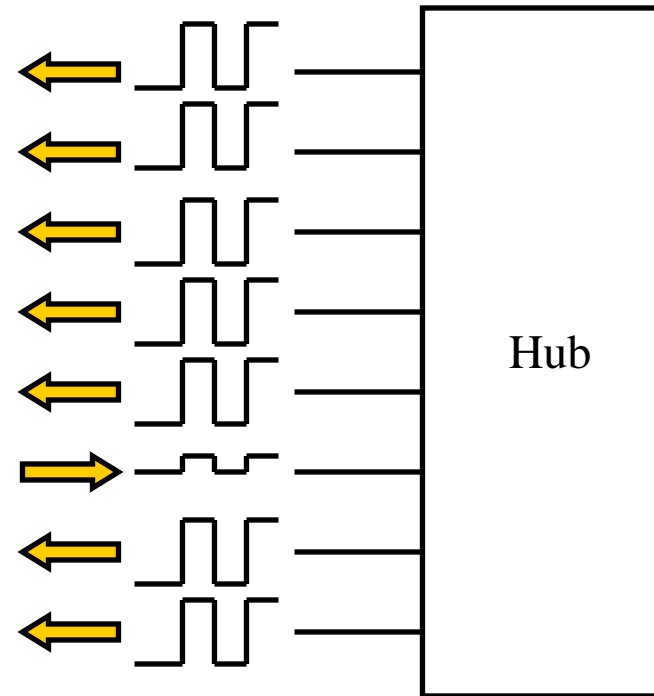


Repeater / Hub (Layer 1)

