Netzwerktechnologien
3 VO

Dr. Ivan Gojmerac
ivan.gojmerac@univie.ac.at

10. Vorlesungseinheit, 05. Juni 2013

Bachelorstudium Medieninformatik
SS 2013

5.3 Klassifikation von MAC-Verfahren

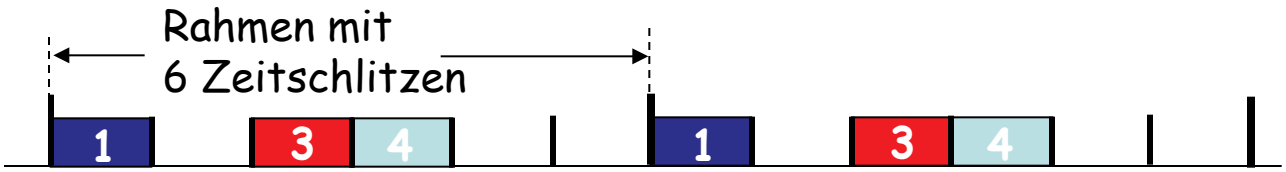
- Kanalaufteilungsprotokolle
  - Das Mediums wird in Subeinheiten zerlegt
  - Jeder Station wird eine Einheit zur exklusiven Benutzung zugeordnet
- Wahlfreier Zugriff (Random Access)
  - Datenrate wird nicht unterteilt
  - Stationen können wahlfrei auf den ganzen Kanal zugreifen
  - Dabei kann es zu Kollisionen kommen
  - Kollisionen müssen geeignet behandelt werden
- Abwechselnder Zugriff
  - Die Zugriffe der Stationen werden koordiniert, es darf abwechselnd gesendet werden
  - Kollisionen werden vermieden

5.3 Kanalaufteilung mittels TDMA

Time Division Multiple Access (**TDMA**, ~ Zeitmultiplexing)
→ Auf das Medium wird in Runden zugegriffen

- Jede Station bekommt einen festen Zeitschlitz zum Senden in jeder Runde
- Nicht verwendete Zeitschlitze gehen verloren

Beispiel: LAN mit 6 Stationen, 1,3,4 senden, 2,5,6 senden nicht:

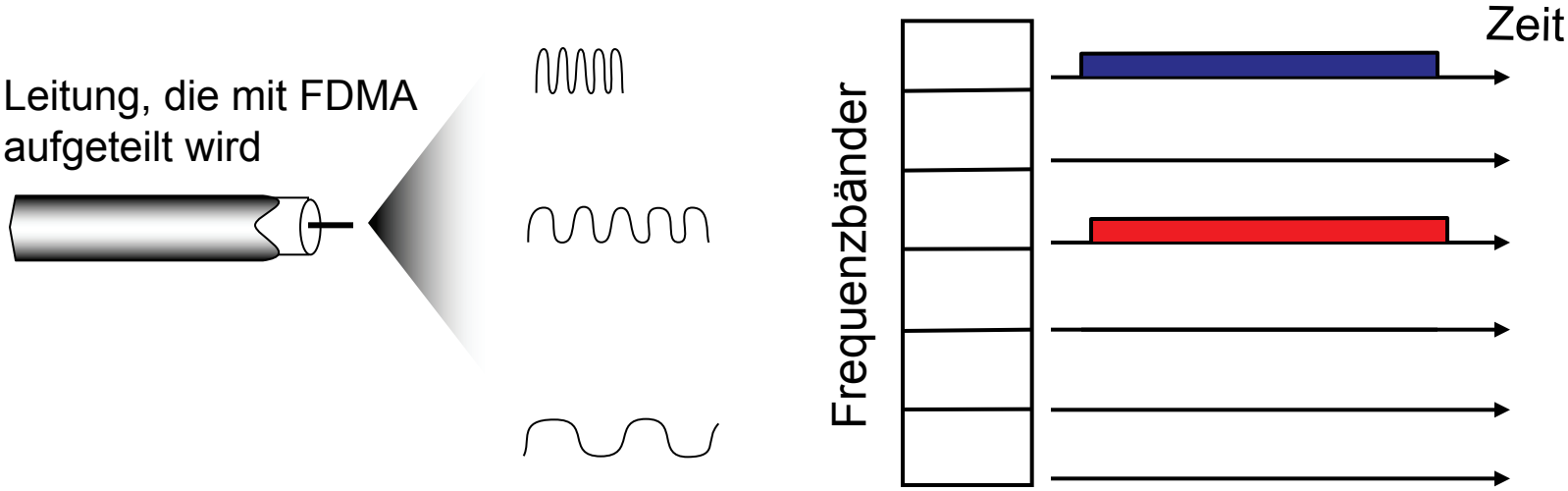


5.3 Kanalaufteilung mittels FDMA

Frequency Division Multiple Access (FDMA, ~Frequenzmultiplexing)
→ Das Spektrum des Mediums wird in Frequenzen aufgeteilt

- Jeder Station wird ein fester Frequenzbereich zugeteilt
- Wenn eine Station nicht sendet, wird der entsprechende Frequenzbereich nicht verwendet

Beispiel: LAN mit 6 Stationen, 1,3,4 senden, 2,5,6 senden nicht



5.3 Protokolle mit wahlfreiem Zugriff

- Wenn ein Knoten einen Rahmen senden möchte
  - Senden mit voller Datenrate des Kanals
  - Keine vorherige Koordination zwischen Knoten
- Wenn mehrere Knoten gleichzeitig übertragen: Kollision
- **Protokolle mit wahlfreiem Zugriff** legen fest:
  - Wie Kollisionen erkannt werden
  - Wie Kollisionen behandelt werden (z.B. durch eine verzögerte Neuübertragung)
- Beispiele für Protokolle mit wahlfreiem Zugriff:
  - Slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

5.3 Slotted ALOHA

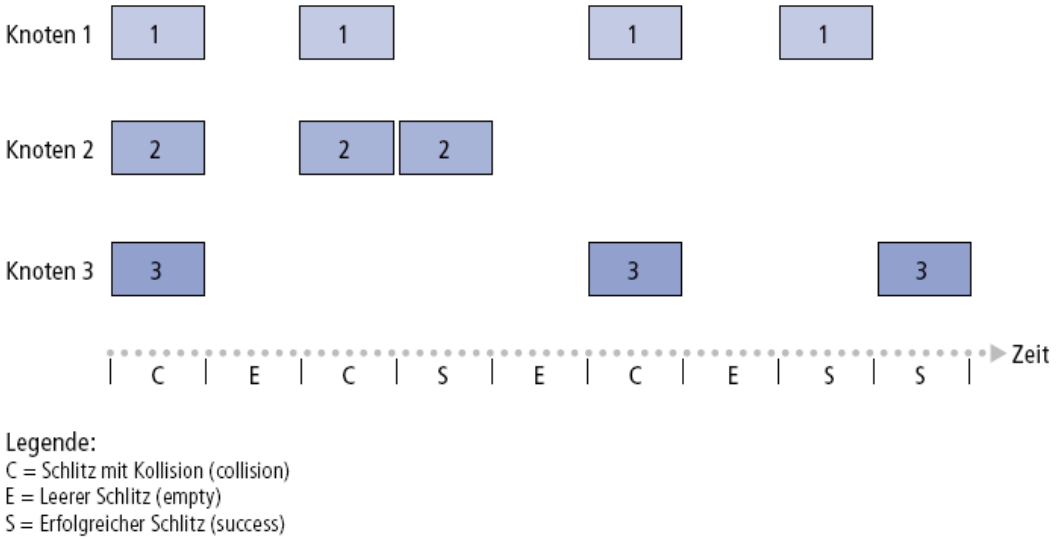
Annahmen:

- Alle Rahmen haben die gleiche Größe
- Zeitschlitze konstanter Größe, ausreichend für einen Rahmen
- Systeme starten ihre Übertragung nur zu Beginn eines Zeitschlitzes
- Systeme sind synchronisiert (sie kennen den globalen „Takt“ der Zeitschlitze)
- Wenn zwei oder mehr Systeme im gleichen Zeitschlitz senden, erkennen alle eine Kollision

Vorgehen:

- Wenn ein System Daten hat, überträgt es diese im nächsten Zeitschlitz
- Keine Kollision: Nächsten Rahmen im nächsten Zeitschlitz senden
- Kollision: Übertragung mit Wahrscheinlichkeit p im nächsten Zeitschlitz, bis Übertragung erfolgreich ist

5.3 Slotted ALOHA



Legende:
C = Schlitz mit Kollision (collision)
E = Leerer Schlitz (empty)
S = Erfolgreicher Schlitz (success)

Vorteile

- Einzelnes System kann die volle Bandbreite des Mediums nutzen
- Dezentral
- Einfach

Nachteile

- Synchronisation der Zeitschlitze notwendig
- Kollisionen verschwenden Bandbreite
- Leere Zeitschlitze
- Systeme können Kollisionen in kürzerer Zeit als die Dauer eines Zeitschlitzes erkennen

5.3 Effizienz von Slotted ALOHA

Effizienz: Durchschnittlich erzielte Datenrate, wenn viele Systeme viele Rahmen senden wollen, dividiert durch die Rate **R** des Mediums.

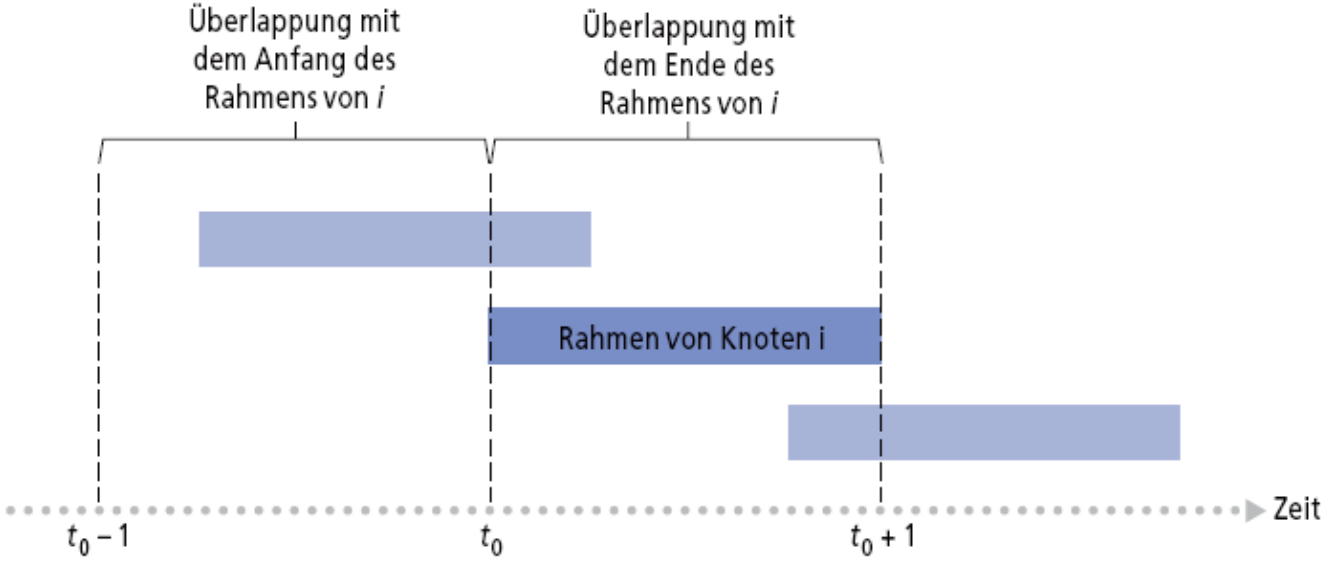
- Annahme: N sendewillige Systeme, jedes überträgt in einem Zeitschlitz mit Wahrscheinlichkeit p
- Wahrscheinlichkeit, dass das erste System Erfolg hat: $p(1-p)^{N-1}$
- Wahrscheinlichkeit, dass ein beliebiges System Erfolg hat: $Np(1-p)^{N-1}$
- Für eine optimale Auslastung finde p*, welches diesen Ausdruck maximiert
- Berechne dann den Grenzwert des Ausdrucks, wenn N gegen unendlich geht (siehe auch http://tinyurl.com/cm6ny4z)

→ **p* = 1/N**

→ **Maximale Effizienz: 1/e*R ~ 0.37*R**

5.3 Reines ALOHA

- Einfacher, keine Synchronisation notwendig
- Wenn neue Daten zum Senden ankommen:
  - Direkt übertragen
- Wahrscheinlichkeit für Kollisionen erhöht sich:
  - Ein zum Zeitpunkt t_0 gesendeter Rahmen kollidiert mit anderen Rahmen, die im Bereich $[t_0-1,t_0+1]$ gesendet wurden



5.3 Effizienz von reinem ALOHA

P(erfolgreiche Übertragung) = P(System überträgt) *
P(kein anderes System überträgt in $[p_0-1,p_0]$) *
P(kein anderes System überträgt in $[p_0,p_0+1]$)

$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$
$= p \cdot (1-p)^{2(N-1)}$

Wähle optimales p* und lasse N gegen unendlich gehen ...

