

## 6. Foliensatz Computernetze

Prof. Dr. Christian Baun

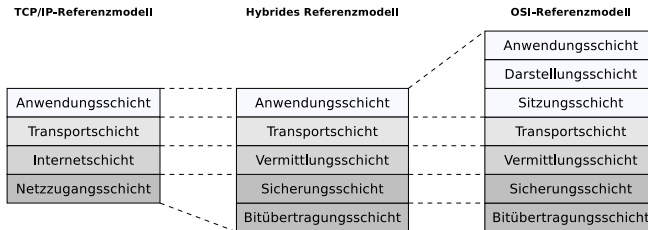
Frankfurt University of Applied Sciences  
(1971–2014: Fachhochschule Frankfurt am Main)  
Fachbereich Informatik und Ingenieurwissenschaften  
[christianbaun@fb2.fra-uas.de](mailto:christianbaun@fb2.fra-uas.de)

# Lernziele dieses Foliensatzes

- Sicherungsschicht (Teil 3)
  - Medienzugriffsverfahren
    - Medienzugriffsverfahren bei Ethernet
    - Medienzugriffsverfahren bei WLAN
  - Adressauflösung mit ARP

# Sicherungsschicht

- Aufgaben der Sicherungsschicht (Data Link Layer):
  - Sender: Pakete der Vermittlungsschicht in Rahmen (Frames) verpacken
  - Empfänger: Rahmen im Bitstrom der Bitübertragungsschicht erkennen
  - Korrekte Übertragung der Rahmen innerhalb eines physischen Netzes gewährleisten durch Fehlererkennung mit Prüfsummen
  - Physische Adressen (MAC-Adressen) bereitstellen
  - Zugriff auf das Übertragungsmedium regeln



- Geräte: Bridge, Layer-2-Switch (Multiport-Bridge), Modem
- Protokolle: Ethernet, Token Ring, WLAN, Bluetooth, PPP

100

- Bei Ethernet 10BASE2/5 und WLAN verwenden die Netzwerkgeräte bzw. Stationen ein gemeinsames Übertragungsmedium
  - Um den Medienzugriff zu koordinieren und Kollisionen zu vermeiden, sind Medienzugriffsverfahren nötig
    - Ethernet verwendet das Medienzugriffsverfahren **CSMA/CD**
    - WLAN verwendet das Medienzugriffsverfahren **CSMA/CA**
- Bluetooth wird hier nicht behandelt, da sich Bluetooth-Geräte in **Piconetzen** organisieren
  - In jedem Piconetz koordiniert ein Master den Medienzugriff

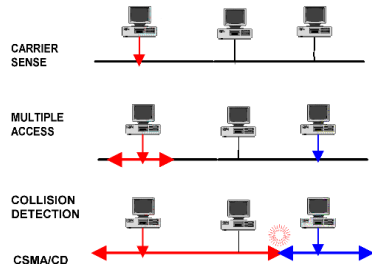
- Anders als bei Token Ring sind bei Ethernet die **Wartezeit** und **übertragbare Datenmenge** nicht eindeutig vorhersagbar
- Alle Teilnehmer stehen in Bezug auf den Medienzugriff im **direktem Wettbewerb**
- Wartezeit und Datenmenge hängen ab von...
  - der Anzahl der Teilnehmer und
  - der Datenmenge, die die einzelnen Teilnehmer versenden
- Ethernet verwendet das Medienzugriffsverfahren Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

Bildquelle: <http://www.payer.de/cmc/cmcs08.htm>

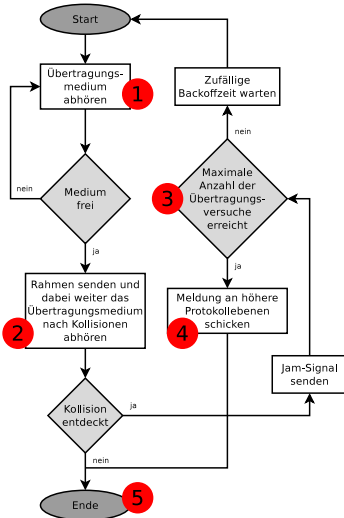
- Jedes Netzwerkgerät hört vor dem Senden den Kanal ab, und sendet nur dann, wenn der Kanal frei ist
- Die Netzwerkgeräte können also zwischen einer freien und einer besetzten Verbindungsleitung unterscheiden

- Alle Netzwerkgeräte greifen auf dasselbe Übertragungsmedium konkurrierend zu

- Jedes Netzwerkgerät hört auch während des Sendens den Kanal ab, um auftretende Kollisionen zu entdecken und wenn nötig eine Fehlerbehandlung durchzuführen