- ◆ Repeater verstärken physikalische Signale

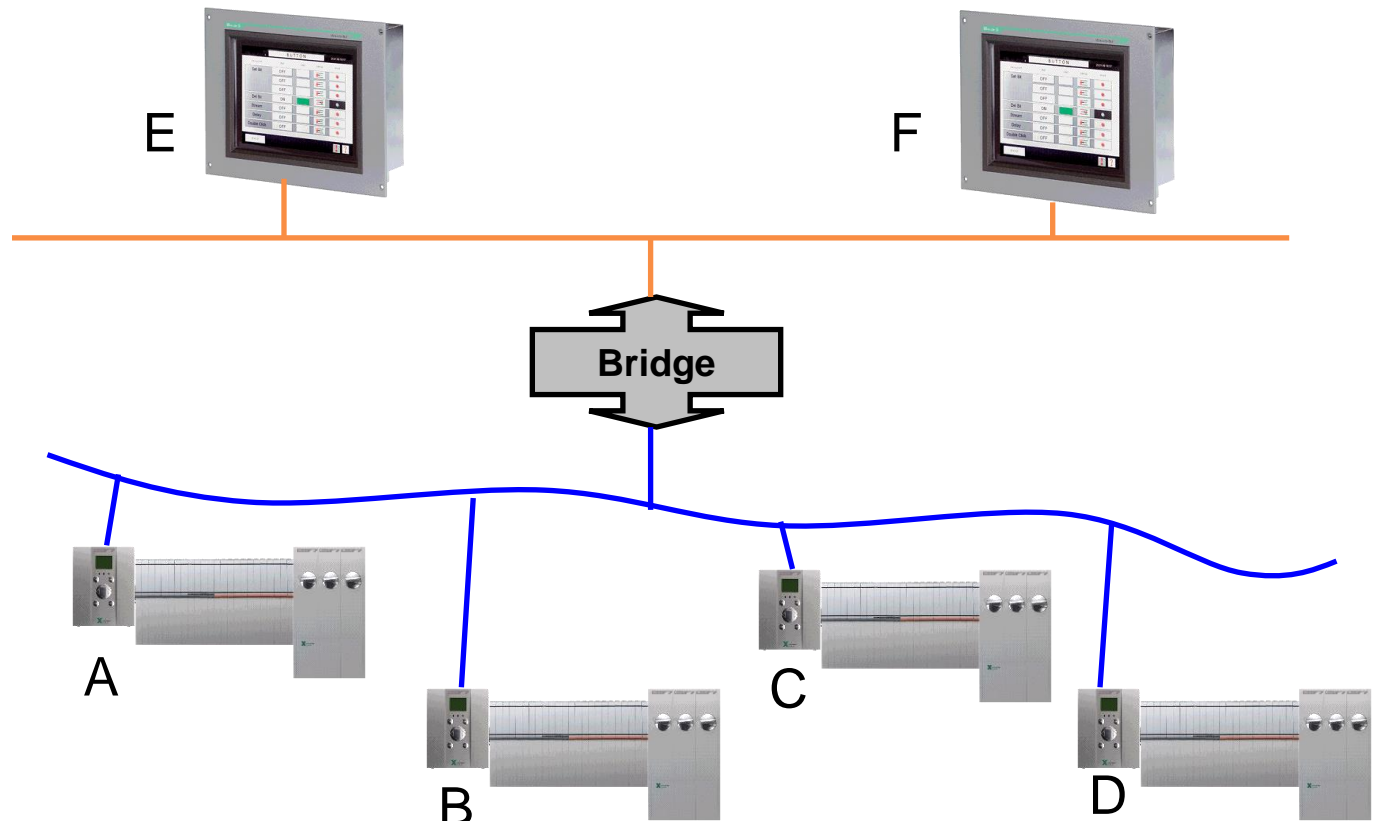


- ◆ Hubs verteilen die Signale an alle Ausgänge



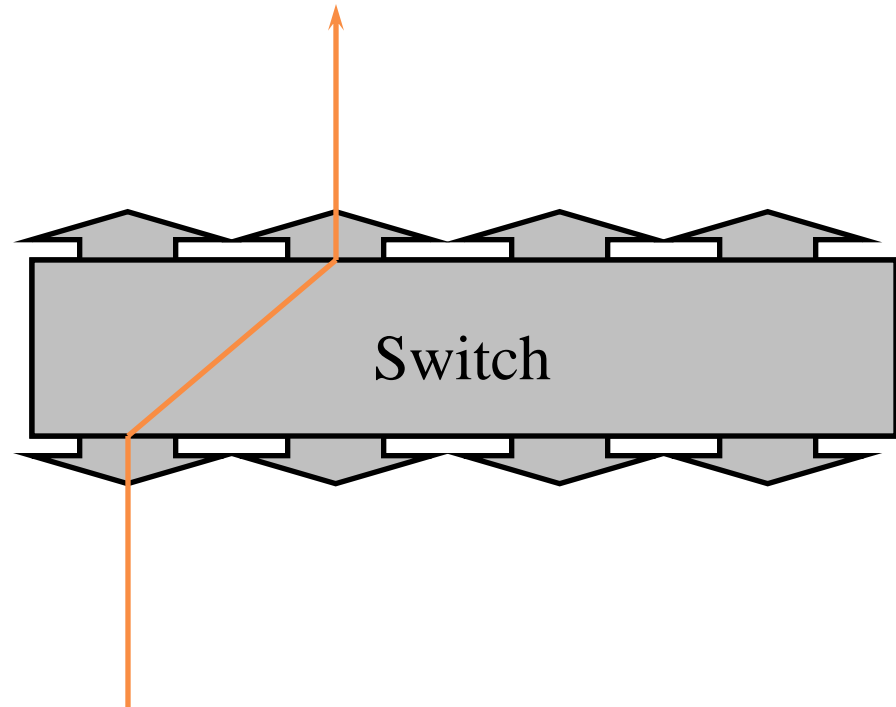
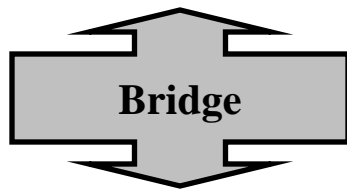
Bridge (Layer 2)

- ◆ Bridges vermitteln zwischen zwei (verschiedenen) physikalischen Schichten (z.B. Ethernet und WLAN)