- **p* = 1 / (2*N-1)**
- **Maximale Effizienz: 1/2e*R ~ 0.18*R → Halb so effizient wie Slotted ALOHA!**

5.3 CSMA

Carrier Sense Multiple Access (CSMA)

Zuhören vor dem Übertragen:

- Wenn der Kanal als leer erkannt wird → Übertrage den Rahmen
- Wenn der Kanal als besetzt erkannt wird → Übertragung verschieben

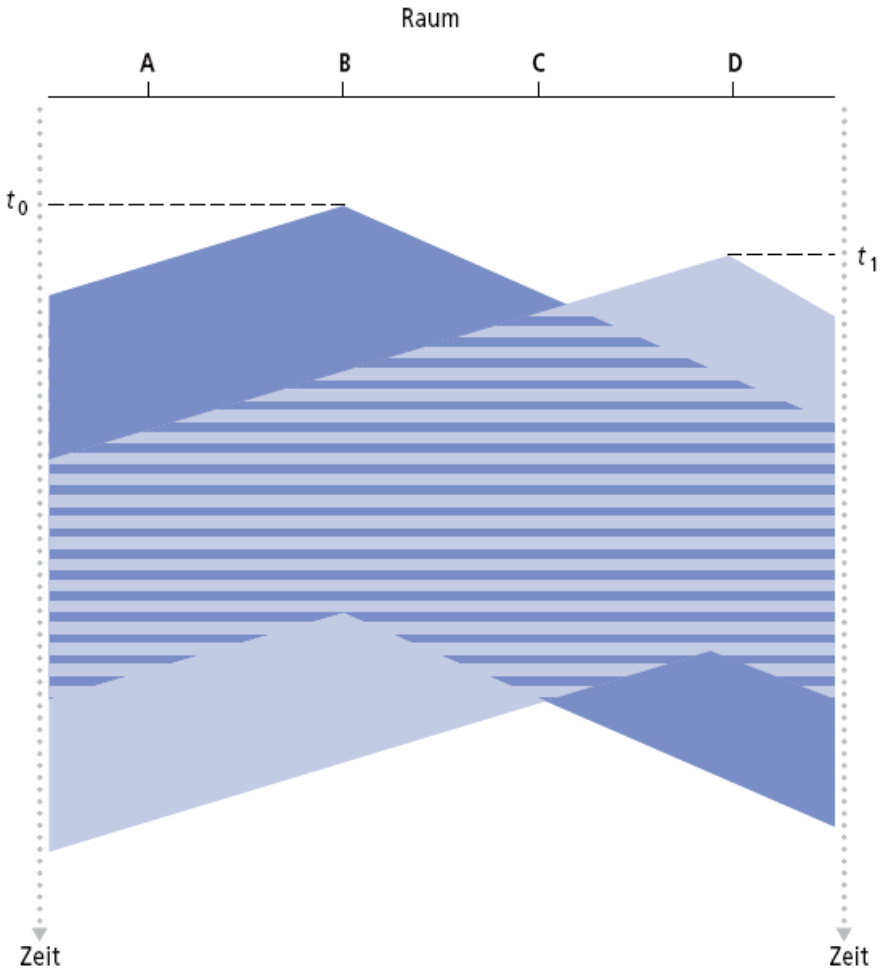
Analogie: *Nicht dazwischenreden, wenn jemand anderes gerade etwas sagt!*

5.3 CSMA - Kollisionen

- Kollisionen können immer noch auftreten:

  Die Ausbreitungsverzögerung kann dazu führen, dass man die Übertragung eines anderen Knotens nicht rechtzeitig erkennt!

- Kollision:
  - Dauert die ganze Übertragungszeit
    → Zeit wird verschwendet



5.3 CSMA/CD

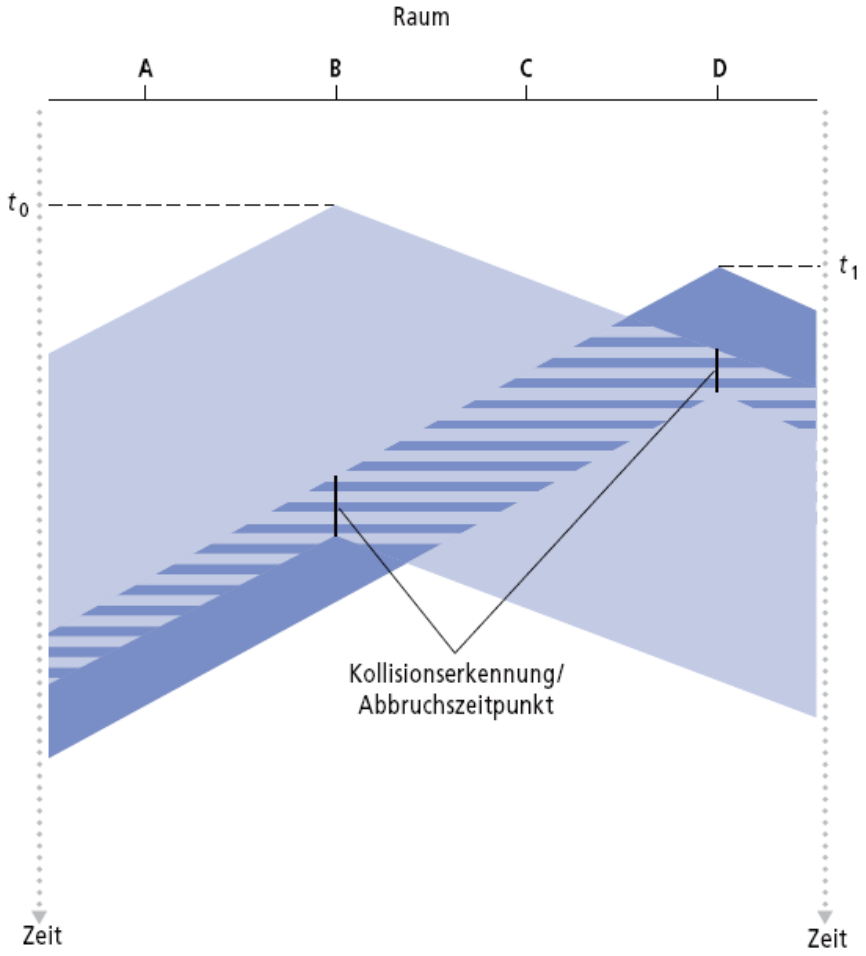
CSMA/CD (Collision Detection): Carrier Sensing wie in CSMA

- Kollisionen werden schnell erkannt
- Übertragungen, die kollidieren, werden abgebrochen

- Kollisionserkennung:
  - Einfach in drahtgebundenen LANs: Messe die empfangene Signalstärke und vergleiche sie mit der gesendeten Signalstärke
  - Schwierig in drahtlosen LANs: Die empfangene Signalstärke wird von der eigenen Übertragung dominiert

- Analogie: *der höfliche Diskussionsteilnehmer*

5.3 CSMA/CD


Raum
A
B
C
D
t_0
t_1
Kollisionserkennung/
Abbruchszeitpunkt
Zeit
Zeit

5.3 Ethernet verwendet CSMA/CD

1. Ethernet Netzwerkkarte empfängt ein Datagramm von der Vermittlungsschicht und erstellt einen Rahmen
2. Die Netzwerkkarte überprüft ob die Leitung belegt ist:
   - Frei: NIC startet die Rahmen-Übertragung.
   - Belegt: NIC wartet bis die Leitung wieder frei ist und sendet dann.
3. Während der Übertragung wird die Leitung weiter überprüft:
   - Wenn der Rahmen ohne Kollision übertragen wurde: Ende
   - Kollision: Übertragung wird abgebrochen und ein Jam-Signal gesendet. Weiter mit Schritt 4.
4. Danach wird „Exponential Backoff“ durchgeführt: Nach der **m**-ten Kollision zieht die Netzwerkkarte eine Zufallszahl K aus dem Bereich $\{0,1,2,...,2^{m}-1\}$.
5. Die Netzwerkkarte wartet K*512 Bit-Zeiten (= Dauer der Übertragung eines Bits) und geht dann zu Schritt 2 zurück.

5.3 CSMA/CD und Ethernet

- Jam-Signal:
  - Sicherstellen, dass alle Sender die Kollision erkennen
  - 48 Bit lang
- Bit-Zeit:
  - 0,1 Mikrosekunden bei 10 MBit/s Ethernet
- Exponential Backoff:
  - Ziel: Frequenz der Übertragungswiederholung der aktuellen Lastsituation anpassen
  - Bei hoher Last werden mehrere Kollisionen in Folge passieren, bis das richtige Intervall für die Zufallszahl gefunden ist
  - Bei der ersten Kollision: wähle K aus {0,1}
  - Bei der zweiten Kollision: wähle K aus {0,1,2,3}…
  - Bei der zehnten Kollision: wähle K aus {0,1,2,3,4,…,1023}

5.3 Effizienz von CSMA/CD

- Hängt von der Signallaufzeit t_{prop} zwischen konkurrierenden Stationen ab
  - Wenn diese gegen 0 geht, dann geht auch die Wahrscheinlichkeit für eine Kollision gegen 0 und somit die Effizienz gegen 1.
  - Wenn die Signallaufzeit groß wird, dann steigt das Risiko einer Kollision und die Effizienz sinkt.
- Hängt von $t_{übertragung}$ (der durchschnittlichen Zeit zur Übertragung eines Rahmens) und damit von der Rahmengröße ab.
  - Geht diese gegen unendlich, dann geht die Effizienz gegen 1.
- Bei Existenz vieler sendewilliger Stationen gilt:
  - Effizienz $\approx 1/(1+5t_{ausbreitung}/t_{übertragung})$
- Herleitung dazu in: S. Lam, *A Carrier Sense Multiple Access Protocol for Local Networks*, Computer Networks, Vol. 4, pp. 21-32, 1980.

5.3 CSMA/CD

MAC-Protokolle mit Aufteilung des Mediums:

- Teilen den Kanal effizient und fair auf, wenn die Last konstant verteilt ist
- Ineffizient bei dynamischer Verteilung der Last. Wenn die Partitionierung gleichmäßig erfolgt, aber nur einer von N Sendern tatsächlich aktiv ist, dann wird nur ein Anteil von 1/N der Bandbreite verwendet!

MAC-Protokolle für den wahlfreien Zugriff

- Effizient, wenn die Auslastung des Netzwerkes gering ist
- Bei hoher Last: Kollisionen

Protokolle mit abwechselndem Zugriff

- Versuchen, beide Vorteile zu vereinen!

5.3 Abwechselnder Zugriff: Polling

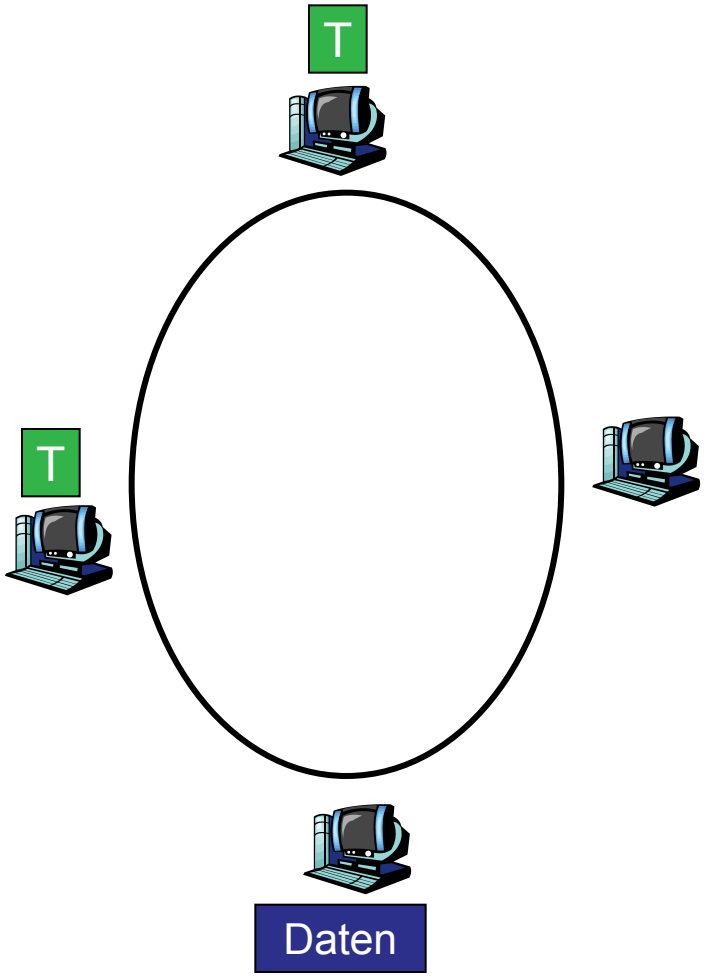
- Eine speziell ausgezeichnete Station ist der **Master**
- Der Master teilt das Medium explizit den sendewilligen Stationen zu

- Vorteile:
  - \+ Aufteilung der Bandbreite erfolgt bedarfsorientiert
  - \+ Keine Verschwendung von Bandbreite durch Kollisionen
- Nachteile:
  - – Aufwand durch Polling
  - – Zentralisiertes Verfahren
    - → Wenn der Master ausfällt, dann funktioniert das Netz nicht mehr
    - → Master als zusätzliche Hardware/Software notwendig

5.3 Abwechselnder Zugriff: Token Passing

- Das **Token** ist ein spezieller Rahmen
- Er wird von Station zu Station weitergereicht
- Nur wer das Token besitzt, darf senden
- Ausprägungen: Token-Ring, Token-Bus

- Vorteile:
  - Aufteilung der Bandbreite erfolgt bedarfsorientiert
  - Keine Verschwendung von Bandbreite durch Kollisionen
  - Verteiltes Verfahren
- Nachteil:
  - Komplexität:
    - Verlust des Tokens
    - Verdoppeltes Token



5.3 Zusammenfassung MAC-Protokolle

- **Aufteilung des Kanals** anhand von Zeit, Frequenz (oder Code)
  - TDMA, FDMA
- **Wahlfreier Zugriff**
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - Carrier Sensing: einfach für manche Medien (drahtgebunden), schwierig für andere Medien (drahtlos)
  - CSMA/CD von Ethernet verwendet
  - CSMA/CA (Collision Avoidance) in IEEE 802.11 WLAN
- **Abwechselnder Zugriff**
  - Polling, Token Passing

5.3 LAN-Technologien

Sicherungsschicht – bisher schon besprochen:

- Angebotene Dienste, Fehlererkennung/-korrektur, Mehrfachzugriff

Als Nächstes: LAN-Technologien

- Adressierung
- Ethernet
- Switches
- PPP

5.4 Adressierung auf der Sicherungsschicht

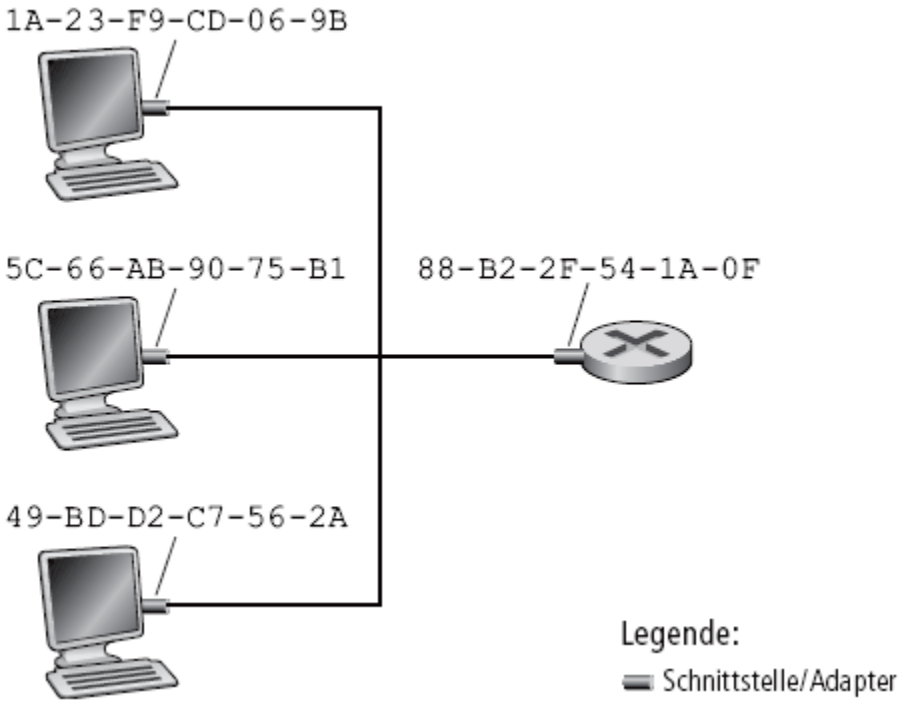
5.4 MAC-Adressen und ARP

- 32-Bit-IP-Adresse:
  - Adresse auf der Netzwerkschicht
  - Wird verwendet, um ein Datagramm zum Zielnetzwerk zu leiten
  - Beinhaltet Ortsinformationen: Wo befindet sich das Zielnetzwerk?

