

# **Rechnernetze:**

## **(10) Sicherungsschicht**



**Prof. Dr. Klaus-Peter Kossakowski**



# Gliederung der Vorlesung

- Einführung und Historie des Internets
- Schichtenmodell
- Netzwerk als Infrastruktur
- Layer 7: Anwendungsschicht
- Layer 5: Sitzungsschicht
- Layer 4: Transportschicht
- Layer 3: Netzwerkschicht
- Layer 2: Sicherungsschicht
  - Kabelgebunden im LAN
  - Funkverbindungen im WLAN



# Inhalte dieses Kapitels

In diesem abschließenden Kapitel werden die Verfahren der Sicherungsschicht getrennt nach kabelbasierten und kabellosen Medien behandelt.

Bei den Medien werden die unterschiedlichen Arten, mehrere Endgeräte im Wechsel das Medium nutzen zu lassen, erklärt und durchgesprochen.

Die Unterschiede zwischen Hubs, Switches (Level 2) und Routern werden dargestellt. Ebenso MAC-Adressen und das ARP/RARP-Protokoll.



# Ziele dieses Kapitels

Sie können die unterschiedlichen Probleme beim Zugang mehrerer Endgeräte auf das gleiche Medium erläutern und die behandelten Protokolle bzw. Verfahren der Sicherungsschicht nennen.

Sie können das Verfahren CSMA/CD und seine Anwendung in Ethernet ebenso wie MAC-Adressen und ARP/RARP erklären.

Sie können Hubs und Switches als weitere Netzwerkkomponenten gegenüber Routern abgrenzen und Unterschiede bzw. Gemeinsamkeiten erklären.

# Wo ist die Sicherungsschicht implementiert?

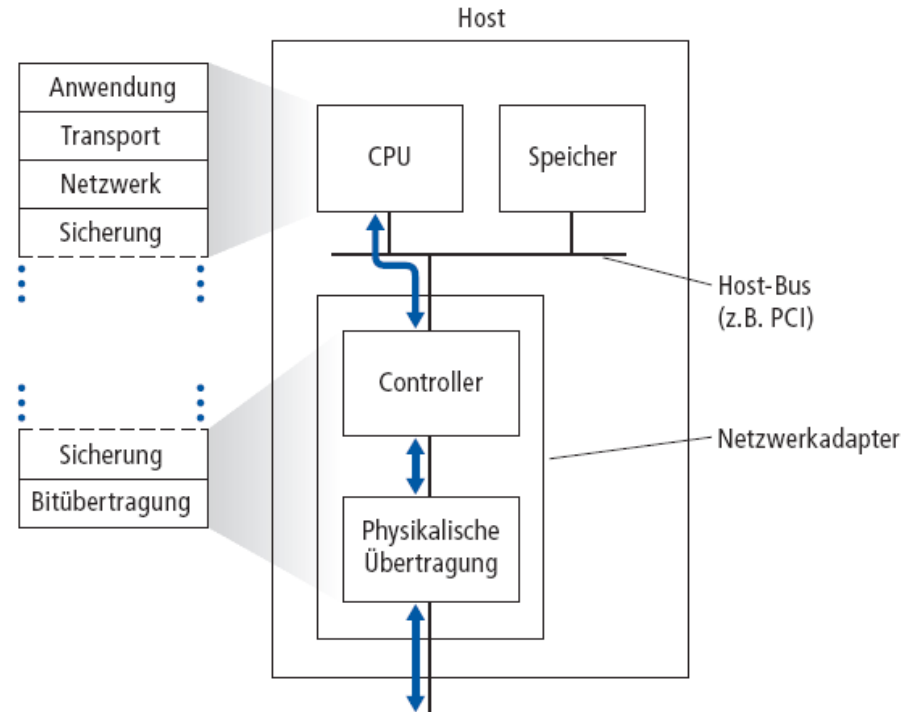


## ■ In jedem Endgerät als Netzwerkadap-ter bzw. -karte implementiert

■ Enthält außerdem die physikalische Schicht

## ■ Kombination von

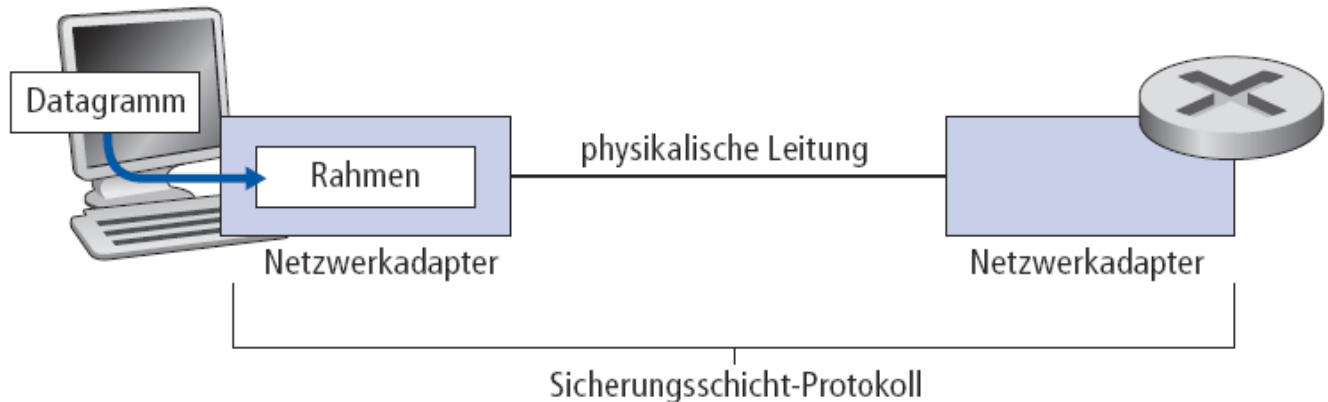
- Hardware
- Software
- Firmware





# Dienste der Sicherungsschicht

- Rahmenbildung und Zugriff auf die physikalische Leitung, genannt „Link“
  - Halbduplex und Vollduplex



- Zuverlässige Datenübertragung zwischen benachbarten Knoten



# Dienste der Sicherungsschicht

- **Rahmenbildung und Zugriff auf den Link**
  - Verpacken eines Datagramms in einen Rahmen, Hinzufügen von Header und Trailer
  - Zugriff auf den Kanal (schwierig, wenn dieser von mehreren Knoten verwendet wird)
  - “MAC”-Adressen (Medium Access Control) werden im Header von Rahmen verwendet, um Sender und Empfänger zu kennzeichnen



# Dienste der Sicherungsschicht

- **Zuverlässige Datenübertragung zwischen benachbarten Knoten**
  - Funktion ist bereits bekannt, trotzdem ...
  - Drahtgebundene Links: geringe Bitfehlerrate
    - Seltener Einsatz, wenn der Link sehr wenige Bitfehler verursacht (Glasfaser, Kupferkabel etc.)
  - Drahtlose Links: hohe Bitfehlerrate
    - Frage: Warum ist hier Zuverlässigkeit auf der Sicherungsschicht und der Transportschicht sinnvoll?





# Zuverlässigkeit durch ...

## ■ Flusskontrolle

- Anpassen der Sendegeschwindigkeit

## ■ Fehlererkennung

- Der Empfänger sollte Fehler erkennen können, aber besser ist ...

## ■ Fehlerkorrektur

- Der Empfänger erkennt und korrigiert Bitfehler, ohne Neuübertragung anzufordern

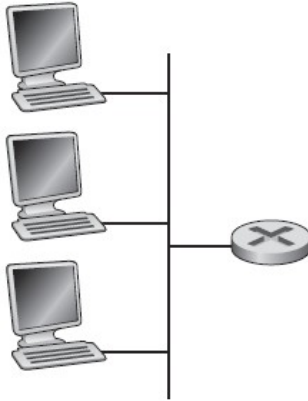


# **Zugriff von mehreren Endgeräten auf das gleiche Medium**



# Links mit Mehrfachzugriff

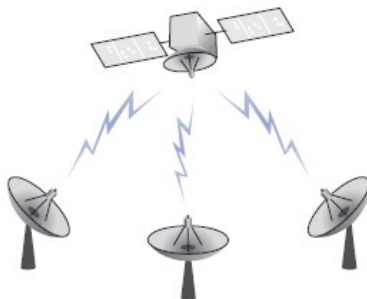
Gemeinsam genutzte Leitung  
(z.B. Ethernet)



Gemeinsam genutzter Funkkanal  
(z.B. WLAN)



Satellit



Cocktailparty



# Links mit Mehrfachzugriff

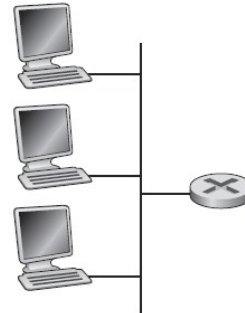


## Zwei Arten von “Links”:

### ■ Punkt-zu-Punkt

- Einwahlverbindungen
- Verbindung zwischen Ethernet-Switch und Host

Gemeinsam genutzte Leitung  
(z.B. Ethernet)