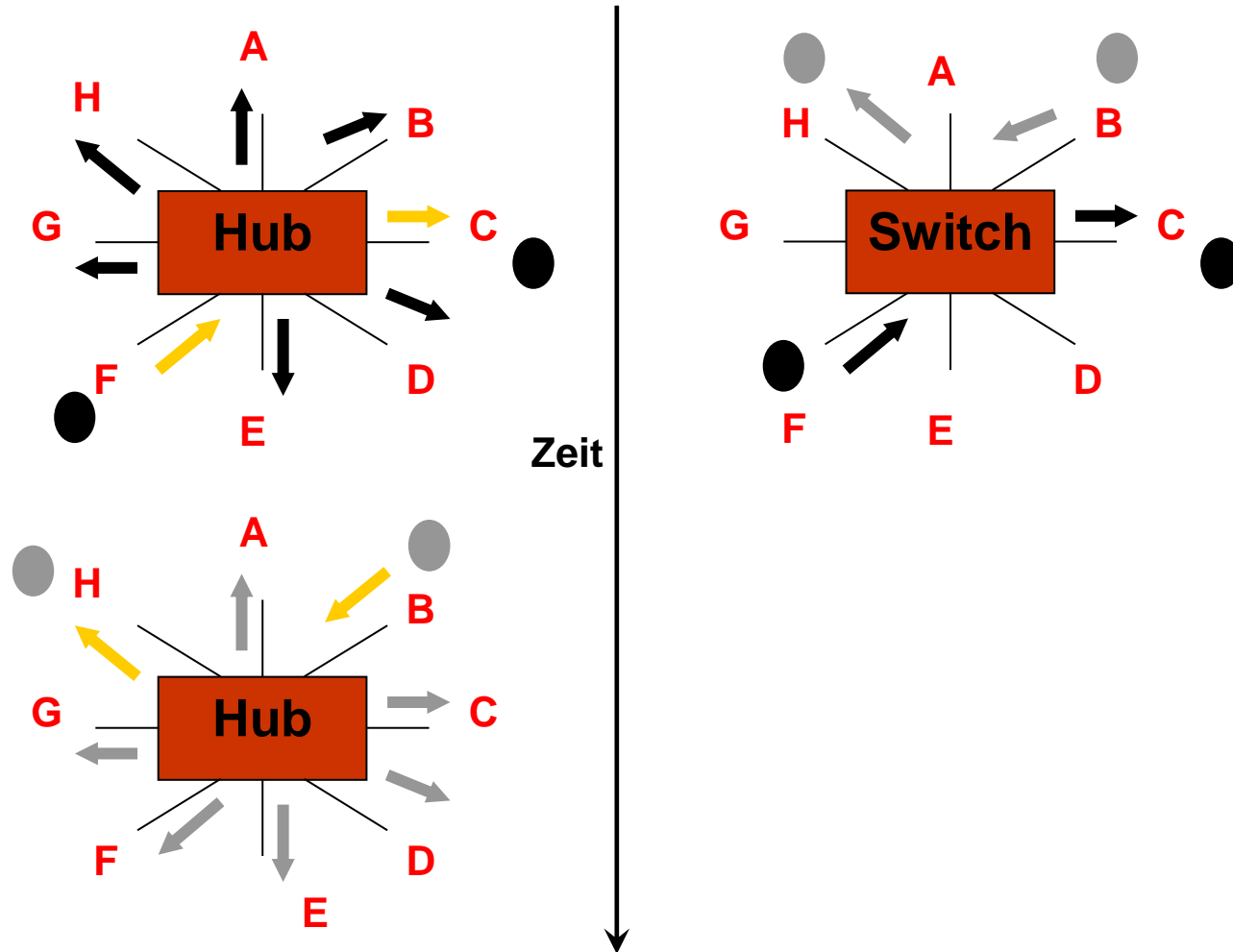


Switch = Multiport Bridge

- ◆ Bridges vermitteln (schaltet) zwischen mehreren Interfaces



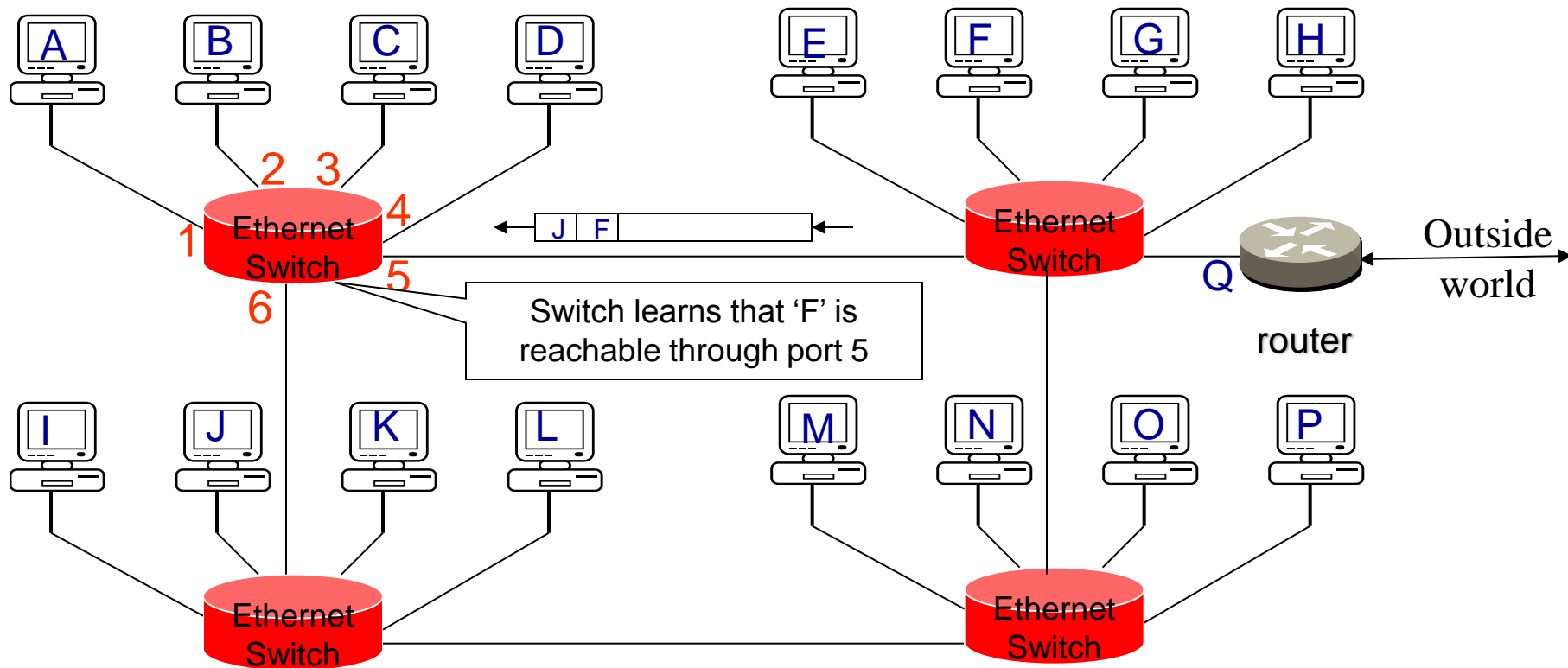
Unterschied Hub - Switch



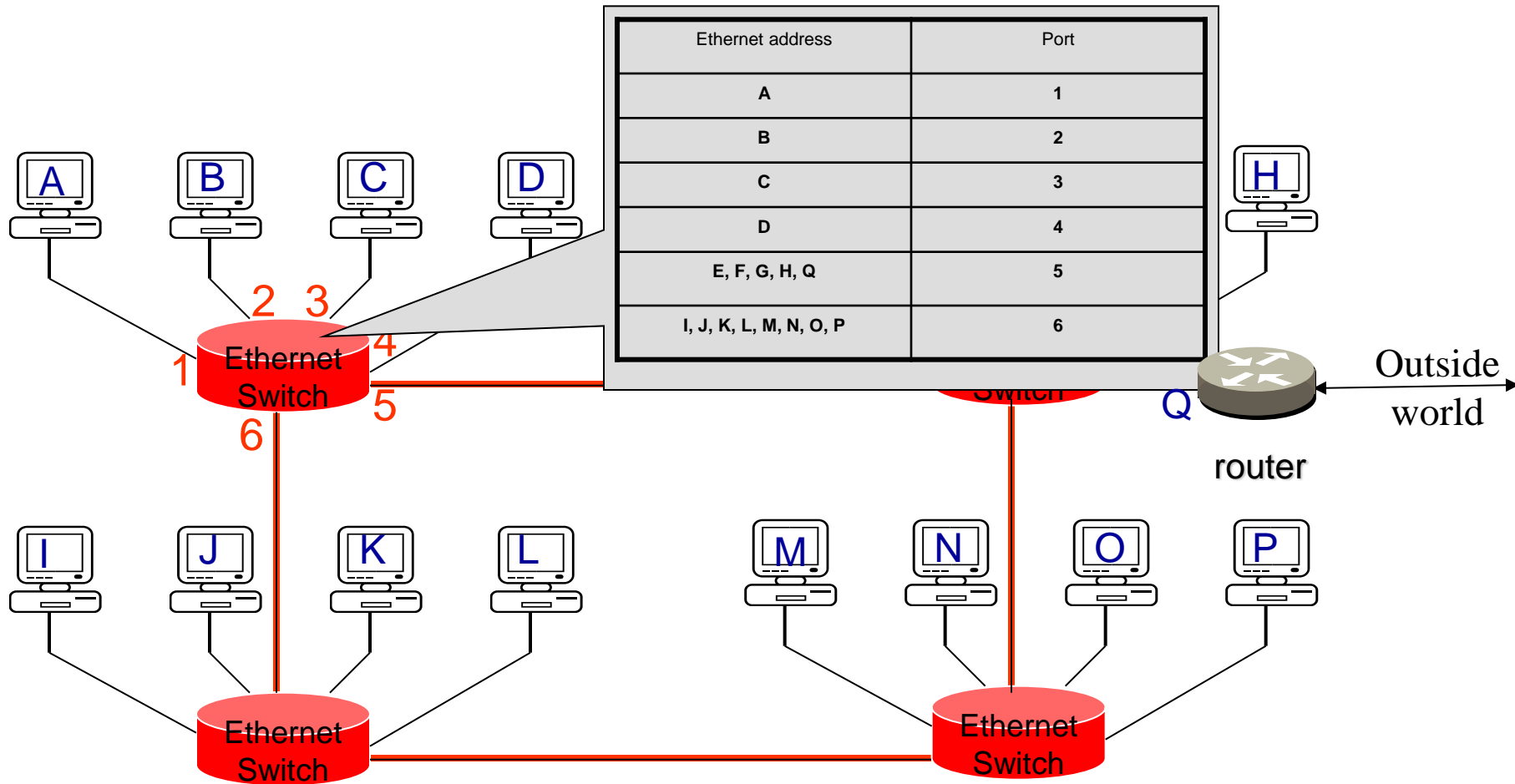
Ethernet Switching (2)