- 48-Bit-MAC-Adresse:
  - Aufgabe: *Wird verwendet, um einen Rahmen von einem Adapter zu einem benachbarten Adapter weiterzuleiten (im selben Netzwerk!)*
  - Keine Ortsinformationen, muss nur im gegebenen Netzwerk eindeutig sein
  - In das ROM der Netzwerkkarte eingebrannt, aber auch durch Software veränderbar (*MAC Address Spoofing*)

5.4 MAC-Adressen und ARP

Jeder Adapter im LAN hat eine eindeutige MAC-Adresse.



Broadcast-Adresse =
FF-FF-FF-FF-FF-FF

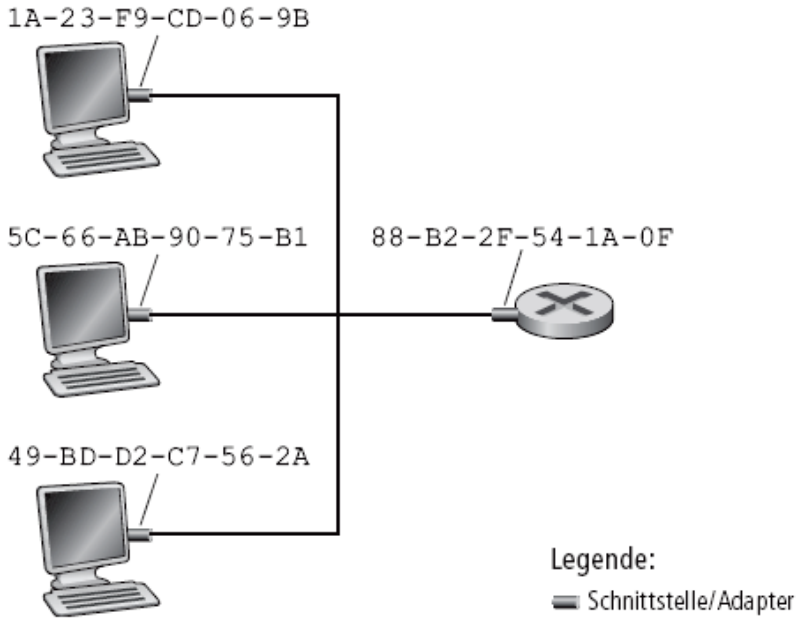
5.4 MAC-Adressen und ARP

- Die Zuordnung von MAC-Adressen wird von der IEEE überwacht
- Hersteller kaufen einen Teil des Adressraums (um die Eindeutigkeit der Adressen sicherzustellen)
- Analogie:
  (a) MAC-Adresse: Sozialversicherungsnummer
  (b) IP-Adresse: Postanschrift
- MAC: flacher Adressraum → Portabilität
  - Eine Netzwerkkarte kann problemlos von einem LAN in ein anderes LAN bewegt werden
- IP: hierarchischer Adressraum → keine Portabilität
  - Adresse hängt vom Subnetz ab, kann im Standardfall nicht in einem anderen LAN verwendet werden

5.4 ARP: Address Resolution Protocol

Problem: Wie erfahre ich die MAC-Adresse von B, wenn ich die IP-Adresse von B kenne?

- Dazu wird das Address Resolution Protocol (ARP) verwendet
- Jedes System in einem LAN hat einen ARP-Cache, in dem die Zuordnung von IP- zu MAC-Adressen gespeichert ist
- Jeder Eintrag ist mit einer Lebenszeit versehen, nach Ablauf der Lebenszeit wird der Eintrag gelöscht (typische Lebenszeit: 20 Minuten)
- Ansehen + Manipulieren des ARP-Caches mit dem Kommando *arp*



5.4 ARP - Funktionsweise

1. A möchte ein Datagramm an B schicken, die MAC-Adresse von B ist nicht im ARP-Cache von A

2. A schickt eine ARP-Query als Broadcast-Rahmen, die Query enthält die IP-Adresse von B
   - Empfänger-MAC-Adresse = FF-FF-FF-FF-FF-FF
   - Alle Systeme im LAN erhalten diese Anfrage

3. B empfängt die ARP-Query, erkennt seine IP-Adresse und antwortet A mit seiner eigenen MAC-Adresse
   - Empfänger-MAC-Adresse = MAC-Adresse von A

4. A trägt die Abbildung der IP-Adresse von B auf die MAC-Adresse von B im ARP Cache ein
   - Soft State: Informationen, die gelöscht werden, wenn sie nicht innerhalb einer gewissen Zeit aufgefrischt werden

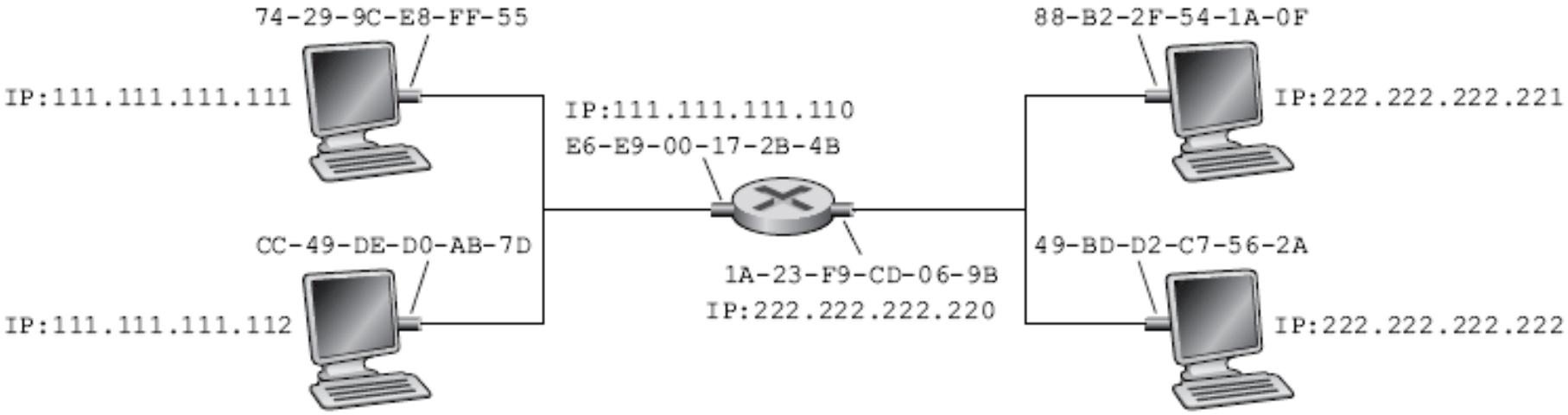
5. A schickt den Datagramm-Rahmen, der die IP- und die MAC-Adresse von B enthält

→ ARP ist “Plug-and-Play”: Keine manuelle Konfiguration notwendig!

5.4 ARP - Routing zwischen zwei LANs

Szenario:

Wir senden ein Datagramm von 111.111.111.111 zu 222.222.222.222 über den Router R:



Zwei ARP-Tabellen in R, eine für jedes LAN.

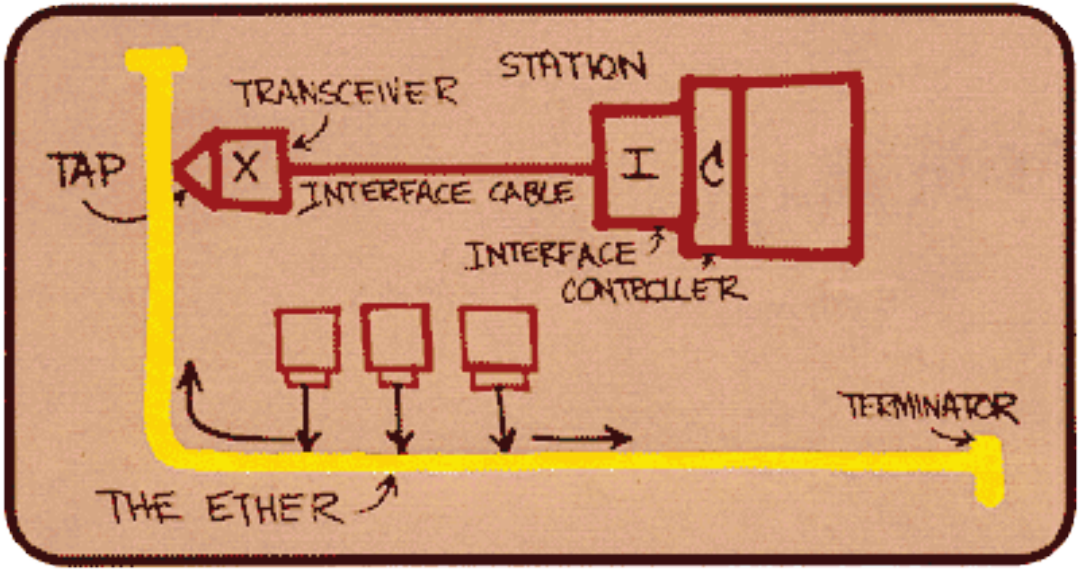
5.4 ARP - Routing zwischen zwei LANs (Bild auf Folie Nr. 41)

1. 111.111.111.111 erstellt ein IP-Datagramm mit dem Ziel 222.222.222.222
2. 111.111.111.111 schlägt in seiner IP-Weiterleitungstabelle nach und stellt fest, dass dieses Paket über R (111.111.111.110) weitergeleitet werden muss
3. 111.111.111.111 verwendet ARP, um die MAC-Adresse von 111.111.111.110 zu bestimmen
4. 111.111.111.111 erstellt einen Rahmen der Sicherungsschicht mit E6-E9-00-17-2B-4B als Zieladresse
   → Dieser Rahmen enthält das IP-Datagramm von 111.111.111.111 an 222.222.222.222
5. Die Netzwerkkarte von 111.111.111.111 sendet den Rahmen
6. Die Netzwerkkarte von 111.111.111.110 empfängt den Rahmen
7. R packt das IP-Datagramm aus und stellt fest, dass es für 222.222.222.222 bestimmt ist
8. Über die IP-Weiterleitungstabelle stellt R fest, dass er das Datagramm direkt an 222.222.222.222 ausliefern kann
9. R verwendet ARP, um die MAC-Adresse von 222.222.222.222 zu erfahren
10. R erstellt einen Rahmen, der das Datagramm von 111.111.111.111 an 222.222.222.222 enthält, und sendet es an die so ermittelte MAC-Adresse

5.5 Ethernet

5.5 Ethernet

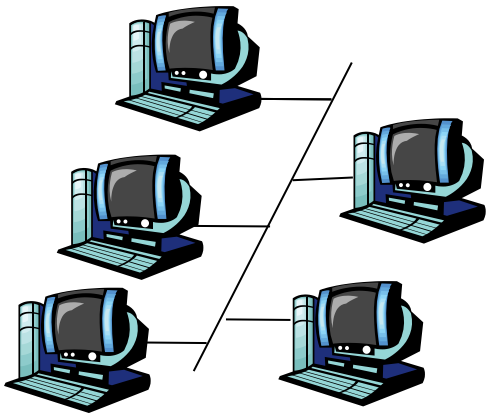
- Marktbeherrschende LAN-Technologie auf CSMA/CD-Basis:
- Sehr günstige Preise
- Erste weitverbreitete LAN-Technologie
- Einfacher und billiger als Verfahren mit koordiniertem Kanalzugriff
- Datenrate hat sich über die Zeit stark erhöht: 10, 100, 1000, 10000 MBit/s