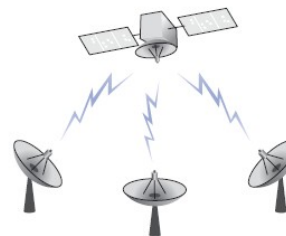
Gemeinsam genutzter Funkkanal  
(z.B. WLAN)



### ■ Broadcast (gemeinsam verwendetes Medium)

- Ursprüngliches Ethernet mit Coax-Kabel
- Upstream bei HFC (Downstream über das Fernsehkabelnetz)
- IEEE 802.11 WLAN

Satellit



Cocktailparty





# Protokolle für den Mehrfachzugriff

- Ein gemeinsam genutzter Broadcast-Kanal
- Mehrere gleichzeitige Übertragungen verschiedener Knoten:
  - Kollision, wenn ein Knoten mehrere Signale zur gleichen Zeit empfängt
  - Durch Kollision unbrauchbare Signale
- Protokolle für den Mehrfachzugriff sog. MAC-Protokolle (Medium Access)
  - Verteilte Algorithmen, die bestimmen, wie sich die Knoten den Kanal teilen



# Protokolle für den Mehrfachzugriff

- **Protokolle für den Mehrfachzugriff (MAC-Protokolle)**
  - Verteilte Algorithmen, die bestimmen
    - wie sich die Knoten den Kanal teilen
    - wer wann senden darf
- **Kein zusätzlicher Kanal für die Koordination**
  - Die dazu notwendige Kommunikation muss wiederum über den Broadcast-Kanal selbst abgewickelt werden

# Das perfekte Protokoll für den Mehrfachzugriff



## Gegeben: Ein Broadcast-Kanal mit $R$ bps

- Wenn nur ein Knoten übertragen möchte, dann kann er mit der Rate  $R$  senden
- Wenn  $M$  Knoten übertragen möchten, dann kann jeder mit der Rate  $R/M$  senden
- Dezentral:
  - Kein spezieller Knoten zur Koordination der Übertragungen
  - Keine Synchronisation von Uhren oder Zeitschlitz
- Einfach



# Klassifikation von MAC-Verfahren

## □ Aufteilen des Mediums

- Die Datenrate des Mediums wird in kleinere Einheiten 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

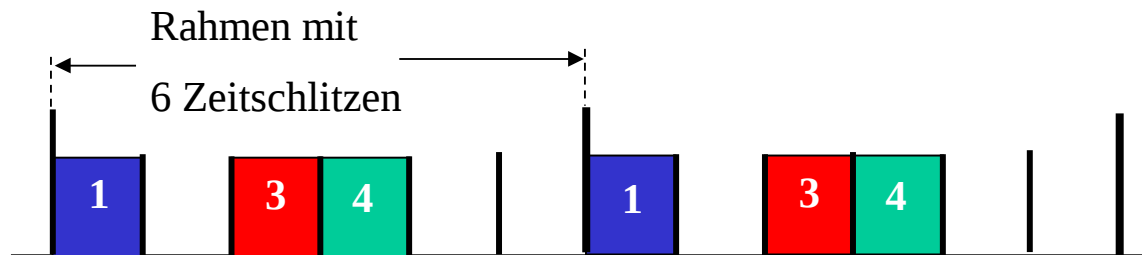
- Die Zugriffe der Stationen werden koordiniert, es darf abwechselnd gesendet werden
- Kollisionen werden vermieden





# Aufteilung mit TDMA

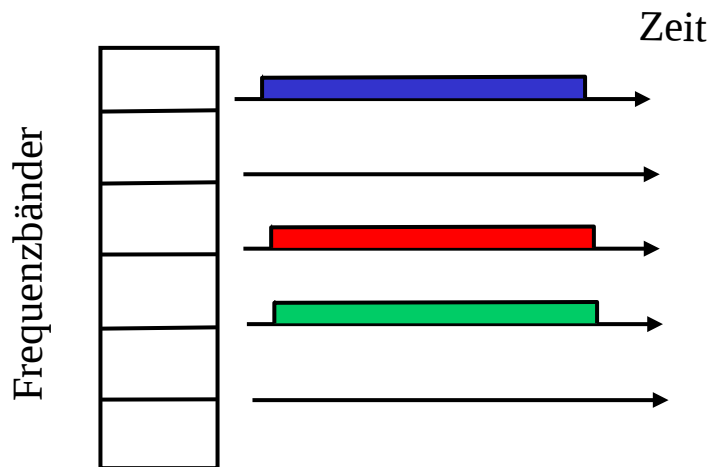
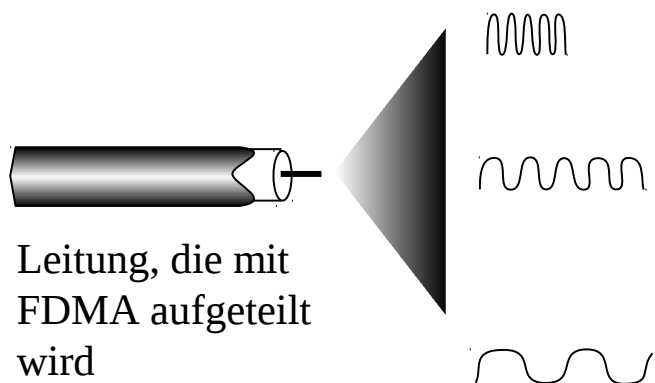
- **TDMA: Time Division Multiple Access, Zeitmultiplexing**
- Auf das Medium wird in Runden zugegriffen
- Jede Station bekommt einen festen Zeitschlitz zum Senden in jeder Runde
- Nicht verwendete Zeitschlitzte gehen verloren
- Beispiel: LAN mit 6 Stationen
  - 1,3,4 senden
  - 2,5,6 senden nicht





# Aufteilung mit FDMA

- **FDMA: Frequency Division Multiple Access, 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
  - ▮ Gleiches Beispiel wie TDMA





# Protokolle mit wahlfreiem Zugriff

## ■ Wenn ein Knoten ein Paket 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

# 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!  
Aber wenn man angefangen hat, auch zuende reden!



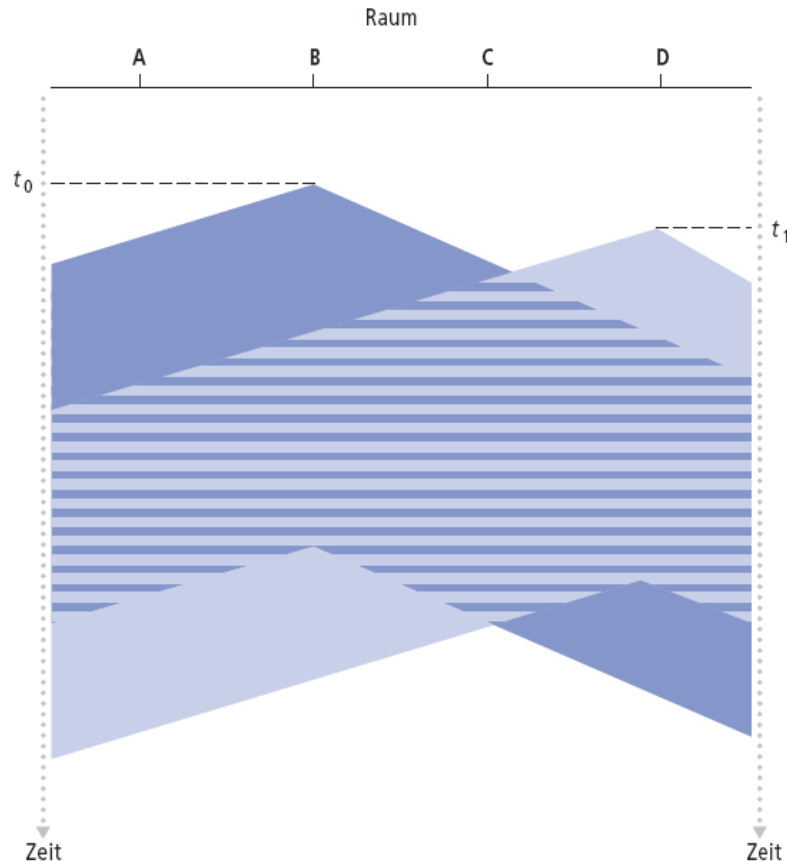
# CSMA: Kollisionen

Kollisionen können immer noch auftreten:

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

## ■ Kollision

- Dauert die ganze Übertragungszeit
- Zeit wird verschwendet





# CSMA/CD (Collision Detection)

## CSMA/CD: Carrier Sensing wie in CSMA

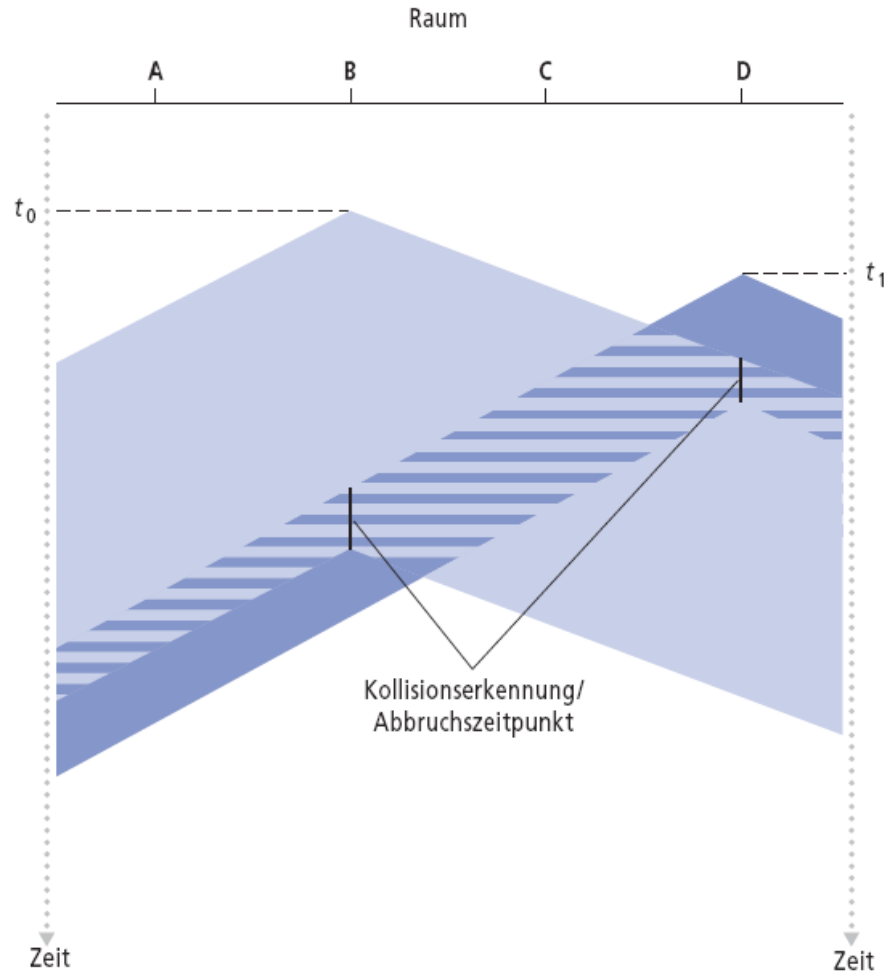
- Kollisionen werden schnell erkannt
- Übertragungen, die kollidieren, werden sofort abgebrochen

## ■ 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

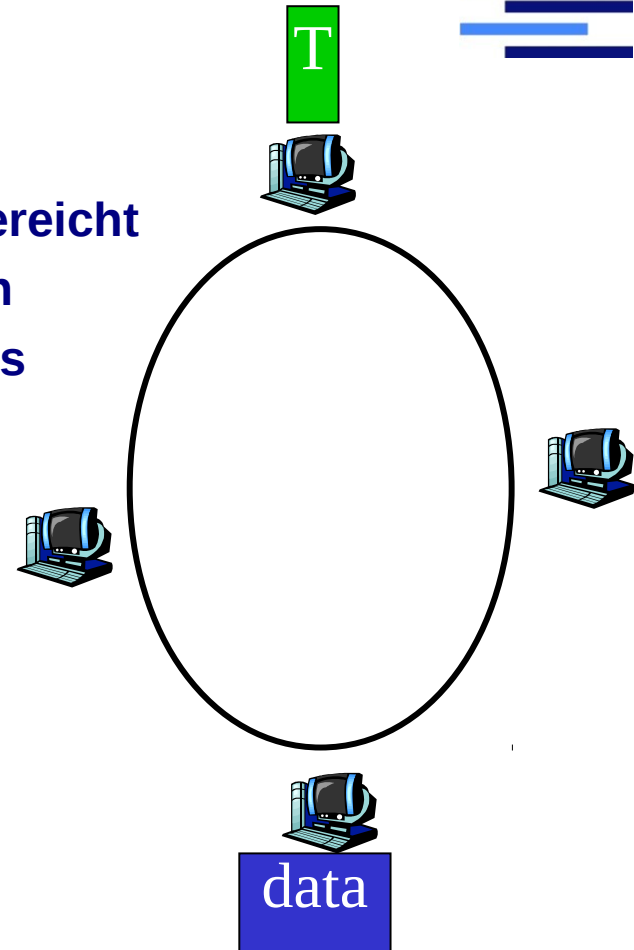
## ■ Analogie: der höfliche Diskussionssteilnehmer

# CSMA/CD: Erkennen von Kollisionen



# 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







# Zusammenfassung MAC-Protokolle

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



# Adressierung in der Sicherungsschicht



# MAC-Adressen und ARP

## ■ 32-Bit-IP-Adresse / Netzwerkschicht:

- Wird verwendet, um ein Datagramm zum Zielnetzwerk zu leiten
- Beinhaltet Ortsinformationen:  
Wo befindet sich das Zielnetzwerk?

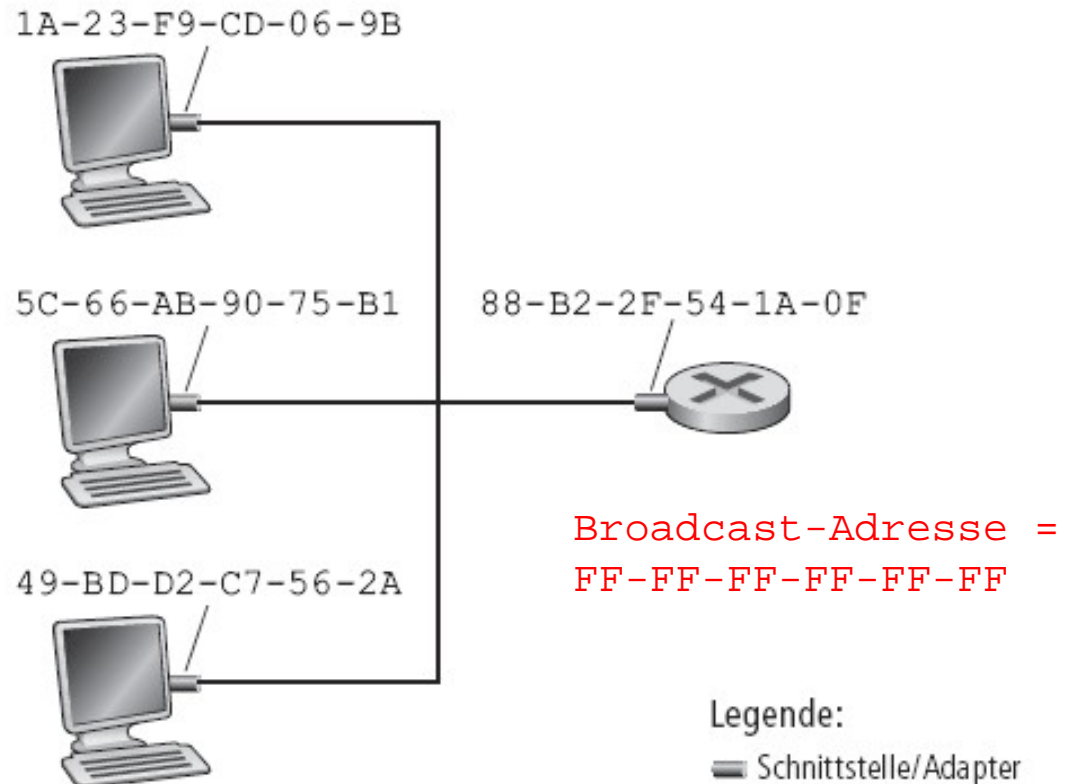
## ■ 48-Bit-MAC-Adresse / Sicherungsschicht:

- Wird verwendet, um einen Rahmen von einem Adapter zu einem benachbarten Adapter weiterzuleiten (im selben lokalen Netzwerk!)
- Keine Ortsinformationen, muss nur im gegebenen Netzwerk eindeutig sein
  - Früher in das ROM der Netzwerkkarte eingebrannt, heute häufig durch Software veränderbar