1. **Überprüft den Header eines einkommenden Frames**
2. **Wenn die Zieladdr. in einer internen Tabelle bekannt ist, wird das Frame zu dem entsprechenden Port weitergeleitet**
3. **Wenn die Zieladdr. in der internen Tabelle nicht bekannt ist, wird das Frame als Broadcast an allen Ports versendet (ausser an dem von dem es gekommen war).**
4. **Die Inhalte der Tabelle werden aus den Quelladr. der einkommenden Frames gelernt.**

Ethernet Switching (3)



Ethernet Switching (4)

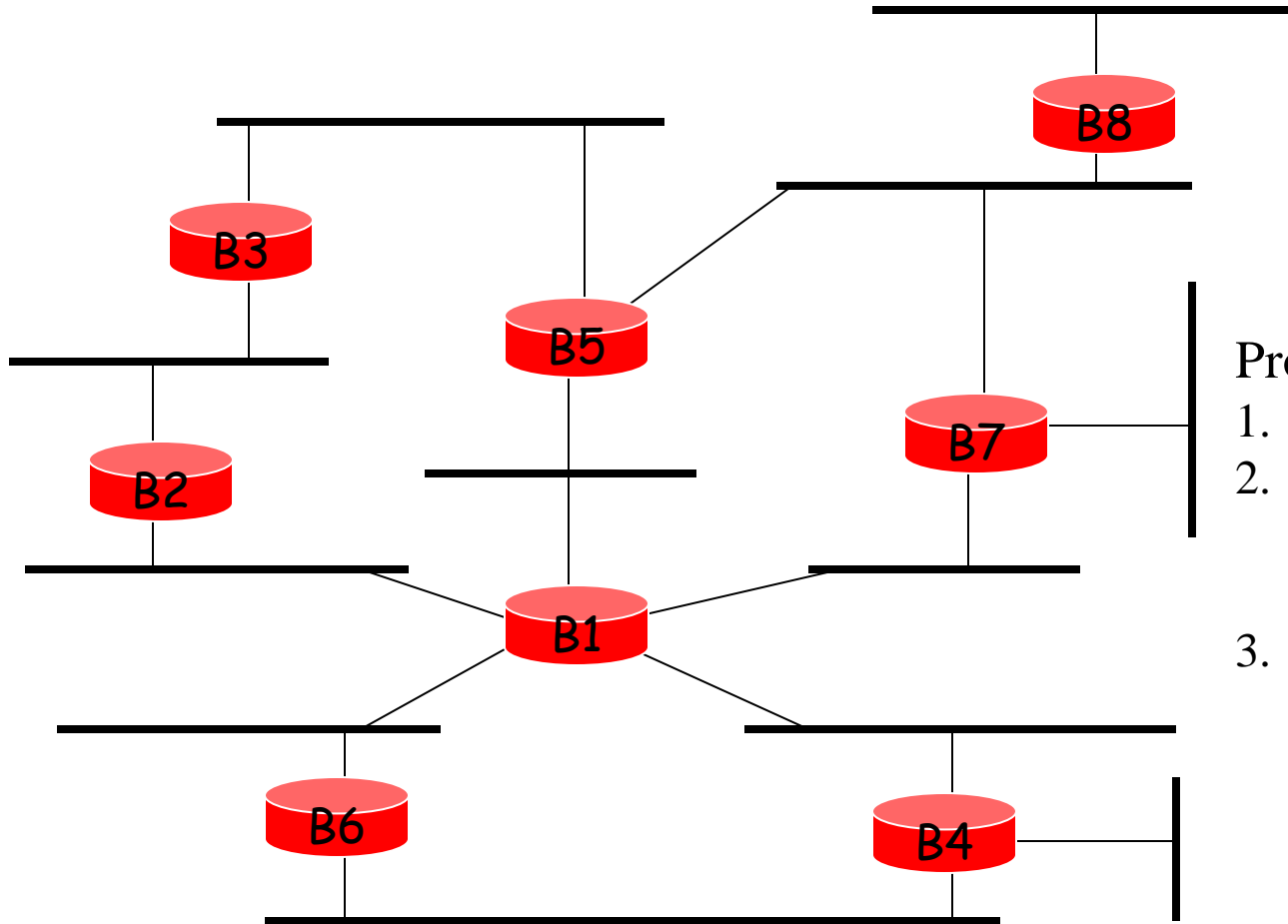


Q: How do we prevent loops?