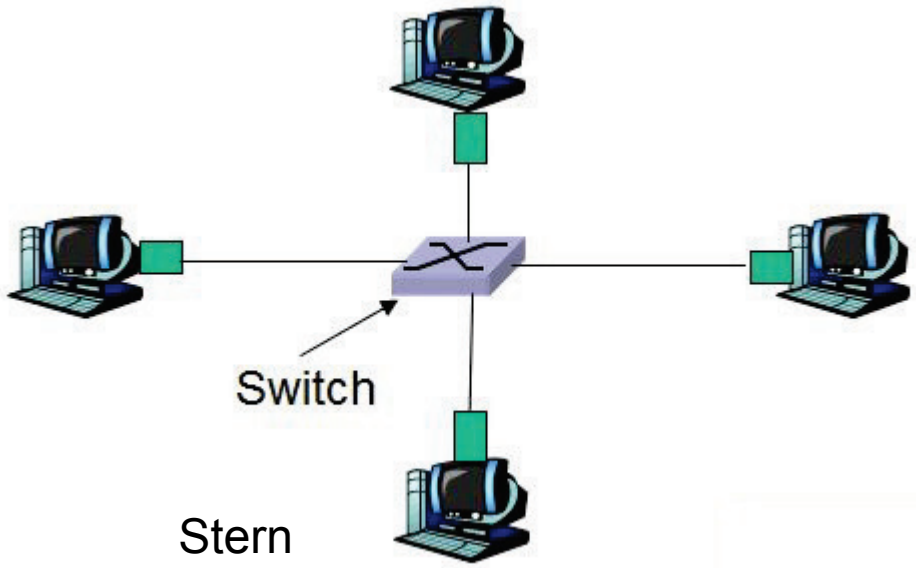
Metcalfes Ethernet-Entwurf

5.5 Ethernet-Topologie

- Bus-Topologie bis in die Mitte der 90er Jahre
  - Alle Knoten in einer Kollisionsdomäne (die Übertragung eines Knotens konnte mit der Übertragung jedes anderen Knotens kollidieren)
- Heutzutage: Stern-Topologie
  - Aktiver Switch im Zentrum
  - Endsysteme sind an den Switch angeschlossen, ihre Übertragungen kollidieren nicht mehr miteinander



Bus: Koaxialkabel



Stern

5.5 Ethernet-Rahmenstruktur

- Sendende Netzwerkkarte verpackt die Nutzdaten in einen Ethernet-Rahmen:

- Präambel:
  - 7 Bytes mit 10101010, gefolgt von einem Byte mit 10101011
  - Verwendet zur Synchronisation von Sender und Empfänger
- Rahmenende:
  - Erkannt durch eine Ruheperiode in der Dauer der Serialisierungszeit von 96 Bits

5.5 Ethernet-Rahmenstruktur

- Adressen: 6 Bytes
  - Wenn eine Host-Netzwerkkarte einen Rahmen mit der eigenen Adresse oder der sogenannten Broadcast-Adresse (= FF:FF:FF:FF:FF:FF) empfängt, dann werden die Daten an die nächsthöhere Schicht weitergegeben
  - Sonst wird der Rahmen verworfen
- Typ: beschreibt, welcher Art die im Rahmen enthaltenen Daten sind
  - Werte ab 0x0600 sind zulässig
  - Werte unter 0x0600 signalisieren einen IEEE 802.x-Rahmen
  - Beispiel 0x0800 = IP-Paket
- CRC: Überprüfen auf Bitfehler, bei Erkennen eines Fehlers wird der Rahmen einfach verworfen

5.5 Dienst von Ethernet

- Ethernet stellt einen unzuverlässigen und verbindungslosen Dienst zum Austausch von Daten zwischen Stationen in einem LAN zur Verfügung. Ethernet verwendet als MAC Protokoll CSMA/CD mit Binary Backoff.

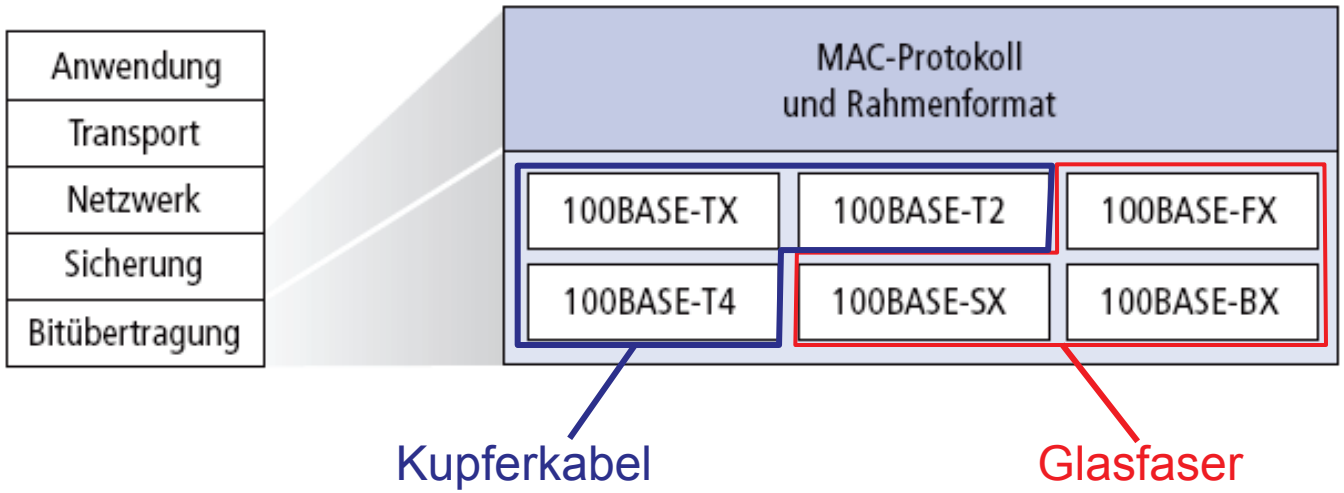
- **Verbindungslos:** kein Verbindungsauf- und -abbau zwischen Sender und Empfänger

- **Unzuverlässig:** Wenn Übertragungsfehler (z.B. Bitfehler) vorkommen, werden die Rahmen einfach verworfen, es erfolgt keine Übertragungswiederholung
  - Achtung: Kollisionen werden von Ethernet per Collision Detection erkannt und durch Übertragungswiederholung behoben!
  - Andere Rahmenverluste müssen auf höheren Schichten behoben werden oder der Inhalt des Rahmens geht verloren.

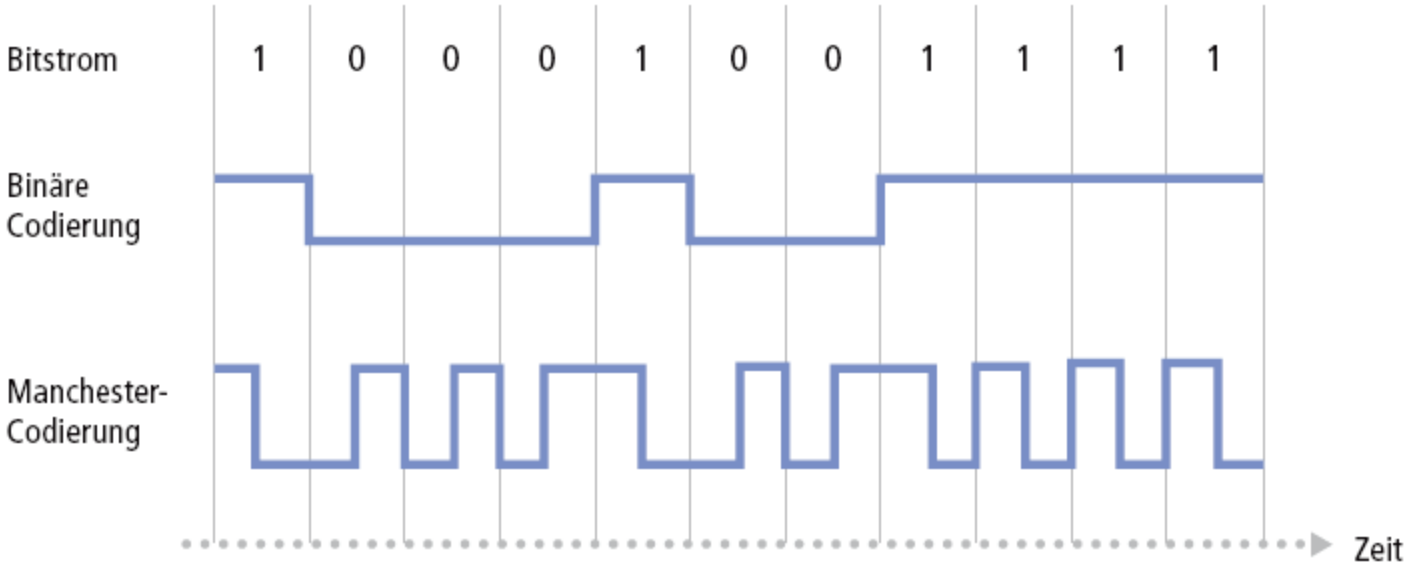
5.5 Ethernet-Standards

802.3-Ethernet-Standards: Sicherungs- und Bitübertragungsschicht

- **Viele** verschiedene Ethernet-Standards
  - Gemeinsames MAC-Protokoll und Rahmenformat
  - Verschiedene Geschwindigkeiten: 2 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps
  - Verschiedene Medien auf der Bitübertragungsschicht: Glasfaser und Kupferkabel



5.5 Manchester-Codierung



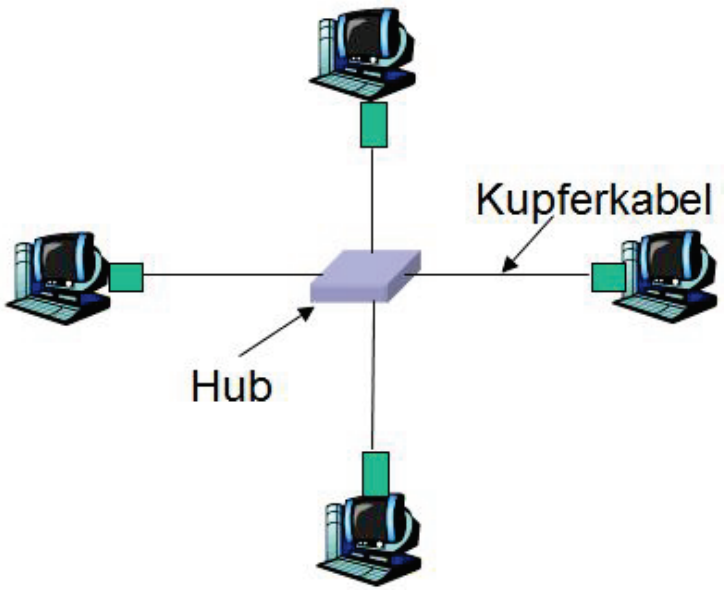
- Verwendet in 10BaseT (10Mbps, Twisted-Pair)
- Jedes Bit hat eine Transition
- Ermöglicht die Synchronisation von Uhren zwischen Sender und Empfänger
  - Es wird keine globale, gemeinsame Uhrzeit benötigt!
- Gehört zur Bitübertragungsschicht!

5.6 Switches auf der Sicherungsschicht

5.6 Hubs

… gehören zur Bitübertragungsschicht:

- Bits, die auf einem Link ankommen, werden auf alle anderen Links mit der Eingangsrate kopiert
- Die Übertragung aller über einen Hub verbundenen Knoten kann miteinander kollidieren
- Ein Hub puffert keine Rahmen
- Kein CSMA/CD im Hub: Die Netzwerkkarten der Hosts führen CSMA/CD aus (und erkennen Kollisionen)



5.6 Switch

- Ein Switch arbeitet auf der Sicherungsschicht:
  - Empfängt Ethernet-Rahmen, puffert sie und leitet sie weiter
  - Untersucht den Header eines Rahmen und leitet ihn gezielt anhand der Empfängeradresse auf eine Ausgangsleitung weiter

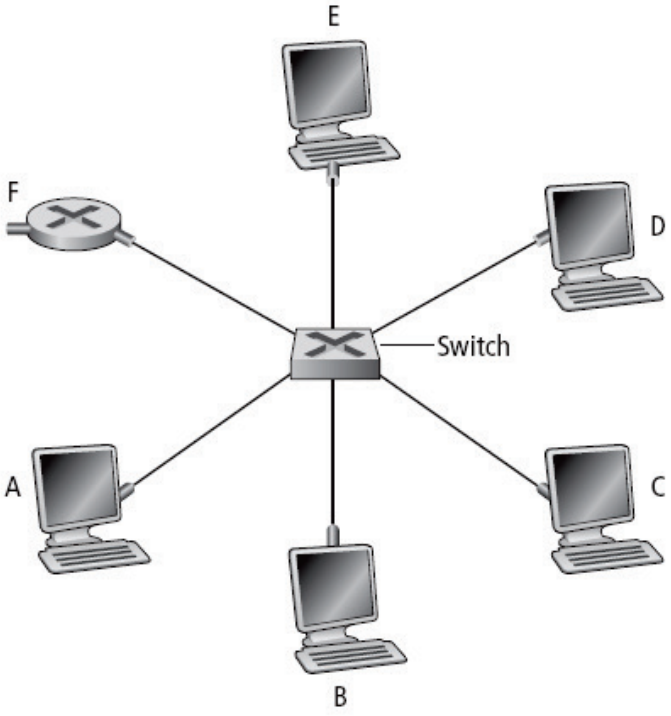
- Transparent
  - Endsysteme wissen nichts über die Gegenwart eines Switches

- Plug-and-Play, selbst lernend
  - Switches müssen nicht konfiguriert werden

5.6 Switch

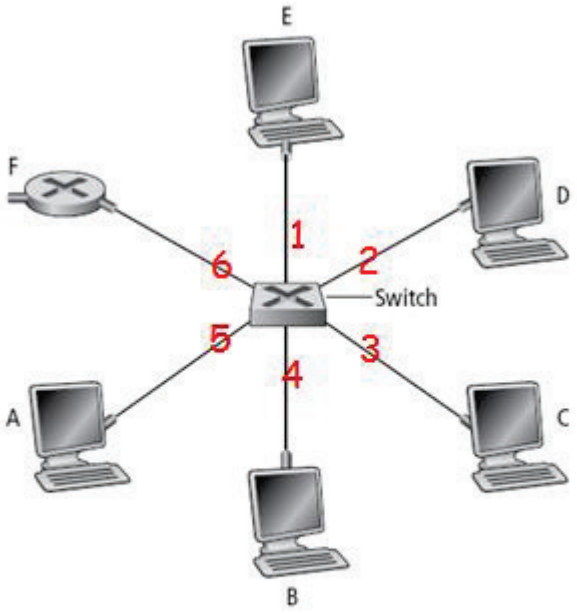
Ein Switch ermöglicht mehrere gleichzeitige Übertragungen:

- Jeder Host hat einen eigenen Link zum Switch
- Ein Switch puffert Rahmen
- Das Ethernet-Protokoll wird auf jedem Link verwendet, es kann jedoch keine Kollisionen geben; Vollduplex
  - Jeder Link ist eine eigene Kollisionsdomäne
- **Switching:** E-nach-B und D-nach-A gleichzeitig ohne Kollisionen möglich
  → Geht nicht mit einem Hub !