# MAC-Adressen und ARP (2)

**Jeder Adapter im LAN hat eine eindeutige MAC-Adresse**





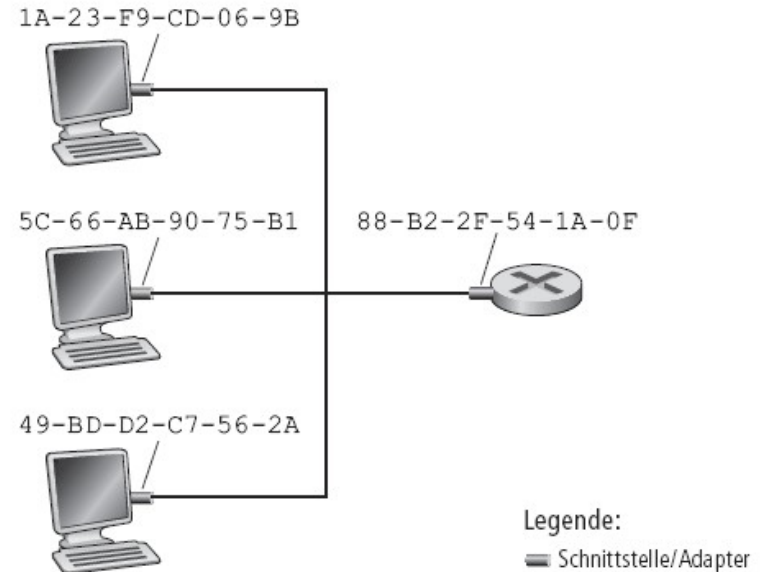
# MAC-Adressen und ARP (3)

- **Die Zuordnung von MAC-Adressen wird von der IEEE überwacht**
  - Eindeutigkeit über Hersteller hinweg
- **Analogie:**
  - MAC-Adresse: Rentenversicherungsnummer
  - 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

# ARP: Address Resolution Protocol



- 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



Jetzt habe ich die IP-Adresse, brauche aber die MAC-Adresse???



# ARP: Funktionsweise

- **A möchte ein Datagramm an B schicken, die MAC-Adresse von B ist nicht im ARP-Cache von A**
- **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
- **B empfängt die ARP-Query, erkennt seine IP-Adresse und antwortet A**
- **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
- **A schickt den Datagrammrahmen, der die IP- und die MAC-Adresse von B enthält**
- **ARP ist “Plug-and-Play”:**
  - Keine manuelle Konfiguration notwendig

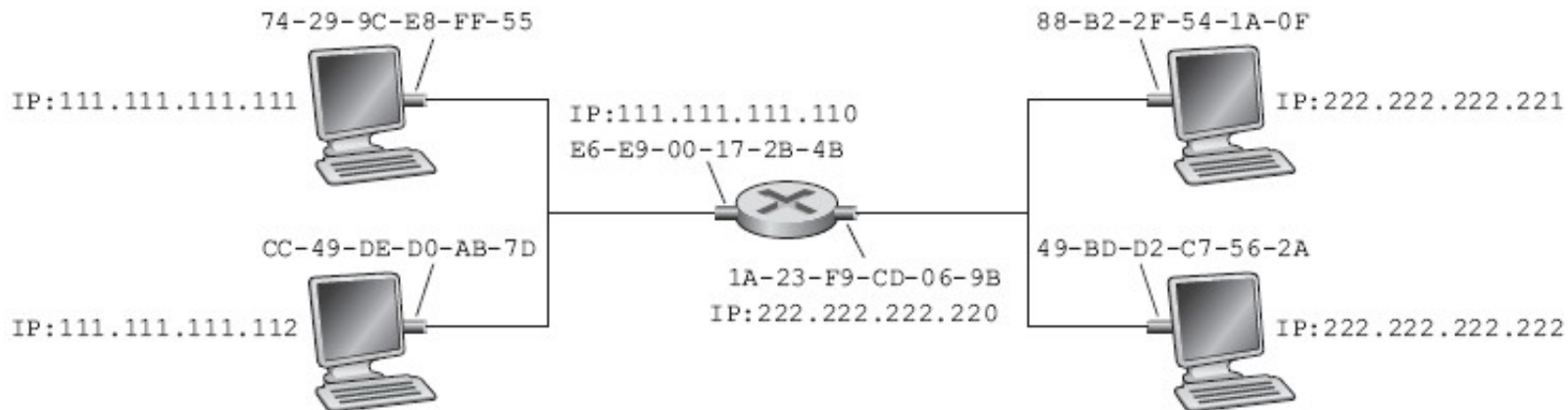
# ARP:

## Routing zwischen zwei LANs



### ■ Szenario:

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

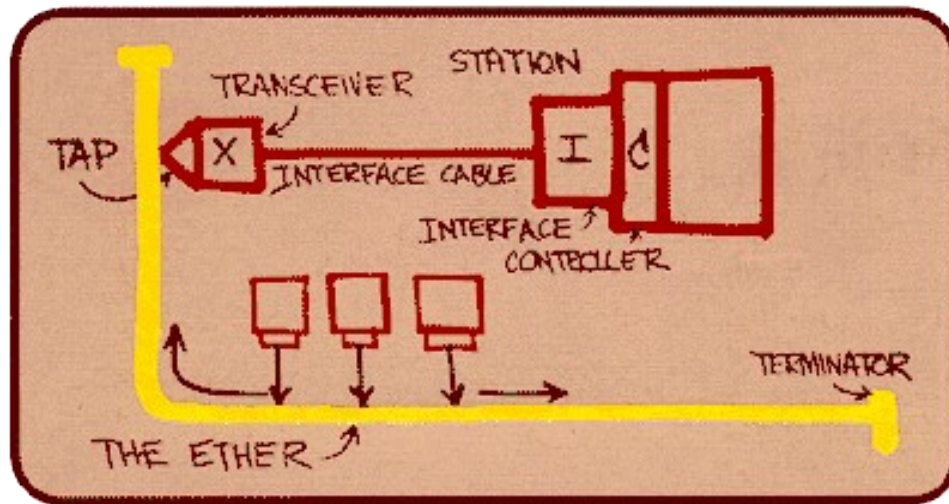


- Zwei ARP-Tabellen in R, eine für jedes LAN

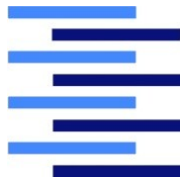




# Ethernet



Metcalfe's  
Ethernet-Entwurf



# Ethernet

- **Marktbeherrschende LAN-Technologie auf Basis von CSMA/CD-Basis**
  - Erste weitverbreitete LAN-Technologie
  - Einfacher und billiger als Verfahren mit koordiniertem Kanalzugriff
  - Billig (Netzwerkkarten für  $< 10$  €)
- **Datenrate hat sich über die Zeit stark erhöht**
  - 10 und 100 Mbit/s
  - 1 und 10 Gbit/s und 100 Gbit/s auch über Kupfer!



# Ethernet (2)

## ■ Wie bekommen wir 100 Gbit/s Ethernet? entweder

- parallele Übertragung von jeweils 10 Gbit/s über zehn Kupferleitungen

## oder

- Parallele Übertragung von jeweils 25 Gbit/s über vier Lichtwellenleiter bzw.
- über einen Lichtwellenleiter mit vier verschiedene Wellenlängen (Farben)

## ■ Bitfehlerrate $< 10^{-12}$ gefordert



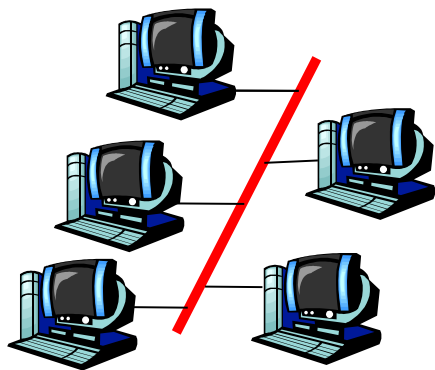
# Ethernet-Topologien

## ■ Bus-Topologie bis in die Mitte der 90er Jahre

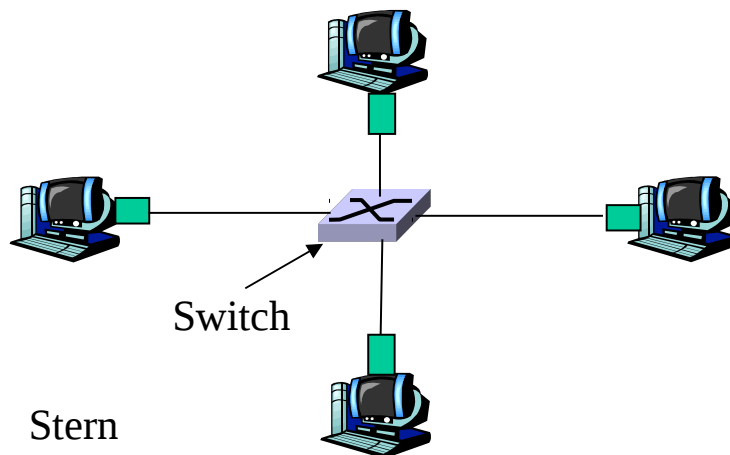
- Alle Knoten in einer Kollisionsdomäne – die Übertragung eines Knotens konnte mit der Übertragung jedes anderen Knotens kollidieren