Redundante Wege

- Bei gekoppelten Netzwerken z.B. über Switches können redundante Wegez zwischen zwei Netzen existieren (z.B. zur Fehlertoleranz).
- Problem:
 - Repliziert empfangene Datenpakete (über verschiedene Wege)
 - Endlos kreisende Datenpakete (Schleifen)
- Lösung:
 - Etablierung einer *logischen Baumstruktur* über allen Brücken der involvierten Netzwerke (⇒ Spanning-Tree-Algorithmus)
 - Weiterleiten von Datenpaketen nur entlang der Baumstruktur (eindeutiger Pfad), restliche Brücken blockieren ihre Ports

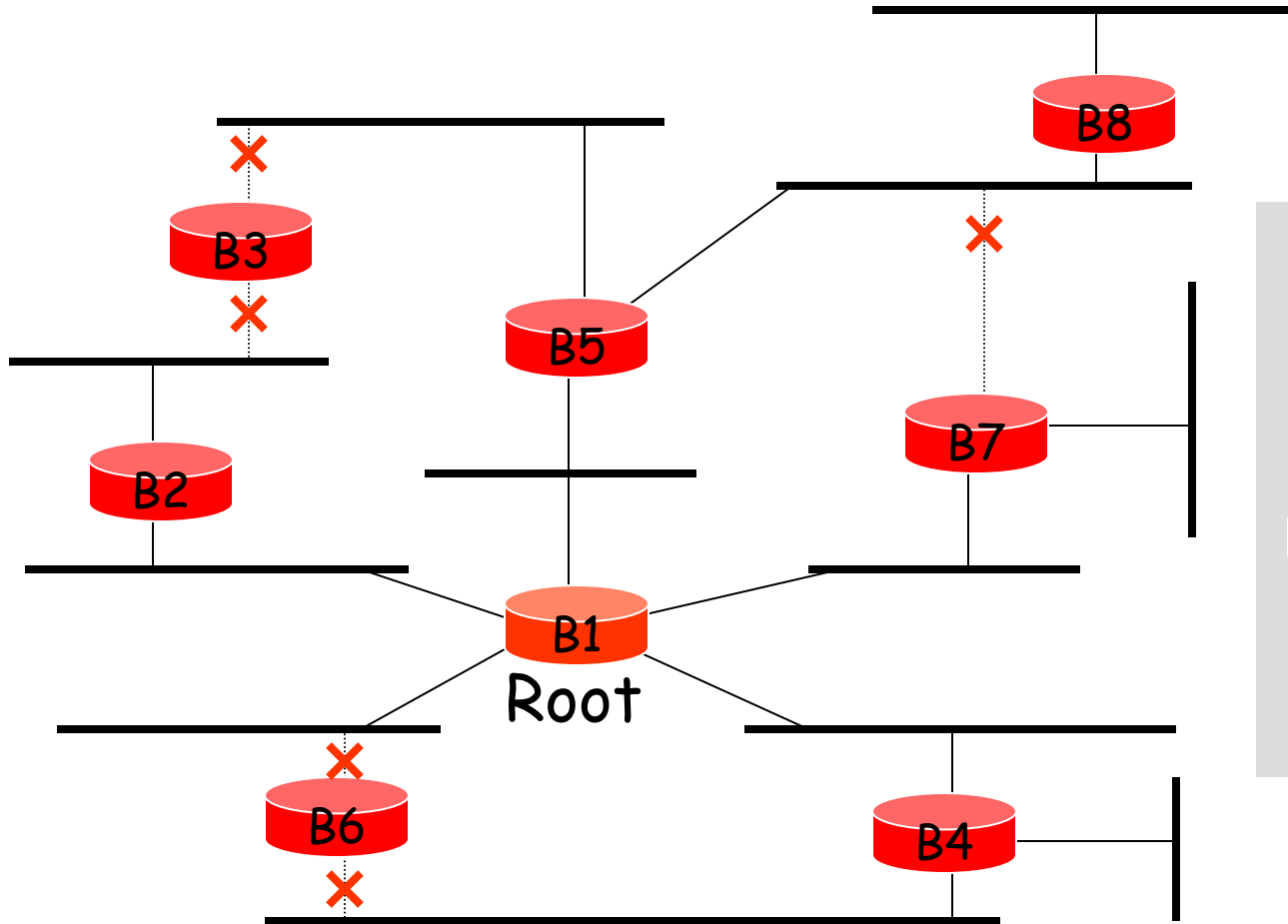
Beispiel: Spanning Tree



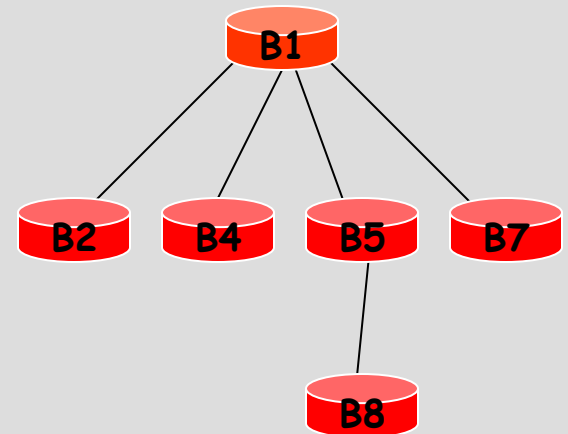
Protocol operation:

1. Picks a **root**
2. For each LAN, picks a **designated** bridge that is closest to the root.
3. All bridges on a LAN send packets towards the **root** via the **designated** bridge.

Example Spanning Tree



Spanning Tree:



Spanning-Tree-Algorithmus

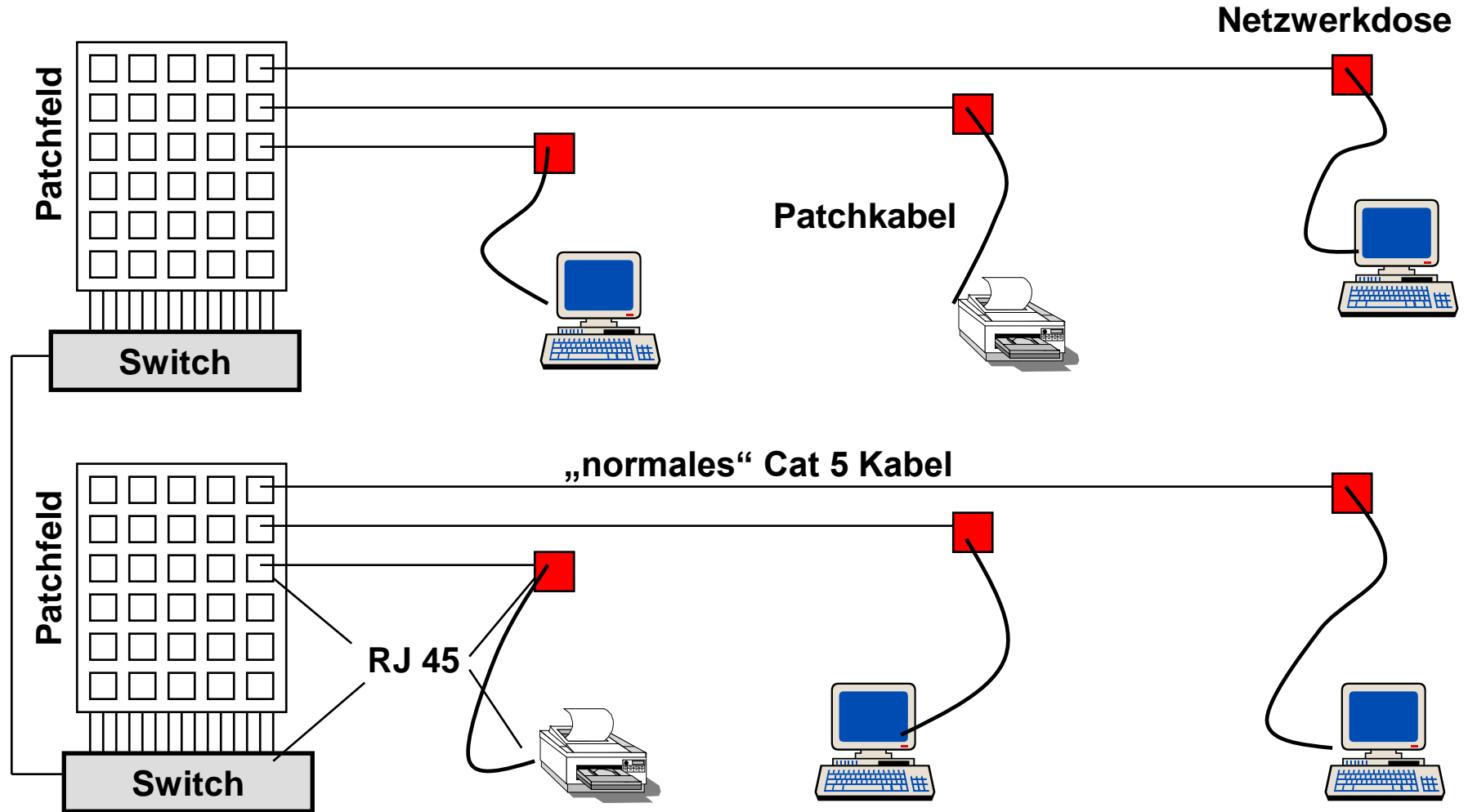
- Voraussetzungen:
- Gruppenadresse zur Adressierung aller Bridges im Netz
 - Eindeutige Bridgekennungen
 - Eindeutige Anschlusskennungen in jeder Brücke
 - Kosten an allen Anschlüssen einer Brücke („Anschlusskosten“)

- ◆ Ablauf: 1. **Bestimmen der Root-Brücke (Wurzel des Baumes):**
- Zuerst nimmt jede Brücke an, dass sie Root-Brücke ist
 - Root-Bridge senden regelmäßig Hello-Pakete mit ihrer Bridgekennung aus
 - Bei Erhalt eines Hello-Pakets mit kleinerer Bridgekennung ordnet sich eine Root-Brücke der anderen unter und sendet das Paket als Broadcast

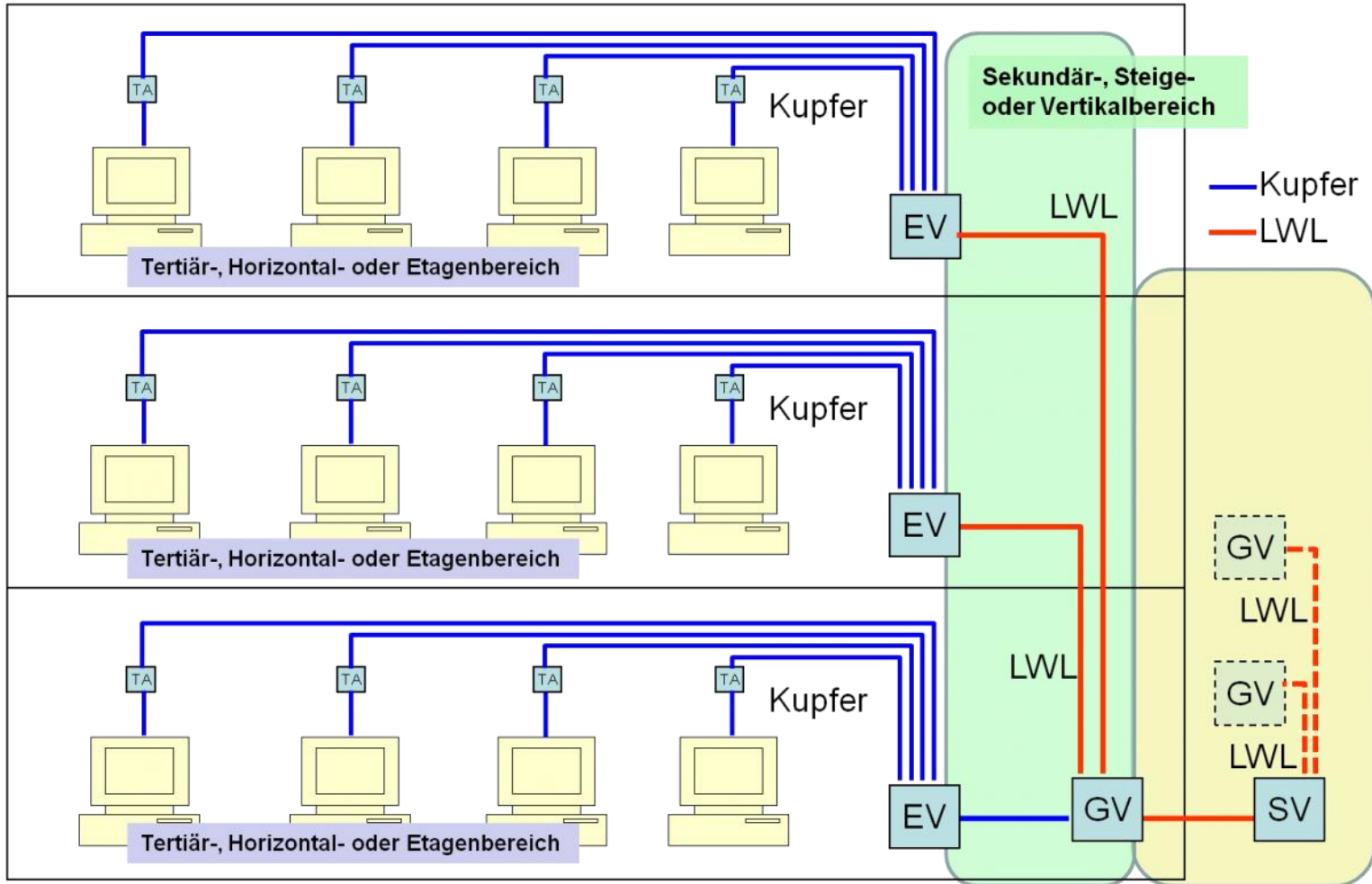
- ◆ 2. **Bestimmen der Root-Ports**
- Root-Port einer Brücke = Port über den der günstigste Pfad Richtung Root-Brücke (nur Kosten für Ausgangsports berücksichtigen!) verläuft
 - Summe über alle Anschlusskosten auf dem Weg zur Root-Brücke ist zu minimieren
 - Übertragungsgeschwindigkeit kann als Kostenfunktion dienen