5.6 Switch-Tabelle

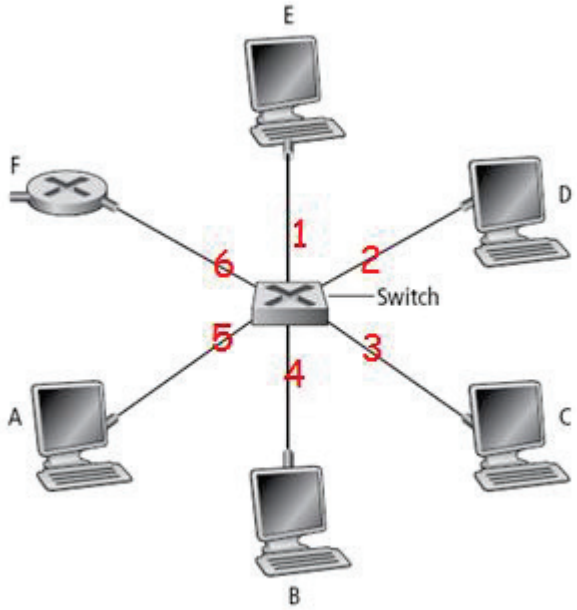
- Woher weiß der Switch, dass B über Interface 4 zu erreichen ist?
- Jeder Switch besitzt eine Switch-Tabelle mit folgenden Einträgen:
  - (MAC-Adresse eines Hosts, Schnittstelle, über die der Host erreicht werden kann, Zeitstempel)
- Ähnlich wie eine Routing-Tabelle!
- Wie kommen die Einträge in die Switch-Tabelle?
  - Routing-Protokolle auf der Sicherungsschicht???



Switch mit sechs Schnittstellen (1,2,3,4,5,6)

5.6 Switch – selbst lernend

- Ein Switch lernt, welche Hosts er über eine gegebene Schnittstelle erreichen kann:
  - Wenn er einen Rahmen empfängt, dann lernt der Switch, dass der Absender hinter dieser Schnittstelle liegen muss
  - Er trägt diese Information in die Switch-Tabelle ein
- *Beispiel*: A schickt einen Rahmen an D



Switch-Tabelle

MAC-Adr.	Schnitt.	TTL
A	5	60

5.6 Switch – Weiterleiten/Filtern

Wenn ein Switch einen Rahmen erhält:

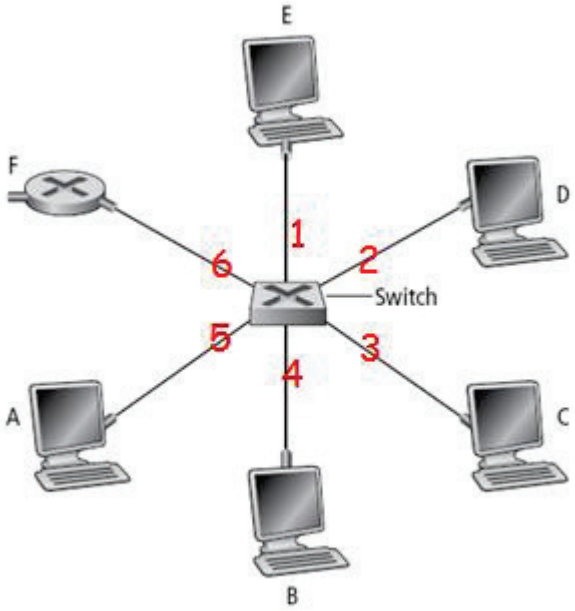
Suche die MAC-Empfängeradresse in der Switch-Tabelle.

```
if Eintrag gefunden
   then {
      if Ausgangs- und Eingangsinterface identisch
           then Rahmen verwerfen
             else Rahmen auf Ausgangsinterface weiterleiten
        }
     else Fluten
```

Auf alle Interfaces weiterleiten, außer dem Eingangsinterface

5.6 Switch – Beispiel

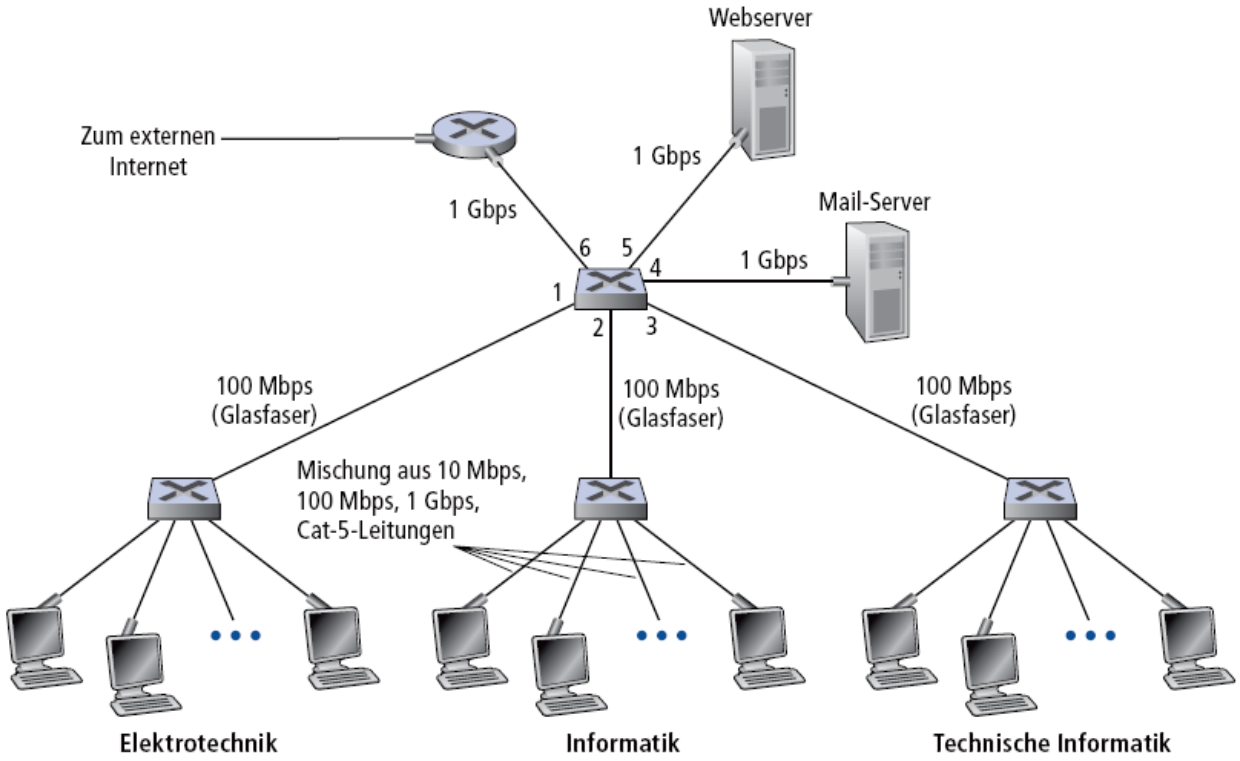
- A sendet einen Rahmen an D
- Der Switch merkt sich, dass A hinter der Schnittstelle 5 liegt
- Der Switch flutet den Rahmen über alle anderen Schnittstellen
- D antwortet mit einem Rahmen an A
- Der Switch merkt sich, dass D hinter der Schnittstelle 2 liegt
- Er leitet den Rahmen gemäß seiner Tabelle über die Schnittstelle 5 weiter zu A



Switch-Tabelle

MAC-Adr.	Schnitt.	TTL
A	5	60
D	2	60

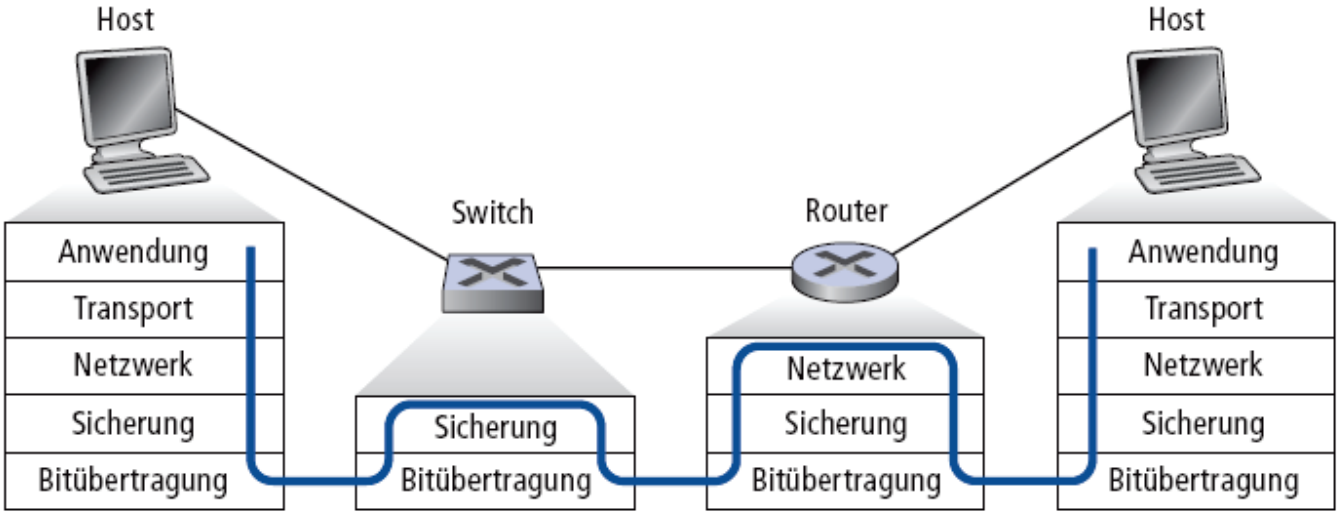
5.6 Switches in einer komplexeren Umgebung



- Wie füllen die Switches in einer solchen Umgebung ihre Tabellen?
- Selbst lernend, genau wie bereits besprochen!

5.6 Vergleich Switch und Router

- Beide speichern Pakete/Rahmen und leiten diese weiter
  - Router: auf der Netzwerkebene (verwendet IP-Adressen)
  - Switch: gehört zur Sicherungsschicht (verwendet MAC-Adressen)
- Router verwaltet eine Weiterleitungstabelle und führt Routing-Algorithmen aus
- Switch verwaltet eine Switch-Tabelle und ist selbst lernend



5.6 Zusammenfassender Vergleich

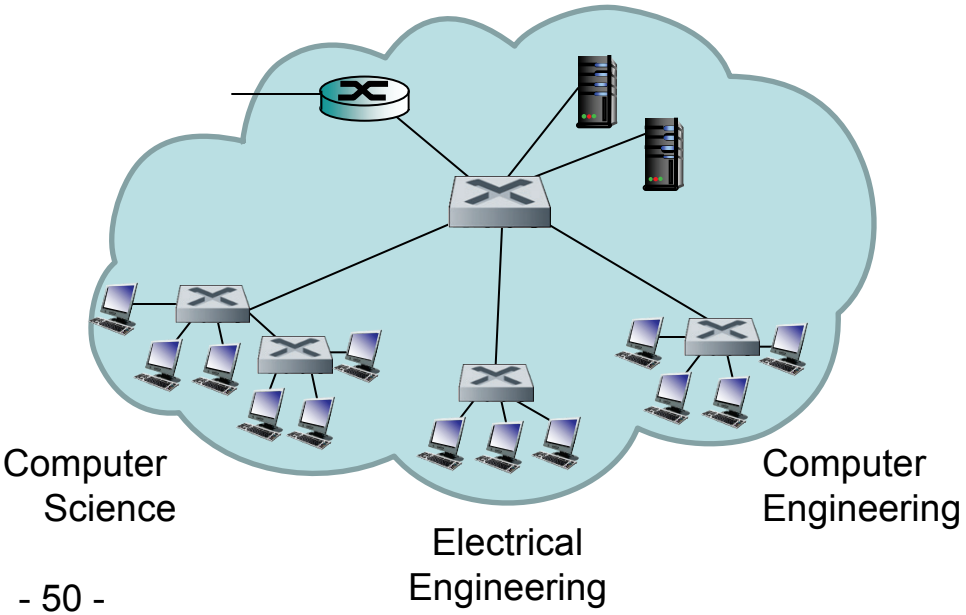
	Hubs	Router	Switches
Isolierung von Verkehr	nein	ja	ja
Plug-and-Play	ja	nein	ja
Optimales Routing	nein	ja	nein

- **Wichtig:**
  - Switching ist nicht als alleiniges Mittel für sehr große Netze gedacht, und insbesondere nicht als Inter-AS-Netzwerkarchitektur!
  - Gründe:
    - „Selbstlernen“ der Switching-Tabellen und Sicherungsschicht-Broadcasts können nicht in beliebig großen Netzen funktionieren
    - Hardware-MAC-Adressen kann man nicht aggregieren, so dass man keine vernünftig kleinen Switching-Tabellen zustande bekommen könnte

5.6 VLAN – Motivation

Probleme bei herkömmlichen LANs:

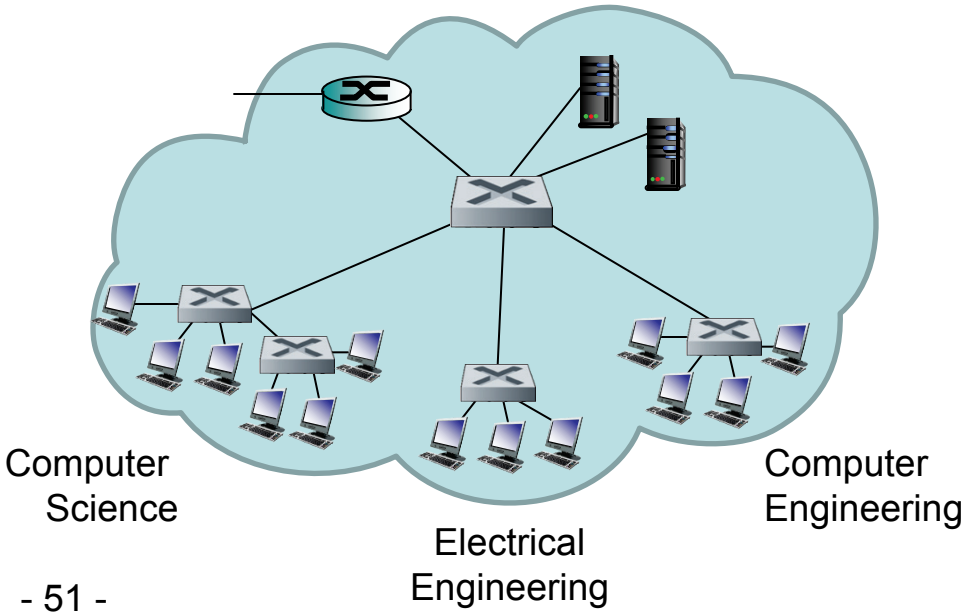
1. Datenströme werden zu wenig isoliert
   - Pakete, die per Broadcast verteilt werden müssen das gesamte Unernehmensnetzwerk durchwandern. Würde der Empfangsbereich dieser Pakete eingeschränkt wäre das Netzwerk entlastet und die Datenströme wären in puncto Privacy/Datensicherheit weniger angreifbar (Packetsniffing!).