## ■ Heute: Stern-Topologie

- Aktiver Switch im Zentrum, an den alle angeschlossen sind



Bus: Koaxialkabel



Stern



# 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
- Paketende:**
  - Erkannt durch eine Ruheperiode von 9,6 Mikrosekunden



# Ethernet-Rahmenstruktur (2)

- **MAC-Adressen: 6 Bytes**
  - Wenn eine 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 unter 0x0600 signalisieren einen IEEE 802.x-Rahmen
  - Werte ab 0x0600 sind zulässig
  - Beispiel 0x0800 = IP-Paket
- **CRC: Überprüfen auf Bitfehler, bei Erkennen eines Fehlers wird das Paket einfach verworfen**





# Dienst von Ethernet

- **Ethernet stellt einen unzuverlässigen und verbindungslosen Dienst zum Austausch von Daten zwischen Stationen in einem LAN zur Verfügung**
  - Verbindungslos: kein Verbindungsauf- und -abbau zwischen Sender und Empfänger
  - Unzuverlässig: Pakete mit Übertragungsfehlern (z.B. Bitfehler, also keine Kollisionen) kommen vor
    - Fehlerhafte Pakete werden einfach verworfen



# Ethernet verwendet CSMA/CD

- ▮ Netzwerkkarte bekommt die zu sendenden Daten
- ▮ Wenn das Medium von der Netzwerkkarte als frei erkannt wird, dann überträgt sie die Daten in einem Ethernet-Rahmen.
- ▮ Wenn das Medium belegt ist, wartet die Netzwerkkarte, bis das Medium frei wird, und überträgt dann
- ▮ Wenn der Rahmen ohne Kollision übertragen wurde: Erfolg
- ▮ Wenn eine Netzwerkkarte eine Kollision feststellt, dann wird die Übertragung abgebrochen und ein Jam-Signal gesendet
- ▮ Danach wird „Exponential Backoff“ durchgeführt: Nach der m-ten Kollision zieht die Netzwerkkarte eine Zufallszahl K aus dem Bereich  $\{0,1,2,\dots,2^m-1\}$ .
- ▮ Die Netzwerkkarte wartet  $K \cdot 512$  Bit-Zeiten (= Dauer der Übertragung eines Bits) und geht dann zum zweiten Schritt zurück



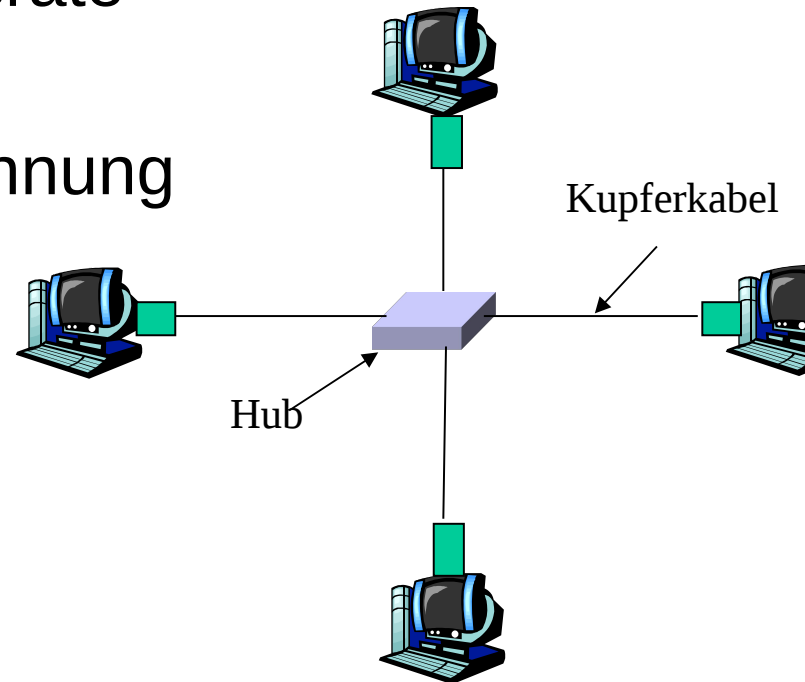


# Ethernet Hubs und Switches



# Hubs - physikalische Kopplung

- Bits, die auf einem Link ankommen, werden auf alle anderen Links kopiert
- Erhalt der Eingangsrate
- Keine Pufferung
- Kein Kollisionserkennung durch den Hub





# Switch - aktive Bearbeitung

## ■ Switch arbeitet auf der Sicherungsschicht:

- Empfängt, puffert und leitet weiter
- Weiterleitung anhand der Empfängeradresse
- Verwendung von CSMA/CD

## ■ Transparent

- Endsysteme wissen nichts über die Gegenwart eines Switches

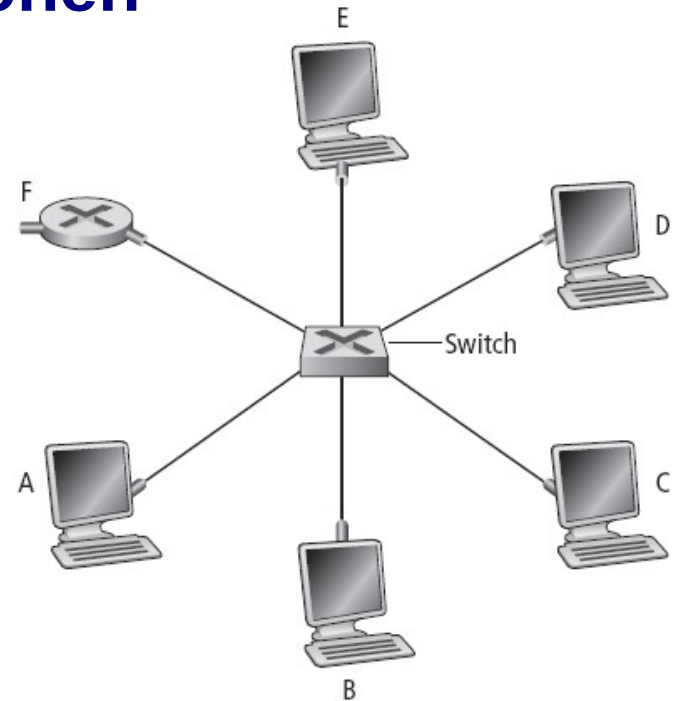
## ■ Plug-and-Play, selbst lernend

- Switches müssen nicht konfiguriert werden

# Switch: Gleichzeitige Übertragungen



- Jeder Host hat einen eigenen Link zum Switch, mit evtl. Kollisionen
- Switching:  
E-nach-B und  
D-nach-A gleichzeitig  
und ohne Kollisionen  
möglich



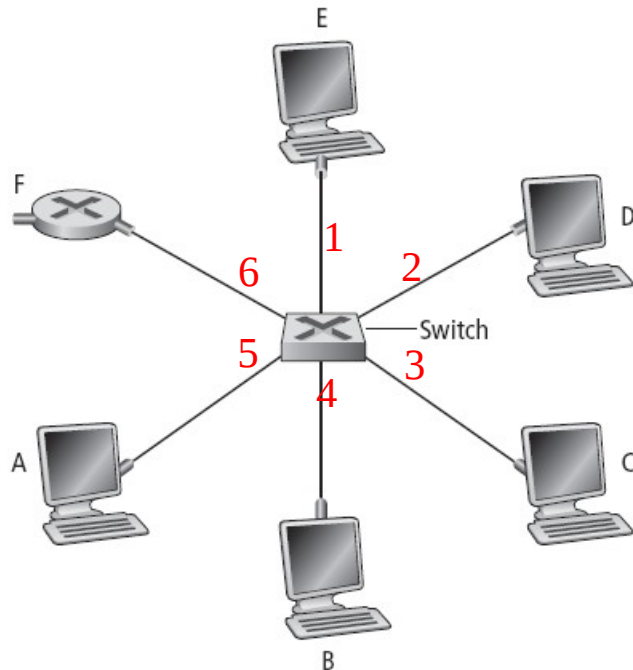


# Switch: selbst lernend

- Ein Switch lernt, welche Hosts er über eine gegebene Schnittstelle erreichen kann:

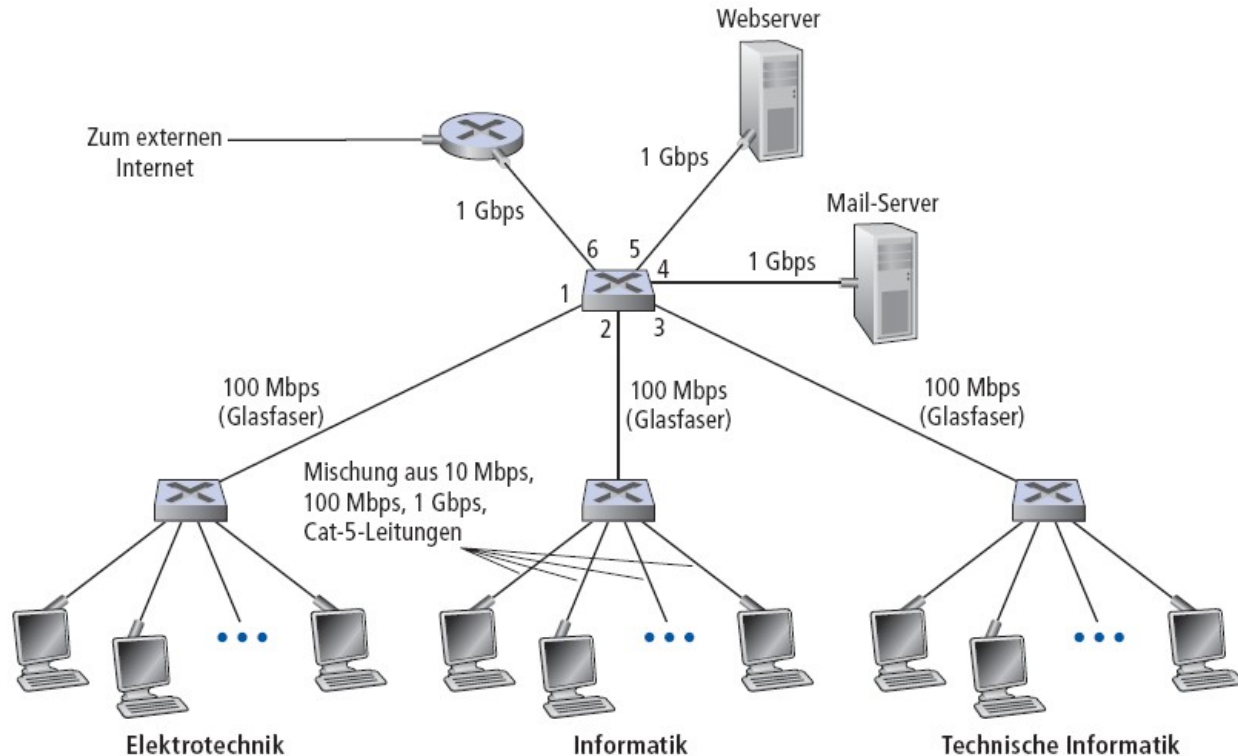
- Wenn er einen Rahmen empfängt, dann lernt der Switch, dass der Absender hinter dieser Schnittstelle liegen muss
- Er trägt diese Information in die Switch-Tabelle ein

- Beispiel: A schickt einen Rahmen an D



MAC-Adr.	Schnitt.	TTL
A	5	60

# Switches in einer komplexeren Umgebung

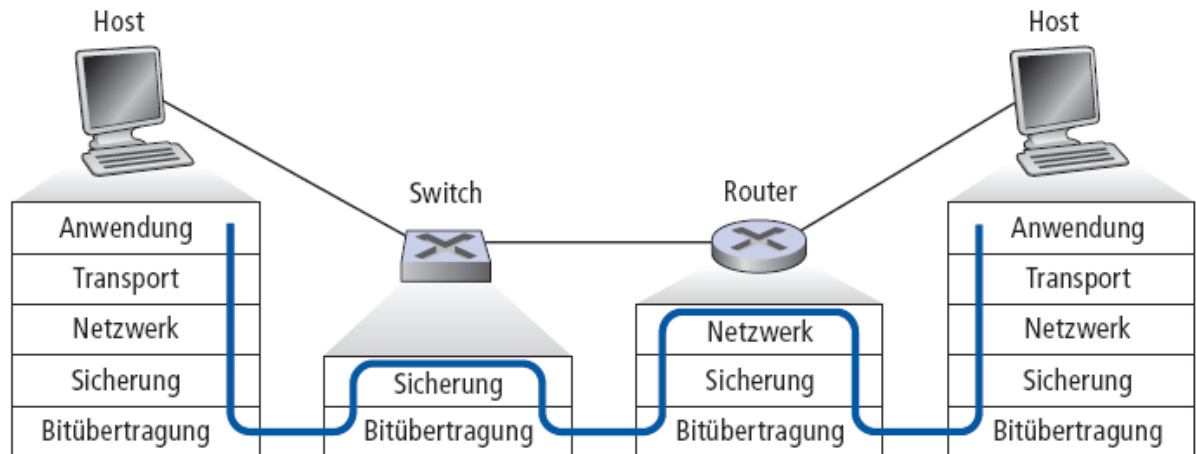


- Wie füllen die Switches in einer solchen Umgebung ihre Tabellen?  
Selbst lernend, genau wie bereits besprochen!

# Vergleich Switch und Router



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





# Zusammenfassender Vergleich

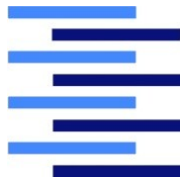
	Hubs	Router	Switches
Isolierung von Verkehr	nein	ja	ja
Plug-and-Play	ja	nein	ja
Optimales Routing	nein	ja	nein





# Gliederung der Vorlesung

- Einführung und Historie des Internets
- Schichtenmodell
- Netzwerk als Infrastruktur
- Layer 7: Anwendungsschicht
- Layer 5: Sitzungsschicht
- Layer 4: Transportschicht
- Layer 3: Netzwerkschicht
- Layer 2: Sicherungsschicht
  - Kabelgebunden im LAN
  - Funkverbindungen im WLAN



# Drahtlose und Mobile Netze

- **Rechnernetze: Laptops, Palmtops, PDAs und Internet-Telefone versprechen jederzeit problemlosen Internetzugang**
- **Zwei wichtige – aber verschiedene – Herausforderungen:**
  - Drahtlos:  
Kommunikation über drahtlose Links
  - Mobil:  
Umgang mit mobilen Benutzern, die ihren Zugangspunkt zum Netzwerk wechseln



# Drahtlose Netze

## **Drahtlose Kommunikationsnetze erleben wir allgegenwärtig:**

- Leuchttürme, Morsen, Buschtrommeln, opt. Telegraphen, ...
- Fernbedienungen an Heimgeräten
- Satellitenkommunikation
- Mobiltelefone: A/B/C/D/E-Netze, Dect, 3G (UMTS)
- Funknetze: Richtfunk, WLAN, Hiperlan, Bluetooth
- Optische Übertragungen: Infrarot (Links, IrDA), LaserLinks

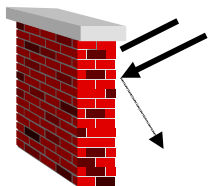
## **Die Techniken drahtloser Netze sind speziell ausgeprägt durch das Medium Luft und der Regulierung!**



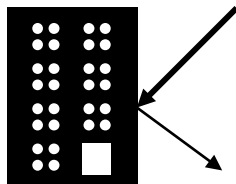
# Signalausbreitung

Ausbreitung im freien Raum grundsätzlich geradlinig wie das Licht

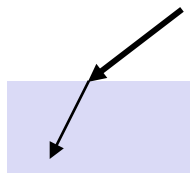
■ Empfangsleistung nimmt mit  $1/d^2$  ab



Abschattung



Reflexion



Refraktion



Streuung

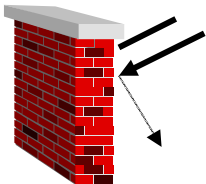


Beugung

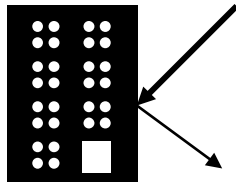


# Empfangsleistung

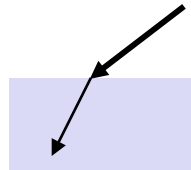
- Freiraumdämpfung (frequenzabhängig)
- Abschattung durch Hindernisse
- Reflexion an großen Flächen
- Refraktion in Abhängigkeit der Dichte eines Mediums
- Streuung (Scattering) an Hindernissen
- Beugung (diffraction) an scharfen Kanten