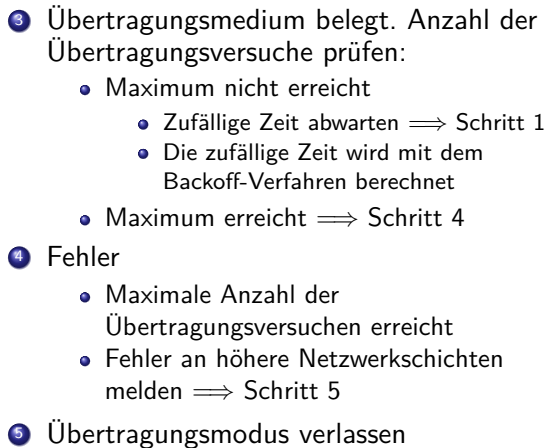


Bildquelle: Wikipedia



- Will ein Netzwerkgerät via Ethernet Datenrahmen übertragen, hält es folgenden Ablauf ein
- 1 Übertragungsmedium überwachen
  - Übertragungsmedium frei  $\implies$  Schritt 2
  - Übertragungsmedium belegt  $\implies$  Schritt 3
- 2 Rahmen senden und Übertragungsmedium weiter abhören
  - Erfolgreiche Übertragung
    - Erfolgsmeldung an höhere Netzwerkschichten melden  $\implies$  Schritt 5
  - Kollision wird entdeckt
    - Sendevorgang abbrechen und das 48 Bits lange Störsignal (*Jam-Signal*) senden, um die Kollision bekannt zu geben  $\implies$  Schritt 3

Bildquelle: Wikipedia







# Netzwerkausdehnung und Kollisionserkennung

- Eine Kollision muss vom Sender erkannt werden
  - Es ist wichtig, dass ein Rahmen **noch nicht** fertig gesendet ist, wenn es zur Kollision kommt
    - Sonst ist das sendende Netzwerkgerät vielleicht schon mit dem Aussenden des Rahmens fertig und nimmt eine erfolgreiche Übertragung an
- Jeder Rahmen muss eine gewisse **Mindestlänge** haben
  - Diese muss so dimensioniert sein, dass die Übertragungsdauer für einen Rahmen minimaler Länge, die maximale RTT (Round Trip Time) nicht unterschritten wird
    - RTT ist die Zeit, die ein Rahmen benötigt, um vom einen Ende des Netzes zum weitest entfernten anderen Ende des Netzes und wieder zurück zu gelangen
  - **So ist sichergestellt, dass sich eine Kollision noch bis zum Sender ausbreiten kann, ohne dass dieser mit dem Senden fertig ist**
    - Erkennt der Sender eine Kollision, weiß er, dass sein Rahmen nicht richtig beim Empfänger angekommen ist, und kann es später erneut versuchen

Ethernet definiert eine maximale Netzwerkausdehnung und eine minimale Rahmenlänge

Mindestlänge der Rahmen bei Ethernet: 64 Bytes

Die maximale Länge des physischen Netzes hängt vom verwendeten Ethernet-Standard ab

# Minimale Rahmenlänge und Kollisionserkennung (Beispiel)

- Für Ethernet ist eine maximal zulässige Netzwerkausdehnung und eine minimale Rahmenlänge festgelegt
- Um die **minimale Rahmenlänge** zu berechnen, bei der die Kollisionserkennung noch möglich ist, gilt:

$$P = 2 * U * \frac{D}{V}$$

$P$  = Minimale Rahmenlänge in Bits

$U$  = Datenübertragungsgeschwindigkeit des Übertragungsmediums in Bits pro Sekunde

$D$  = Länge des Netzes in Metern

$V$  = Signalgeschwindigkeit auf dem Übertragungsmedium in Metern pro Sekunde

- Rechenbeispiel für 10BASE5 mit 10 MBit/s und Koaxialkabeln:

- $U = 10 \text{ MBit/s} = 10.000.000 \text{ Bits/s}$
- $D = 2.500 \text{ m}$  (das ist die Maximallänge für 10BASE5)
- $V = \text{Lichtgeschwindigkeit} * \text{Ausbreitungsfaktor}$ 
  - Lichtgeschwindigkeit =  $299.792.458 \text{ m/s}$
  - Ausbreitungsfaktor =  $0,77$  für Koaxialkabel
  - $V = 299.792.458 \text{ m/s} * 0,77 \approx 231.000.000 \text{ m/s}$

$$P = 2 * 10 * 10^6 \text{ Bits/s} * \frac{2.500 \text{ m}}{231 * 10^6 \text{ m/s}} \approx 217 \text{ Bits} \approx 28 \text{ Bytes}$$

- Schlussfolgerung: Die minimale Rahmenlänge von 64 Bytes bei Ethernet ist mehr als ausreichend