5.6 VLAN – Motivation

Probleme bei herkömmlichen LANs:

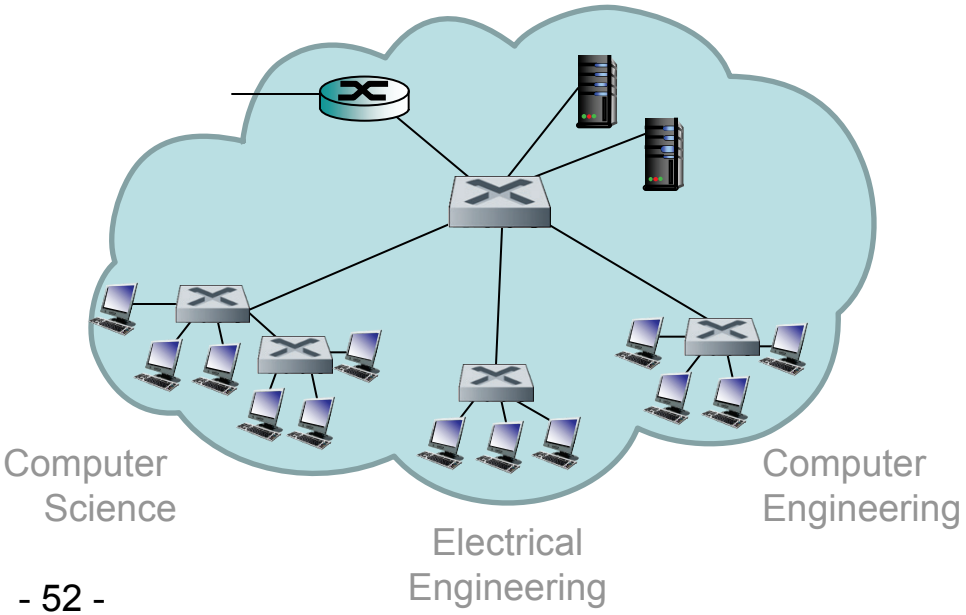
2. Switches werden ineffizient genutzt
   - Durch eine Hierarchie können Datenströme unterschiedlicher Gruppen in einem Unternehmen (z.B. Manager und Angestellte) in unterschiedlichen Switches isoliert werden. Um dies zu erreichen verwenden Unternehmen oft eine Vielzahl an Switches für einen Datenverkehr, der auch von einem einzigen Switch mit einer größeren Anzahl an Ports (z.B. 96-Port Switch) geregelt werden könnte.



5.6 VLAN – Motivation

Probleme bei herkömmlichen LANs:

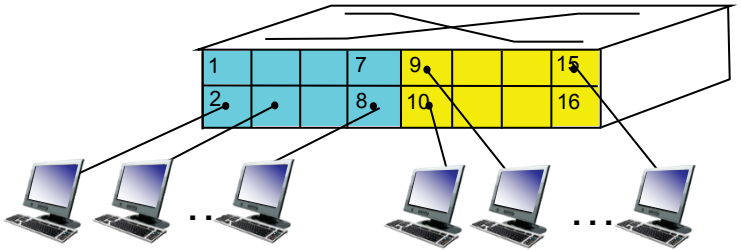
3. User-Verwaltung
   - Wenn ein Angestellter in einem Unternehmen in eine andere Gruppe wechselt, muss (durch die Trennung der Datenströme) die physische Verkabelung geändert werden um ihn mit dem neuen Switch zu verbinden. Wenn ein Angestellter gleichzeitig ein Mitglied von zwei oder mehr Gruppen ist wird das noch problematischer.



5.6 VLAN

- Ein Switch, der Virtual Local Area Networks (VLANs) unterstützt, kann **Datenverkehr im selben physischen Netzwerk** in mehrere unterschiedliche Datenströme gliedern und diese **als virtuelle lokale Netzwerke definieren**.
- Hosts innerhalb eines VLAN kommunizieren miteinander als ob nur sie (und keine anderen Hosts) mit diesem Switch verbunden wären.

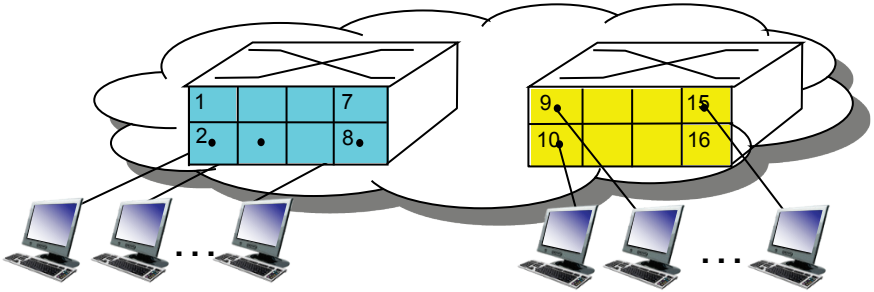
5.6 Port-basiertes VLAN



Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-15)

Die Switch Ports werden (von einer Switch Management Software) so gruppiert, dass ein einziger physischer Switch…



Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-16)

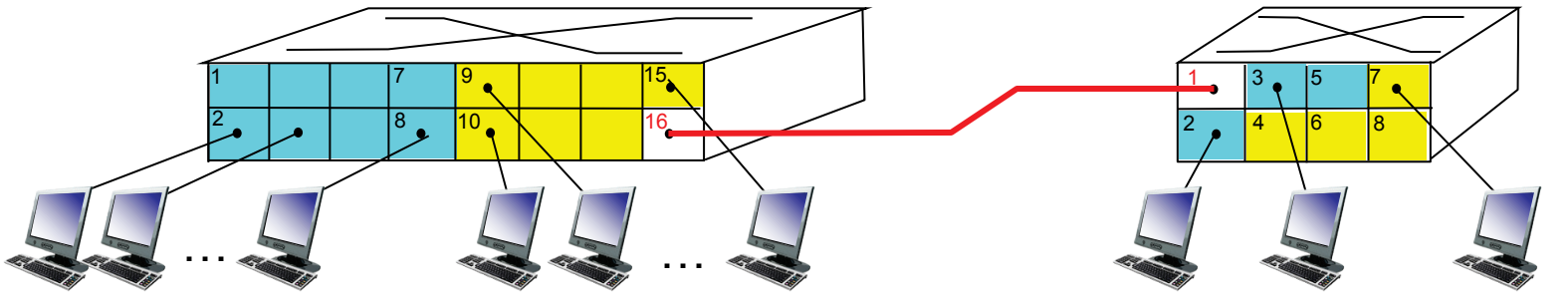
…als mehrere virtuelle Switches fungieren kann.

5.6 Port-basiertes VLAN

Ein Port-basiertes VLAN geht folgendermaßen auf die Probleme von LANs ein:

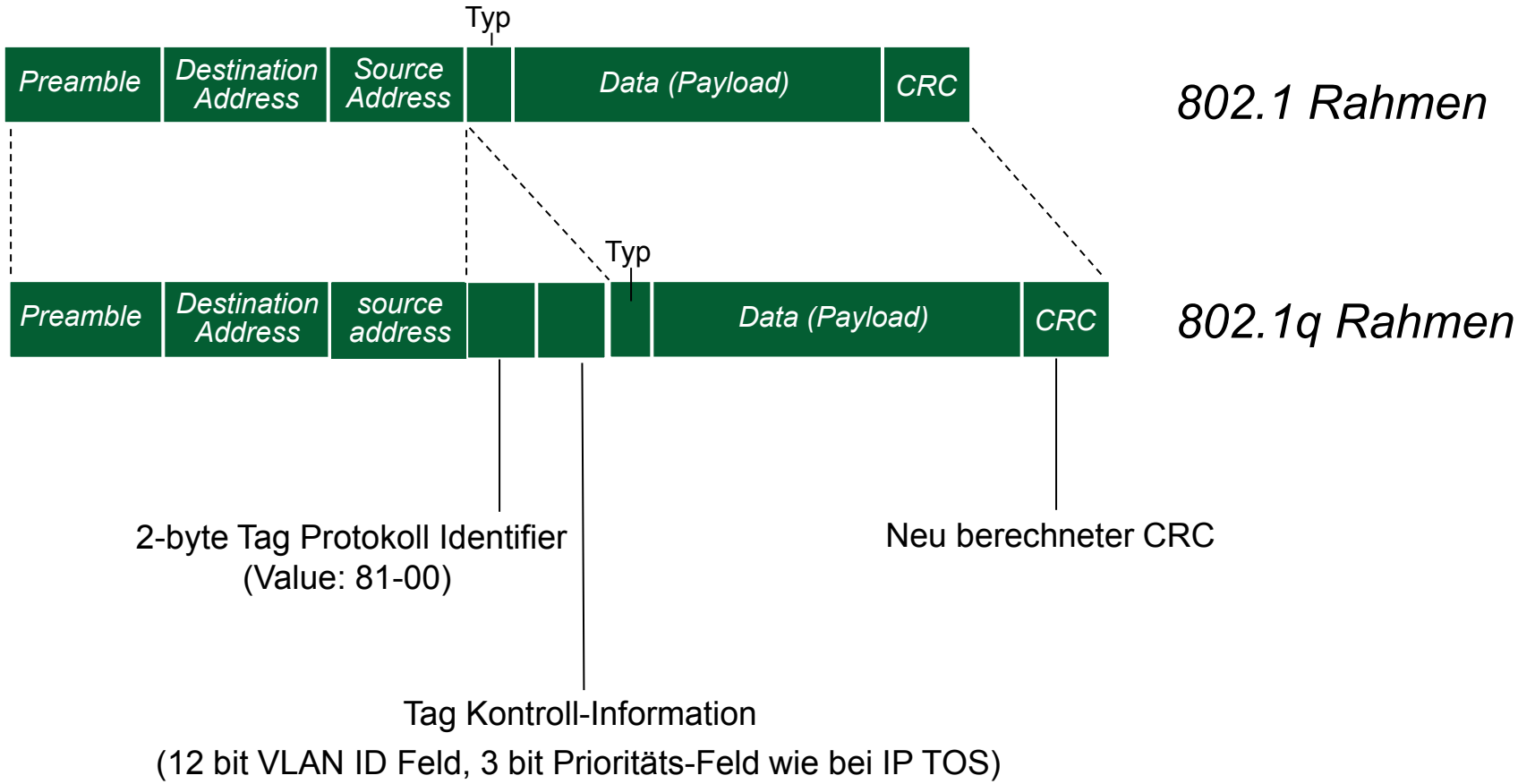
- *Datenströme werden zu wenig isoliert*: Rahmen zu/von den Ports 1-8 können auch nur die Ports 1-8 erreichen.
  - VLAN kann die Gruppenteilnehmer statt über den Switch Port auch über die MAC Adresse des Hosts definieren.
- *Dynamische Mitgliedschaft*: Ports können in einem VLAN dynamisch zugewiesen werden.
- *Weiterleitung in andere VLANs*: Wird durch Routing gehandhabt (so wie bei der Verwendung von unterschiedlichen Switches)
  - Üblicherweise bieten kommerzielle Lösungen heutzutage Kombinationen von Switches und Routern an

5.6 VLANs über mehrere Switches



- **Trunk Port**: Überträgt Rahmen von einem Switch zu einem anderen im selben VLAN.
  - Rahmen die in einem VLAN zwischen Switches übertragen werden können keine üblichen 802.1 Rahmen sein, sondern müssen ihre zugehörige VLAN ID Information tragen
  - Das 802.1Q Protokoll fügt bei Rahmen die zwischen Trunk Ports übertragen werden zusätzliche Header Felder hinzu und entfernt sie wieder

5.6 802.1Q Protokoll Format



5.7 PPP

5.7 Sicherungsschicht für Punkt-zu-Punkt-Verbindungen

- Ein Sender, ein Empfänger, ein Link – einfacher als Broadcast-Links:
  - Kein Mehrfachzugriff
  - Explizite MAC-Adressierung ist nicht nötig
  - Beispiele: Einwahlverbindung

- Bekannte Protokolle:
  - PPP (Point-to-Point Protocol)
  - HDLC: High-Level Data Link Control