Abschattung



Reflexion



Refraktion



Streuung



Beugung



# Signalausbreitungsbereiche

## Übertragungsbereich

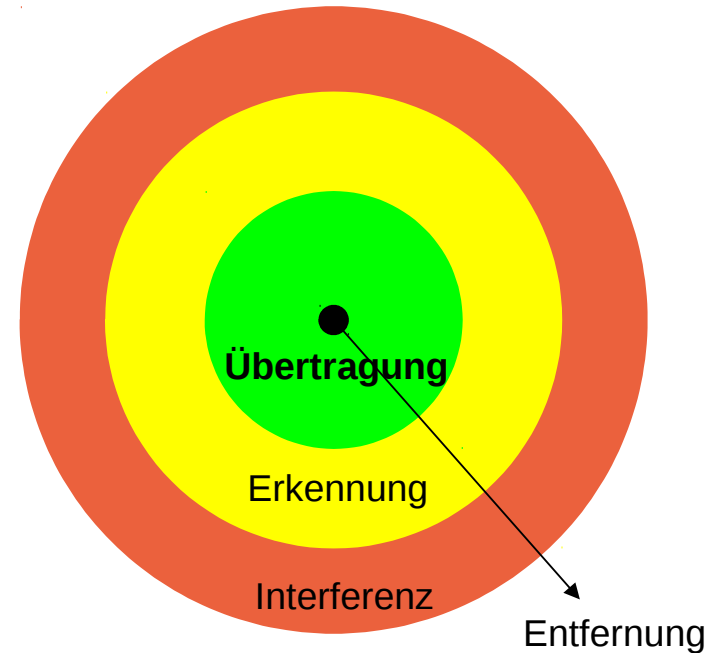
- Kommunikation möglich
- niedrige Fehlerrate

## Erkennungsbereich

- Signalerkennung
- keine Kommunikation möglich

## Interferenzbereich

- Signal kann nicht detektiert werden
- Signal trägt zum Hintergrundrauschen bei





# Medienzugriffsverfahren

**Beschränkte Frequenzbänder bedingen geteiltes Medium ‚Luft‘ → nicht homogen**

- Signalstärke nimmt quadratisch mit der Entfernung ab
- Sender können einander übertönen
- **Kollisionsvermeidung, wenn zwei oder mehr Knoten gleichzeitig senden wollen**
  - CSMA – erst prüfen, dann senden
  - Aber keine Kollisionserkennung, weil das von anderen empfangene Signal schwach ist



# Medienzugriffsverfahren (2)

**Andere Zugriffsverfahren werden benötigt,  
z.B. Multiplexing:**

- SDMA (Space Division Multiple Access)
- FDMA (Frequency Division Multiple Access)
- TDMA (Time Division Multiple Access)
- CDMA (Code Division Multiple Access)



# CDMA

## Code Division Multiple Access

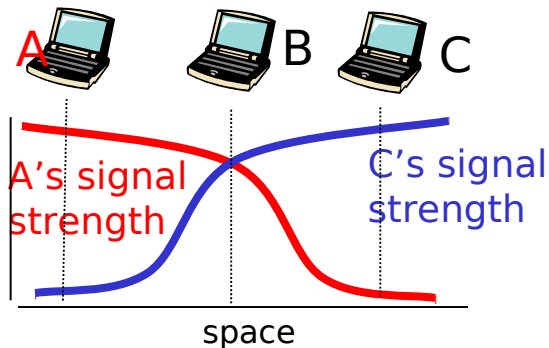
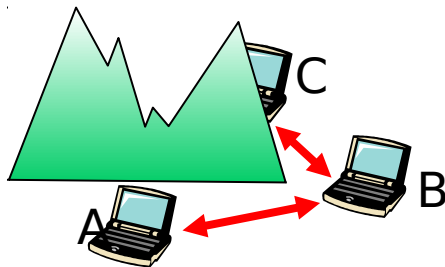


- Wird in mehreren Standards für Netze mit drahtlosen Broadcast-Kanälen verwendet (zellulärer Mobilfunk, Satelliten,...)
- Jedem Benutzer wird ein individueller “Code” == „Chipping Sequenz“ zugeordnet
  - Codiertes Signal =  
(Originaldaten) X (Chipping Sequenz)
- Erlaubt es mehreren Benutzern gleichzeitig mit minimaler Interferenz auf dem selben Kanal zu übertragen

# IEEE 802.11: Mehrfachzugriff



- Es gibt Fälle, in denen Kollisionen nicht bemerkt werden können: Hidden Terminal, Signalabschwächung
  - Ziel: *Kollisionsvermeidung*: CSMA/C(ollision)A(voidance)





# MA/CA - Kollisionsvermeidung

MACA (Multiple Access with Collision Avoidance) setzt kurze Signalisierungspakete zur Kollisionsvermeidung ein

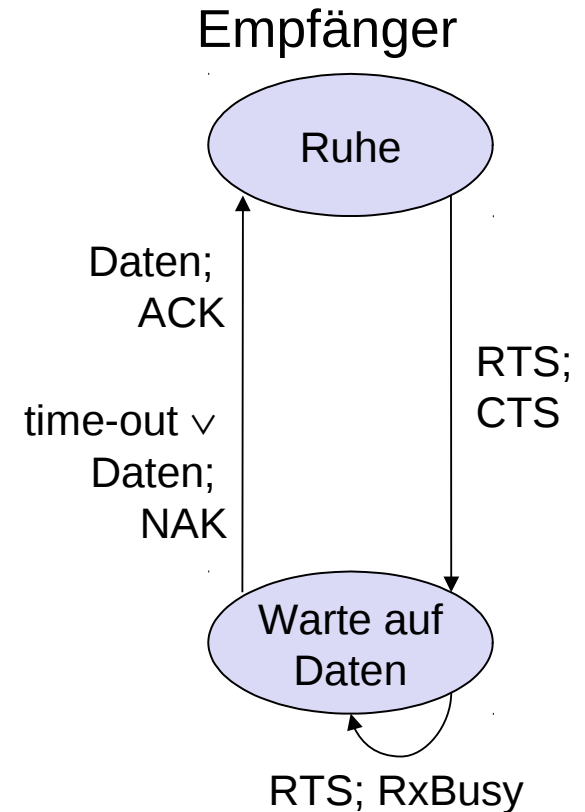
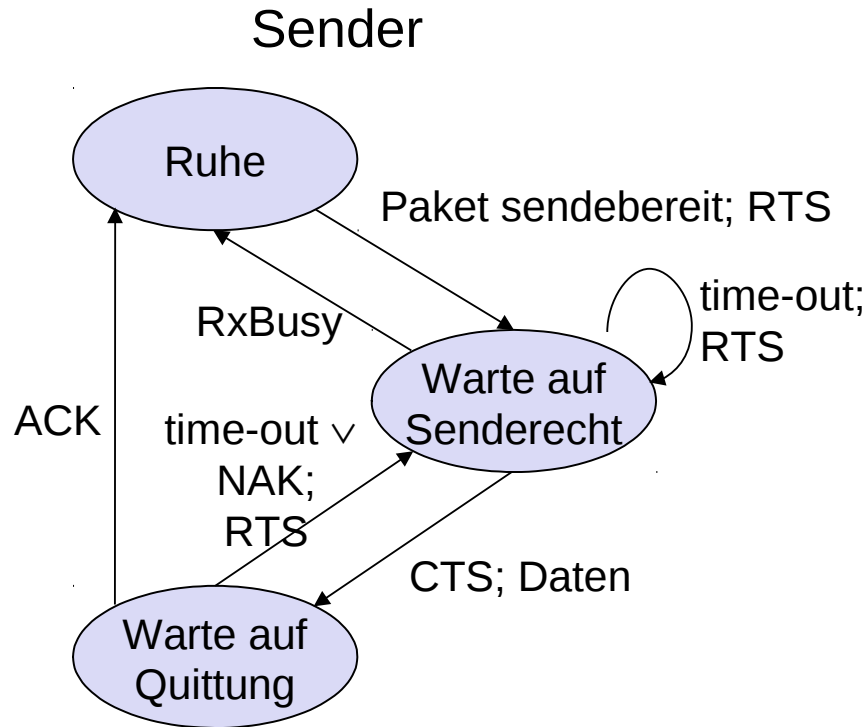
- RTS (request to send): Anfrage eines Senders an einen Empfänger, bevor ein Paket gesendet werden kann
- CTS (clear to send): Bestätigung des Empfängers sobald er empfangsbereit ist

Signalisierungspakete beinhalten:

- Senderadresse
- Empfängeradresse
- Paketgröße

Varianten dieses Verfahrens finden in IEEE802.11 als DFWMAC (Distributed Foundation Wireless MAC) Einsatz