- ◆ 3. **Bestimmen der Designated-Brücke:**
- Brücke mit günstigstem Root-Anschluss in einem Netzwerk wird als Designated-Brücke bestimmt
 - Root-Brücke ist Designated-Brücke für alle an sie angeschlossenen Netze

Typische Büroverkabelung



Strukturierte Verkabelung Bereiche



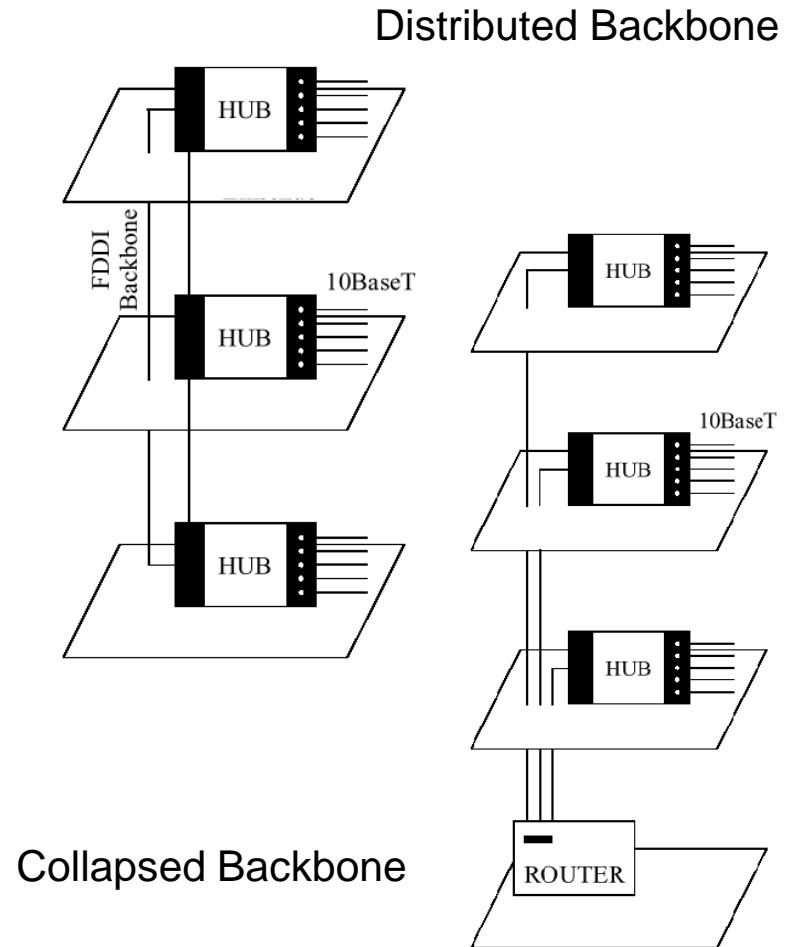
Backbone Concepts

◆ Distributed Backbone

- Subnets sind verbunden über ein (schnelles) Netzwerk
- Möglicherweise über Bridges oder Routers