5.7 PPP-Designanforderungen [RFC 1557]

- Rahmenbildung:
  - Rahmen der Sicherungsschicht zum Einpacken der Datenpakete der Netzwerkschicht
  - Beliebige Protokolle der Netzwerkschicht sollen gleichzeitig über dieselbe physikalische Verbindung übertragen werden können
  - Demultiplexing der einzelnen Netzwerkprotokolle muss möglich sein, d.h., man muss einem PPP-Rahmen ansehen, zu welchem Netzwerkprotokoll er gehört
- Transparenz:
  - Beliebige Daten müssen übertragen werden können
- Fehlererkennung (aber nicht Fehlerkorrektur)
- Verbindungszustand überwachen:
  - Erkennen und Signalisieren des Zusammenbruchs einer Verbindung an die Netzwerkschicht
- Konfiguration der Netzwerkschicht:
  - Per PPP soll die Netzwerkschicht (z.B. Netzwerkadressen) konfiguriert werden können

5.7 Keine Designforderungen waren…

- Fehlerkorrektur
- Zuverlässige Übertragung
- Flusskontrolle
- Reihenfolgeerhaltende Auslieferung der Rahmen
- Unterstützung von Punk-zu-Mehrpunkt-Verbindungen

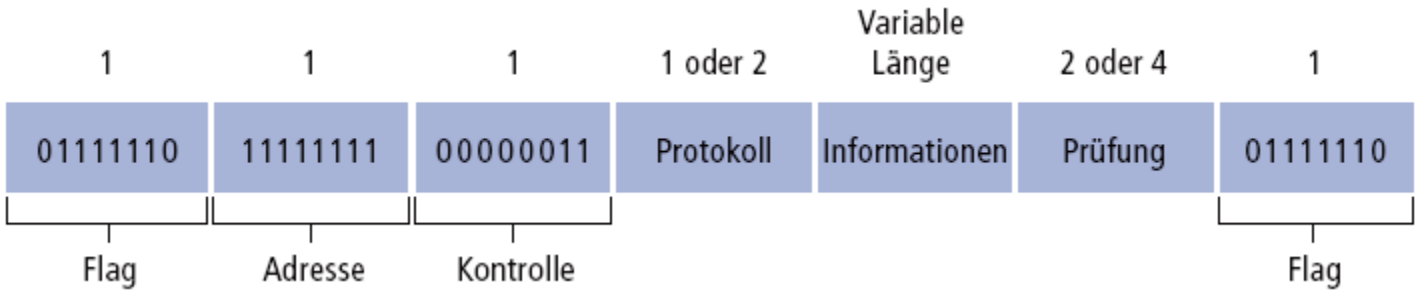
→ Zuverlässige Übertragung, Flusskontrolle und Reihenfolgeerhaltung werden **an die höheren Schichten delegiert**!

5.7 Was leistet PPP?

PPP [RFC 1661 / RFC 1662]:

- Schicht-2-Rahmenformat mit Fehlererkennung, Rahmenbegrenzung
  - Übertragung von Paketen der Netzwerkschicht als Nutzdaten
- Steuerprotokoll (LCP, Link Control Protocol)
  - Verbindungsaufbau
  - Verbindungstest
  - Verbindungsverhandlung
  - Verbindungsabbau
- Separates Protokoll (NCP, Network Control Protocol) für alle unterstützten Schicht-3-Protokolle
  - Zur Konfiguration des Netzwerkprotokolls eines der beiden verbundenen Endsysteme
  - Beispiel: Konfiguration des Netzwerkprotokolls IP durch den Service-Provider
    - Unter anderem: Zuweisung von Netzwerkadressen

5.7 PPP Rahmenformat



- **Flag:** Begrenzt den Rahmen
- **Adresse:** Keine Bedeutung, immer 11111111
- **Kontrolle:** Derzeit nicht verwendet
- **Protokoll:** Zu welchem Netzwerkprotokoll gehört das Paket im Datenteil
  - IP, AppleTalk, usw.
- **Informationen:** Die Nutzlast
  - Falls nicht anderweitig verhandelt, ist die maximale Länge der Nutzlast auf 1500 Byte begrenzt. (Durch zusätzliche Verhandlung kann der Paketkopf verkleinert werden.)
- **Prüfung:** CRC-Prüfsumme

5.7 Bytestopfen

- Transparenz: Im Informationenfeld darf das Bitmuster <01111110> vorkommen
  - **Problem:** Wenn man diese Folge empfängt, sind dies dann Daten oder das Flag?

→ **Lösung:** Bytestopfen (Byte Stuffing)

- Sender:
  - Fügt ein zusätzliches <01111101>-Kontroll-Escape-Byte vor jedem <01111110>-Datenbyte ein
- Empfänger:
  - Ein <01111101>-Kontroll-Escape-Byte vor einem <01111110>-Datenbyte erhalten:
    → erstes Byte verwerfen, zweites Byte als <01111110>-Datenbyte interpretieren
  - Zwei aufeinanderfolgende <01111101>-Kontroll-Escape-Bytes erhalten:
    → erstes Byte verwerfen, zweites Byte als <01111101>-Datenbyte interpretieren
  - Einzelnes <01111110>-Byte:
    → Flag

5.7 Bytestopfen - Beispiel

5.7 PPP Verbindung

Typisches Szenario beim Zugriff eines PCs auf das Internet via Einwahlverbindung:

1. Anruf beim Service-Provider und Aufbau einer physikalischen Verbindung
2. Anrufer sendet mehrere LCP-Pakete in PPP-Rahmen zur Auswahl der gewünschten PPP-Parameter
3. Austausch von NCP-Paketen, um die Vermittlungsschicht zu konfigurieren
   - Zum Beispiel kann hier dynamisch mittels DHCP eine IP-Adresse zugewiesen werden, falls IP als Protokoll gewählt wurde
4. Der Anrufer kann nun genauso wie ein fest verbundener Rechner Internetdienste nutzen
5. Zur Beendigung der Verbindung wird via NCP die IP-Adresse wieder freigegeben und die Vermittlungsschichtverbindung abgebaut
6. Über LCP wird die Schicht-2-Verbindung beendet, schließlich trennt das Modem die physikalische Verbindung

5.8 Link-Virtualisierung: ATM und MPLS

5.8 ATM und MPLS

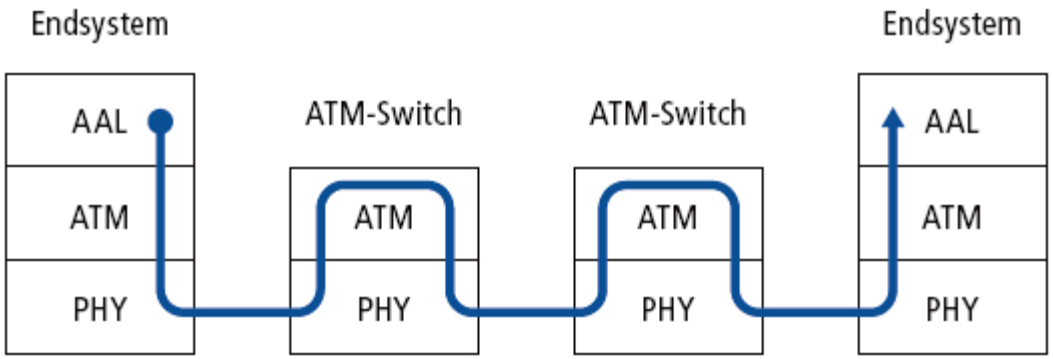
- ATM, MPLS sind eigenständige Netzwerktechnologien
  - Eigene Dienstmodelle, Adressierung, Routing
  - Unterscheiden sich von IP !!!
- Vom Internet als logischer Link zwischen zwei IP-Routern betrachtet
  - Genauso wie eine Einwahlverbindung zu einem eigenständigen Netzwerk (dem Telefonnetzwerk) gehört
- ATM, MPLS: Technisch spannend, auch unabhängig vom Internet

Wir betrachten hier vor allem das Zusammenspiel mit dem Internet.

5.8 Asynchronous Transfer Mode - ATM

- Standard der 1990er und 2000er Jahre für Broadband-ISDN **(**155 Mbps bis 622 Mbps und mehr)
- Ziel: **integrierter Ende-zu-Ende-Transport von Sprache, Video und Daten**
  - Sollte die Dienstgüteanforderungen von Sprache und Video erfüllen (im Gegensatz zu den Diensten, die das Internet anbietet)
  - Nächste Generation des Telefonnetzwerkes: technischer Ursprung im Telefonnetzwerk
  - Paketvermittlung (**kleine Pakete fester Länge** werden in ATM **als Zellen bezeichnet**) mit virtuellen Leitungen

5.8 ATM-Architektur



- **AAL (ATM Adaptation Layer):** nur am Rand des ATM-Netzwerkes
  - Segmentieren und Zusammenfügen von Daten
  - Entspricht grob der Transportschicht im Internet
- **ATM (ATM Layer):** “Netzwerkschicht”
  - Weiterleiten von Zellen, Routing
- **PHY (Bitübertragungsschicht, Physical Layer)**

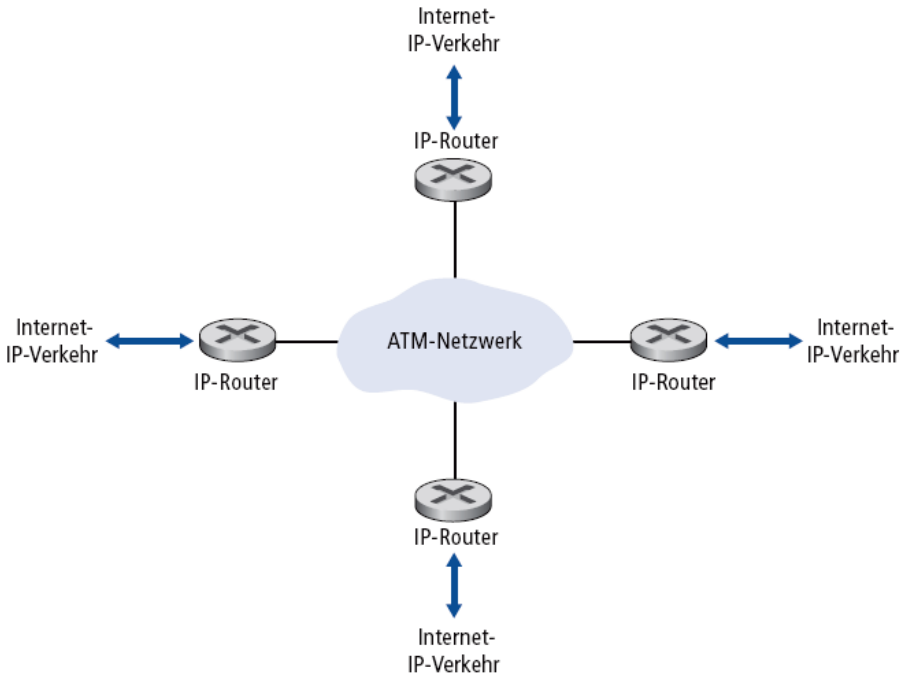
5.8 ATM – Netzwerk- oder Sicherungsschicht?

Vision: Ende-zu-Ende-Transport: “ATM von PC zu PC”

- ATM ist eine Netzwerktechnologie

Realität: wird verwendet, um IP-Backbone-Rechner zu verbinden (der Einsatz von ATM nimmt derzeit aber sehr stark ab!)

- “IP over ATM”
- ATM als Sicherungsschicht



5.8 ATM Adaption Layer (AAL)

- Die AAL-Schicht erhält Anwendungsdaten zur Übertragung über das ATM-Netzwerk
- Hier: Die Anwendung ist die Netzwerkschicht (IP) des Internets
- Sie stellt verschiedene Dienste zur Verfügung:
  - AAL1: Verbindungen mit konstanter Bitrate (z.B. Telefonie)
  - AAL2: Verbindungen mit variabler Bitrate (z.B. Videoübertragung)
  - AAL5: Datendienste, wird für IP verwendet:

- Aus Sicht der Vermittlungsschicht im Internet (IP) entspricht ein AAL5-Paket einem Ethernet-Rahmen

5.8 ATM Virtual Channels

- Virtual Circuits bzw. virtuelle Verbindungen werden in ATM Virtual Channels (VCs) genannt
- Ein **Virtual-Channel-Identifier** kennzeichnet den Teil einer virtuellen Verbindung, der zwischen zwei Routern liegt
  - Dies entspricht der VC-Kennung, wie wir sie bei virtuellen Verbindungen besprochen haben
- Virtual Channels werden entweder permanent betrieben und manuell konfiguriert
  - Verbinden zweier IP-Router über IP-over-ATM
- ... oder mithilfe eines Protokolls namens Q.2931 dynamisch auf- und abgebaut (eher selten)

5.8 ATM Virtual Channels

+ Vorteile:
  + Es können Dienstgütegarantien für einen VC abgegeben werden, jedem VC können Ressourcen zugewiesen werden
- Nachteile:
  – Ineffizient für normalen Datenverkehr
  – Ein VC pro Sender-Empfänger-Paar skaliert nicht
  – Bei dynamischem Aufbau entsteht eine zusätzliche Verzögerung, bis der VC aufgebaut ist

5.8 ATM Zellen

Für die Übertragung der Daten werden die AAL-Pakete in sogenannte ATM-Zellen zerlegt:

- 48 Byte Nutzdaten (konstante Größe)
- 5 Byte Header

•**VCI** = Virtual Channel Identifier:

- Identifiziert den Virtual Channel für diese Zelle
- Verändert sich von ATM-Switch zu ATM-Switch

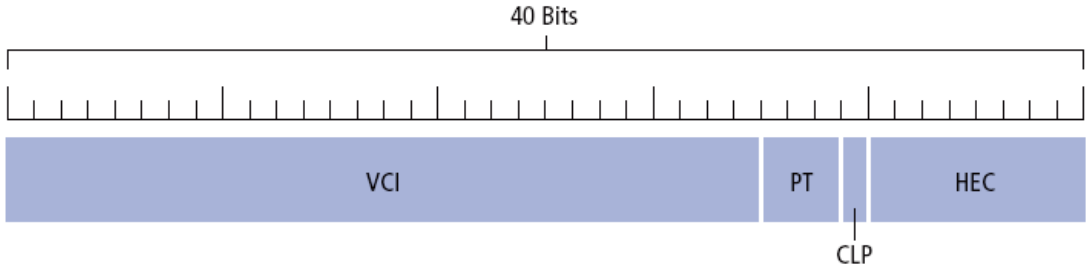
•**PT** = Payload Type:

- Bestimmt, was im Datenteil steht

•**CLP** = Cell Loss Priority

- Erlaubt eine *Priorisierung* von Zellen: zuerst werden Zellen mit niedriger Priorität verworfen

•**HEC** = Header Error Control



5.8 IP over ATM

IP-Paket kommt an einem IP-Router am Rand des ATM-Netzwerkes an

1. Routing-Tabelle konsultieren, IP-Adresse des nächsten IP-Routers bestimmen, Interface zum nächsten IP-Router bestimmen
2. Herausfinden der Schicht-2-Adresse zu dieser IP-Adresse
   - Bei Ethernet: ARP
   - Bei ATM: ATM ARP [RFC2225]
   - ATM ARP identifiziert den VC, der verwendet werden soll
3. Übergeben des IP-Paketes an ATM AAL5
4. Zerlegen des ATM-AAL5-Rahmens in ATM-Zellen
5. ATM-Zellen über mehrere ATM-Switches an den Router am Rand des ATM-Netzwerkes weiterleiten
6. Dort wird der ATM-AAL5-Rahmen wieder zusammengesetzt und das IP-Paket ausgepackt

5.8 MPLS - Hintergrund

Weiterleiten von Paketen mit IP:

- Alle Router entscheiden unabhängig voneinander, wie jedes einzelne Paket zu handhaben ist
- Ein IP-Router schlägt für jedes IP-Paket in der Routing-Tabelle die Zieladresse nach und bestimmt anhand der Zieladresse, wie das Paket zu handhaben ist (z.B. wohin es weitergeleitet wird)
  - In schlechten/alten Implementierungen war das sehr zeitaufwendig (Longest Prefix Matching)
- Ein IP-Router hat über ein IP-Paket nur die Informationen, die mit dem Paket mitgeschickt werden
  - Insbesondere kann ein Router im Netz nicht mehr feststellen, auf welchem Pfad das IP-Paket zu ihm gelangt ist
- **Für ISPs ist es relativ schwierig, den Netzwerkverkehr zu einem Präfix auf Basis von IP zu steuern - das geht nur implizit über die Linkgewichte!**

5.8 MPLS - Idee

Multiprotocol Label Switching – Grundlegende Idee:

High-speed IP Weiterleitung durch die Einführung sogenannter **Fixed-Length Labels** (die statt der IP Adresse für die Weiterleitung herangezogen werden).

- Schnelle Adressauflösung durch Fixed Length Identifier (statt Shortest Prefix Matching)
- Übernimmt grundlegende Ideen von Virtual Circuit (VC)
- IP Datagramme behalten aber dennoch ihre IP Adresse!

→MPLS verwendet **virtuelle Verbindungen** für Datagrammnetzwerke!

Vorteil: Flexibilität

MPLS Weiterleitungs-Pfad Entscheidungen können sich von IP-basierten Entscheidungen unterscheiden!

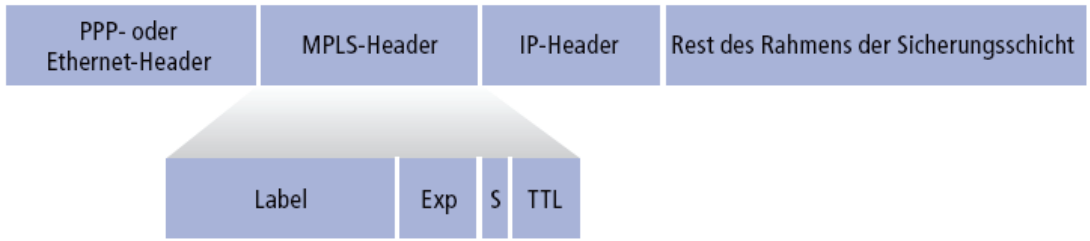
- Kann Ziel- und Quell-Adresse verwenden um Datenströme zum selben Ziel unterschiedlich zu routen (Traffic Engineering)
- Kann bei einem Ausfall Datenströme schnell neu weiterleiten durch im Voraus bestimmten Backup-Pfad (besonders nützlich für VoIP)

5.8 MPLS – Prinzipielle Funktionsweise

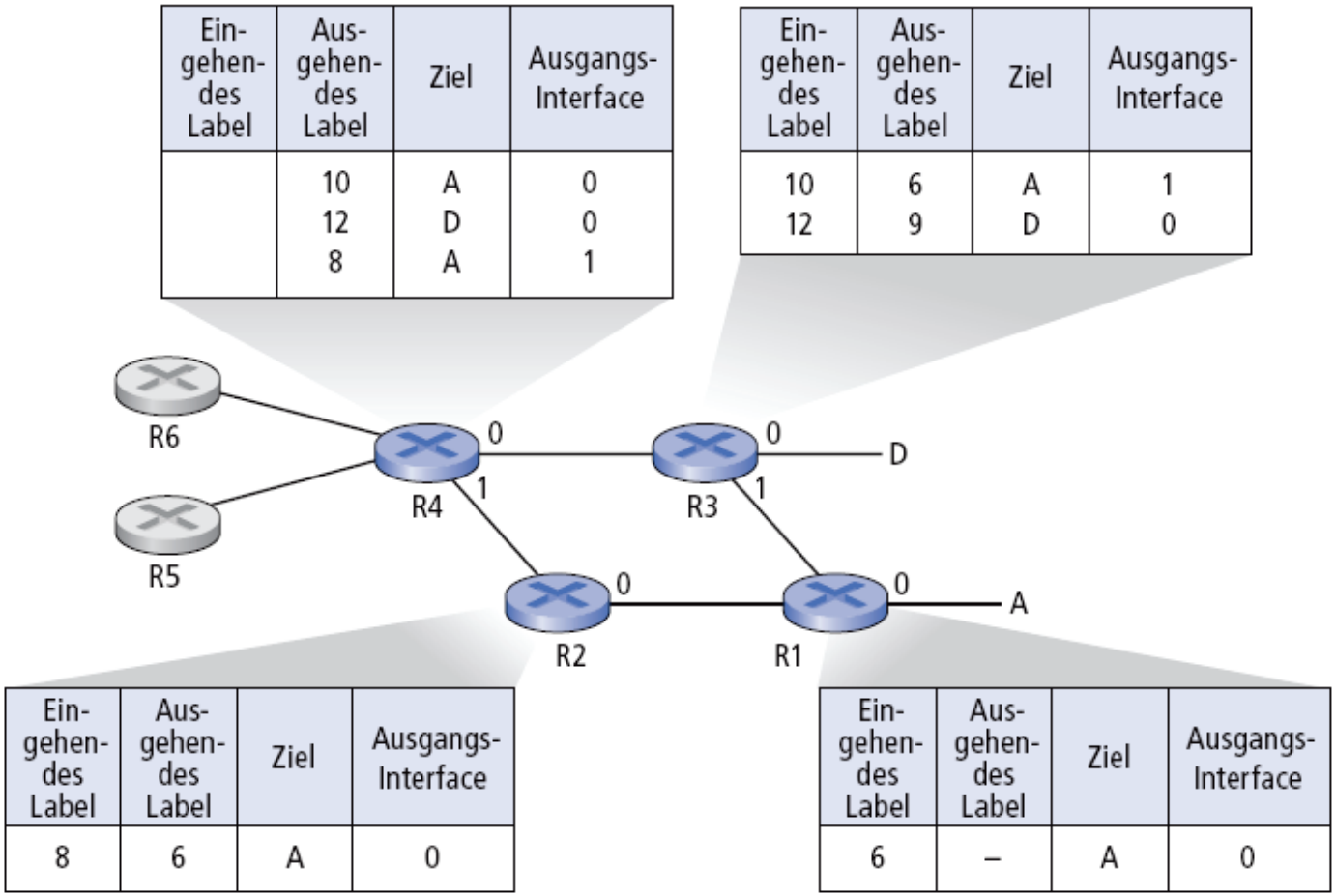
Vorgehen:

1. MPLS-fähige Teilnetzwerke halten virtuelle Verbindungen zwischen den Routern am Rand des MPLS-fähigen Teilnetzwerkes aufrecht.
2. Wenn ein IP-Paket am Rand eines MPLS-fähigen Teilnetzwerkes ankommt:
   - Verwende alle Informationen (woher kommt das Paket, IP-Header, Policies, usw.), um dieses Paket einer virtuellen Verbindung bis zum Ausgang des MPLS-fähigen Teilnetzwerkes zuzuweisen.
   - Die Kennung der virtuellen Verbindung (genannt **Label**) wird in das Paket zwischen dem Header für die Sicherungsschicht und dem Header der Netzwerkschicht eingetragen.
3. Im Inneren eines MPLS-fähigen Teilnetzwerkes:
   - Leite das Paket auf der virtuellen Verbindung zum Ausgang des Teilnetzwerkes weiter, ohne den IP-Header zu beachten.

Ein MPLS-Rahmen sieht wie folgt aus:



5.8 MPLS – Prinzipielle Funktionsweise



5.8 MPLS

- Wie werden die Labels verteilt?
  - Statisch per fester Konfiguration
  - Dynamisch mithilfe geeigneter Protokolle
    - z.B. über RSVP-TE (RFC 3209)
- Warum ist MPLS bei ISPs erfolgreich?
  - Mehr **explizite Kontrolle** über den Netzwerkverkehr!
    - Die (gleichmäßige) Verteilung der Verkehrslast mittels Routing gehört zur Disziplin *Traffic Engineering*
    - MPLS Traffic Engineering wird in RFC 3346 diskutiert
  - **Link Protection** – Schnelle Routenänderungen bei einzelnen Link-Brüchen
  - Realisierung von großen **Virtual Private Networks** mittels BGP/MPLS IP VPNs [RFC 4364] → Ein sehr interessanter Einsatzzweck für BGP
    - Verbinden von Netzwerken in vielen räumlich getrennten Niederlassungen eines Kunden über das Internet
    - Aus Kundensicht entsteht so ein eigenständiges, privates, vom Internet unabhängiges Netzwerk

5.9 Rechenzentren-Netzwerke

5.9 Rechenzentren-Netzwerke

- 10-Tausende bis 100-Tausende Hosts, oft eng verbunden auf kleinem Raum:
  - e-Business (z.B. Amazon)
  - Content-Dienste (z.B. YouTube, Akamai, Apple, Microsoft)
  - Suchmaschinen, Data Mining

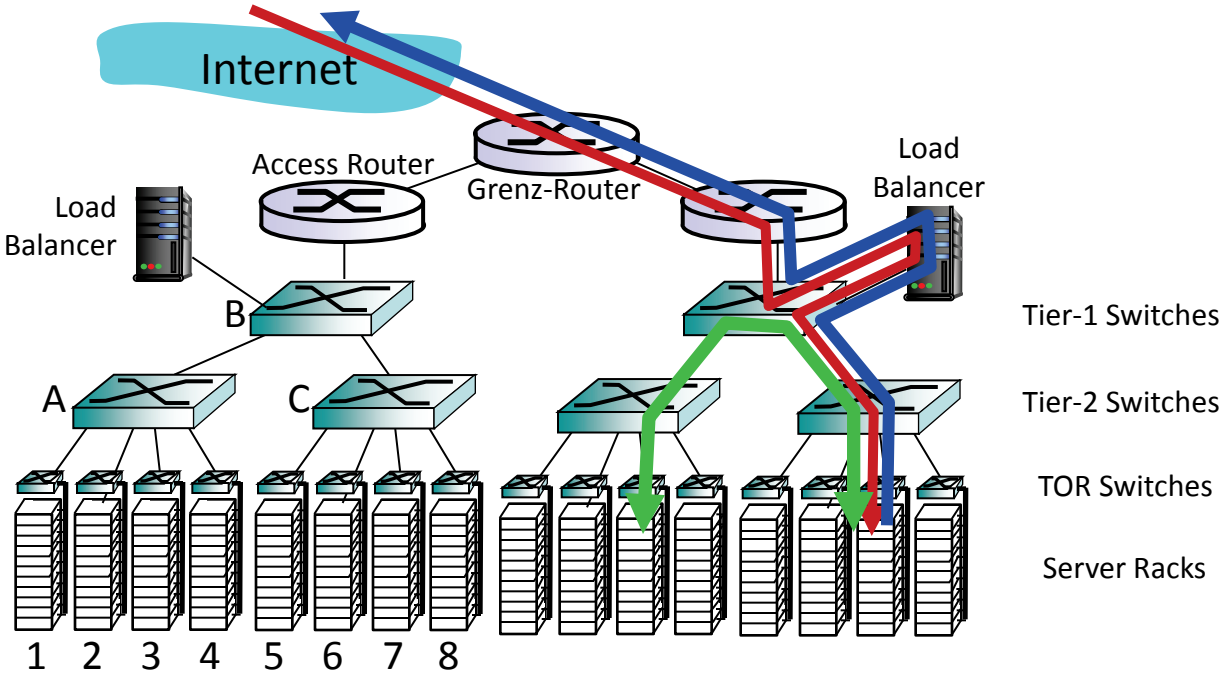
- Herausforderungen:
  - Mehrere Applikationen von denen jede eine große Anzahl an Benutzern bedient
  - Die Last verwalten/verteilen, ohne Rechen-, Netzwerk- oder Datenzugriffs-Bottlenecks zu schaffen

Innenraum eines Microsoft Containers
im Datenzentrum in Chicago

5.9 Rechenzentren-Netzwerke

Load Balancer: Routing auf Applikationsebene

- Empfängt die externen Clientanfragen
- Verteilt die Arbeitslast innerhalb des Rechenzentrums
- Gibt die Ergebnisse an den externen Client zurück (wobei Informationen über die interne Rechenzentrumsbearbeitung vor dem Client verborgen werden)



5.9 Rechenzentren-Netzwerke

- Vielzahl Verbindungen zwischen Switches und Server Racks:
  - Ermöglicht hohen Durchsatz zwischen Racks (mehrere unterschiedliche Routing-Pfade möglich)
  - Erhöhte Zuverlässigkeit durch redundante Pfade