# MACA-Variante: DFWMAC in IEEE802.11



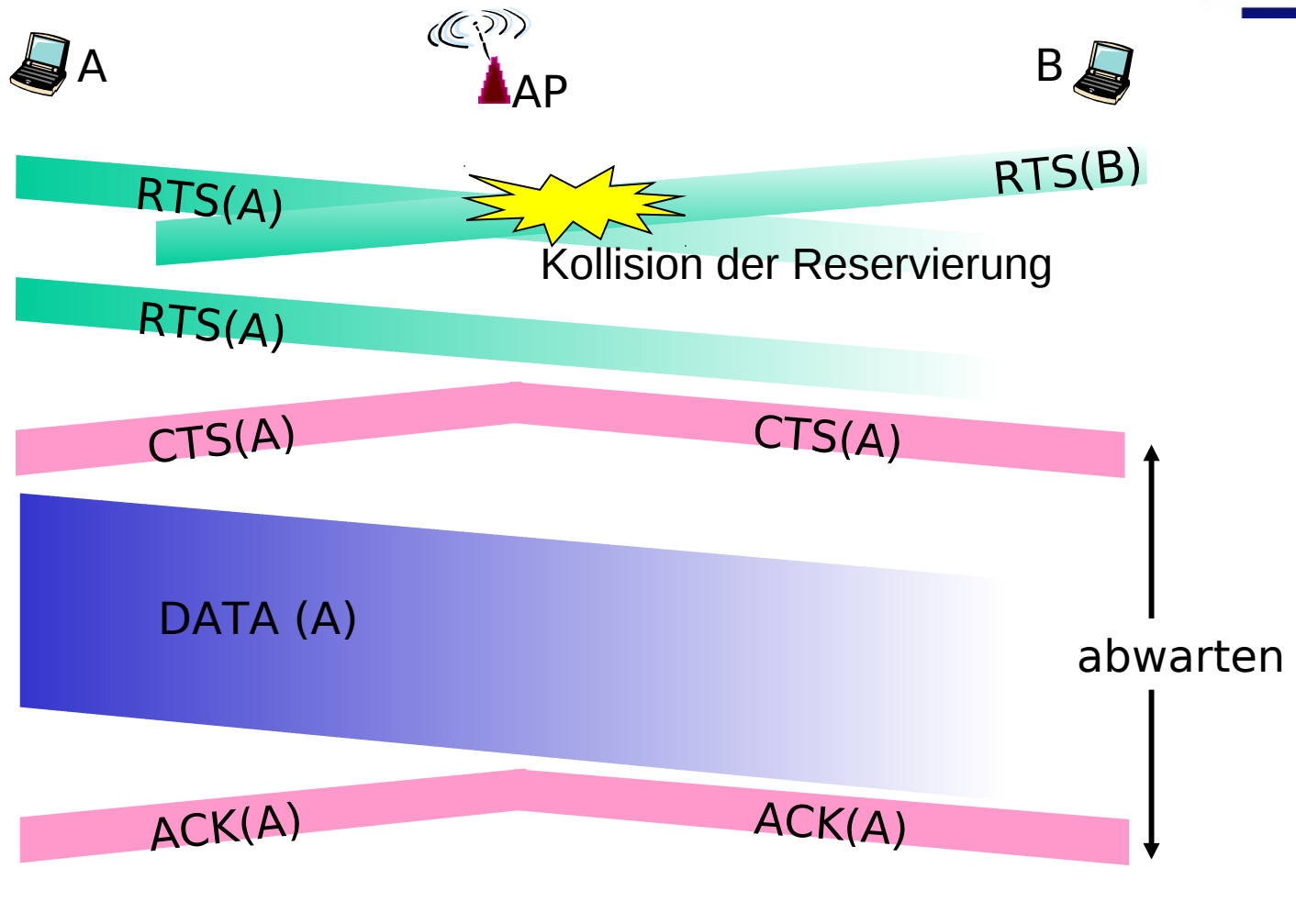
ACK: positive Empfangsbestätigung  
NAK: negative Empfangsbestätigung  
RxBusy: Empfänger beschäftigt

# MACA-Variante: DFWMAC in IEEE802.11 (2)



- **Sender hat Kanal auch für lange Rahmen “reserviert”!**
  - Der Sender überträgt zunächst kurze Request-to-Send-Rahmen (RTS) an die BS
  - RTS-Rahmen können immer noch kollidieren – aber geringes Risiko
- **BS schickt einen Clear-to-Send-Rahmen (CTS) mittels Broadcast als Antwort**
- **alle Knoten hören das RTS und/oder das CTS**
  - Sender sendet seine Daten

# Kollisionsvermeidung: RTS/CTS





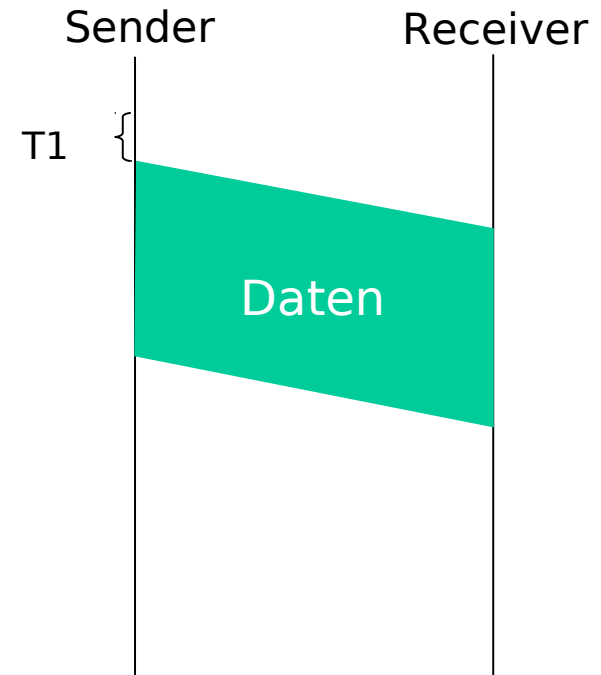
# IEEE 802.11 MAC: CSMA/CA

## ■ 802.11-Sender

- Wenn der Kanal für eine bestimmte Dauer frei ist, dann sende alle Daten

### ansonsten:

- starte zufälligen Backoff-Timer, der runterzählt, wenn der Kanal frei ist
- übertrage, sobald der Timer ausläuft
- warte auf ACK

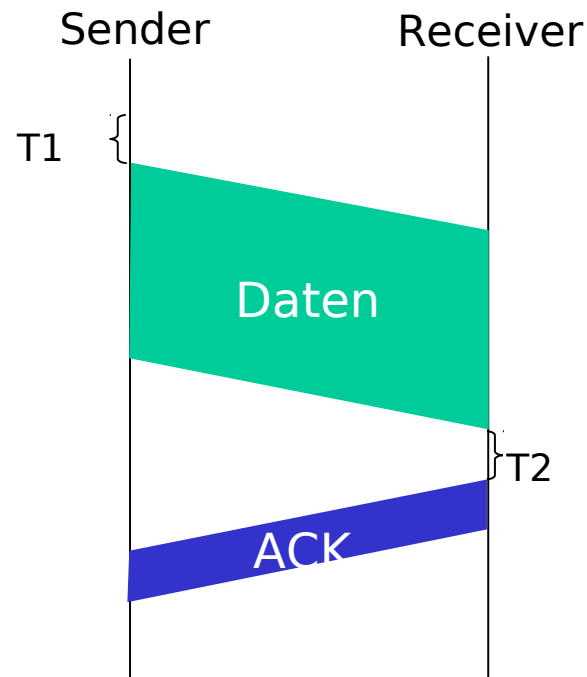




# IEEE 802.11 MAC: CSMA/CA

## ■ 802.11-Empfänger

- Wenn ein Rahmen korrekt empfangen wurde, antworte mit einem ACK
- Warte vorher für bestimmte Dauer







# IEEE 802.11 Wireless LAN

## □ 802.11b

- 2.4-5 GHz unlizensiertes Spektrum
- bis zu 11 Mbps
- Direct Sequence Spread Spectrum (DSSS) auf der Bitübertragungsschicht
  - Alle Hosts benutzen dieselbe Chipping-Sequenz

## □ 802.11a

- 5-6 GHz
- bis zu 54 Mbps

## □ 802.11g

- 2.4-5 GHz
- bis zu 54 Mbps

## □ 802.11n: mehrere Antennen

- 2.4-5 GHz
- bis zu 200 Mbps

- alle verwenden CSMA/CA für den Mehrfachzugriff
- alle haben Infrastruktur- und Ad-Hoc-Modi



# Taxonomie drahtloser Netzwerke

	Single-Hop	Multihop
Infrastruktur (z.B. APs)	Host verbinden sich mit Basisstation(en) (WLAN, WiMAX, Mobilfunk,...), die sie an den Backbone anbinden	Hosts müssen gegebenenfalls über mehrere Zwischenstationen kommunizieren, um das Internet zu erreichen (Mesh-Netzwerke)
infrastrukturlos	Keine Basisstationen, keine Anbindung an das Internet (Bluetooth, Ad Hoc Netze)	keine Basisstationen, keine Internetanbindung; Routing über Relays kann je nach Ziel nötig sein (MANET, VANET)



# Kontakt

**Prof. Dr. Klaus-Peter Kossakowski**

**Email: klaus-peter.kossakowski  
@haw-hamburg.de**

**Mobil: +49 171 5767010**

**<https://users.informatik.haw-hamburg.de/~kpk/>**