◆ Collapsed Backbone

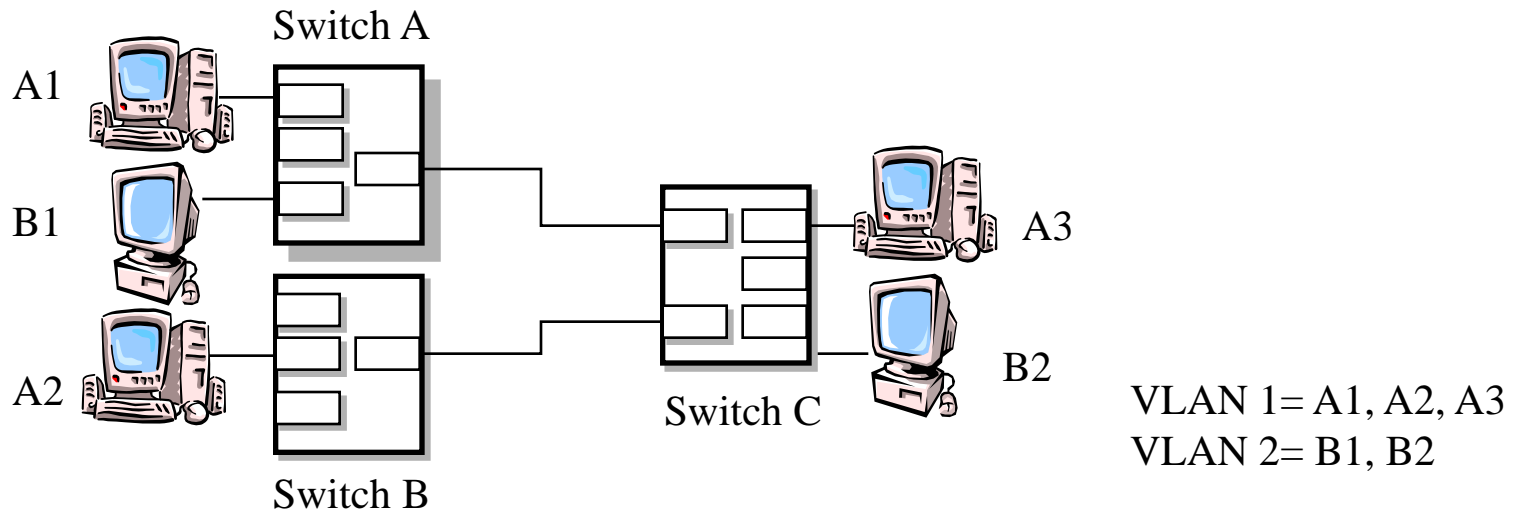
- Subnets sind verbunden über einen zentralen Switch/Router



Virtuelle LANs (1)

- **VLAN**

- Eine nach bestimmten Kriterien definierbare Broadcast-Domän
- Ziel: **Trennung von physikalischer und logischer Netzwerkstruktur**
 - Datenpakete werden ausschließlich innerhalb des jeweiligen VLANs verteilt
 - Mitglieder eines VLANs können räumlich verteilt sein, z.B. an verschiedenen LAN-Switches
 - ⇒ Unabhängigkeit von Standort und VLAN-Zugehörigkeit



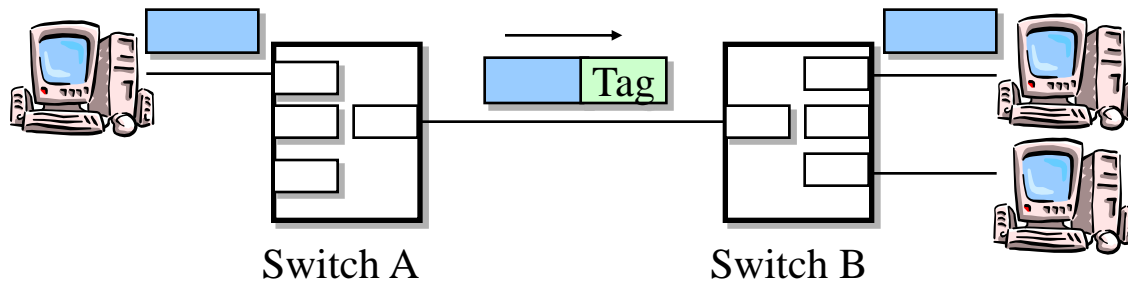
Virtuelle LANs (2)

♦ Vorteile

- Einschränkung von Broadcasts/Multicasts ⇒ bessere Ausnutzung der Bandbreite
- Effizientere Verwaltung durch vereinfachte Konfiguration
 - z.B. bei Änderungen der Netztopologie durch Umzug
- Erhöhte Sicherheit
 - Authentifikation vor dem Beitritt einer Station zu einem VLAN
 - Strikte Trennung des Datenverkehrs verschiedener LANs

♦ Realisierung

- Analyse des eingehenden Pakets auf VLAN-Zugehörigkeit (interne Tabelle)
- Erster Switch fügt ein „Tag“ an das Paket an (Feststehende Kennung für jedes VLAN)
 - IEEE 802.1q
- Weiterleitung des Datenpakets an den nächsten Switch
- Letzter Switch entfernt das Tag und übergibt das Paket an das Endsystem



Virtuelle LANs (3)

◆ Schicht-2-VLANs

- Realisierung durch LAN-Switches
 - VLAN wird durch mehrere Ports festgelegt (*port based VLAN*)
 - VLAN wird durch eine Liste von MAC-Adressen definiert (*MAC-based VLAN*)
 - einfacher Umzug einzelner Stationen möglich
- ⇒ Router zur Kommunikation zwischen VLANs notwendig

◆ Schicht-3-VLANs

- Realisierung durch Layer-3-Switches
 - VLAN wird durch Subnetz-Adresse festgelegt (*subnet-based VLAN*)
 - VLAN wird durch Netzwerkprotokoll festgelegt (*protocol-based VLAN*)
- ⇒ Kein Router zur Kommunikation zwischen VLANs notwendig

◆ Regelbasierte VLANs

- Beliebige Verknüpfung von Feldern der Schicht 2/3 zur Definition eines VLANs

Layer 2 - Geräte

◆ Managed Switches

unterstützen:

- VLANs
- STP
- Port Security
 - IEEE 802.1x („Login am Port“)
- Port Mirroring
 - Zum Monitoring



◆ Unmanaged Switches

Typ. Desktop Switches

- nur Frame-Weiterleitung



Power over Ethernet (PoE)

◆ Nach Standard IEEE 802.3af

- Sinn: nur ein Kabel zum Geräte
- Typisch für WLAN-APs

◆ Hardware

- TP-Kabel nach CAT-5
- RJ45-Stecker

◆ Leistung

- Abgegebene Spannung zwischen 44 V und 54 V (in der Regel 48 V)
- Leistung von 15,4 W (eingeteilt in 4 Klassen)
- Kabellänge bis zu 100 m

◆ Varianten der Energieversorgung

- Endspan (direkte Versorgung durch Switch)
- Midspan (Versorgung über zwischengeschaltete Quellen)
 - -sog. „Power Injector“