# Ausbreitungsfaktor

- Der **Ausbreitungsfaktor**, der auch Verkürzungsfaktor heißt, hängt vom Übertragungsmedium ab und ist:
  - 1 für Vakuum
  - 0,64 für Twisted-Pair-Kabel Cat-5e
  - 0,66 für Koaxialkabel RG-58 ( $\implies$  Ethernet 10BASE2)
  - 0,67 für Glasfaser
  - 0,77 für Koaxialkabel RG-8 ( $\implies$  Ethernet 10BASE5)
- Beschreibt die Signalgeschwindigkeit in einem Übertragungsmedium in Relation zur Lichtgeschwindigkeit

# Netzwerkausdehnung und Kollisionserkennung (Beispiel)

- Um die **maximale Ausdehnung** zwischen zwei Netzwerkgeräten zu berechnen, bei der die Kollisionserkennung noch funktioniert, gilt:

$$2 * S_{max} = V * t_{Rahmen}$$

$S_{max}$  = Maximale Ausdehnung mit Kollisionserkennung

$V$  = Signalgeschwindigkeit auf dem Übertragungsmedium in Metern pro Sekunde

$t_{Rahmen}$  = Übertragungsdauer eines Rahmens in Sekunden

- Rechenbeispiel für 10BASE5 mit 10 MBit/s und Koaxialkabeln:
  - $V = 231.000.000 \text{ m/s} = 231 * 10^6 \text{ m/s}$
  - Übertragungsdauer  $t_{Rahmen}$  = Übertragungsdauer für ein Bit multipliziert mit der Anzahl der Bits in einem Rahmen ( $\Rightarrow 512 \text{ Bits} = 64 \text{ Byte}$ )
    - Die Übertragungsdauer für ein Bit bei 10 MBit/s ist 0,1 Mikrosekunden
    - Ein Rahmen mit der kleinsten erlaubten Rahmenlänge vom 64 Byte benötigt somit 51,2  $\mu\text{s}$ , um vollständig gesendet zu werden
  - Ein 51,2  $\mu\text{s}$  langer Rahmen legt im Koaxialkabel folgende Strecke zurück:
 
$$231 * 10^6 \frac{\text{m}}{\text{s}} * 51,2 * 10^{-6} \text{ s} = 11.827,20 \text{ m} = 11,83 \text{ km}$$
    - Schlussfolgerung: Bei einer maximal erlaubten Ausdehnung von 2,5 km ist Kollisionserkennung möglich

# CSMA/CD heute

- Das Medienzugriffsverfahren **CSMA/CD** ist nur bei Ethernet mit der **Bus-Topologie zwingend nötig**
  - Grund: Dort sind alle Netzwerkgeräte direkt mit einem gemeinsamen Medium verbunden
- Fast alle auf Ethernet basierenden Netze sind heute **vollständig geswitcht** und darum **frei von Kollisionen**

# Medienzugriffsverfahren CSMA/CA bei Wireless LAN

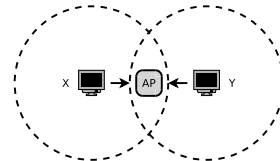
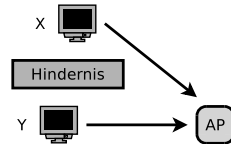
- CSMA/CD versagt bei Funknetzen
- Bei CSMA/CD stellt der Sender auftretende Kollisionen fest
  - Bei kabelgebundenen Netzen mit gemeinsamem Übertragungsmedium empfängt jeder Teilnehmer die Übertragungen aller anderer Teilnehmer
    - Darum bekommt auch jeder Teilnehmer jede Kollision mit
  - Bei Funknetzen wie WLAN ist das nicht immer der Fall
    - Aus diesem Grund will man das Entstehen von Kollisionen mit dem Medienzugriffsverfahren *Carrier Sense Multiple Access / Collision Avoidance* (CSMA/CA) **minimieren**
- Spezielle Eigenschaften des Übertragungsmediums führen bei Funknetzen zu unerkannten Kollisionen beim Empfänger
  - **Hidden-Terminal-Problem**
  - **Fading**

Auch PowerLAN bzw. Powerline verwendet CSMA/CA als Medienzugriffsverfahren

Quelle: Analysis of CSMA/CA used in Power Line Communication. *Martin Koutny, Petr Mlynek, Jiri Misurec*. IEEE (2013)

# Spezielle Eigenschaften des Übertragungsmediums

- **Hidden-Terminal-Problem** (verursacht durch unsichtbare/versteckte Endgeräte)
  - X und Y senden an die Basisstation (Access Point)
  - Wegen Hindernissen können die Stationen X und Y ihre Übertragungen gegenseitig nicht erkennen, obwohl sie an der Basisstation interferieren
- **Fading** (abnehmende Signalstärke)
  - X und Y senden an die Basisstation
  - Die elektromagnetischen Wellen werden durch Hindernisse und im freien Raum allmählich abgeschwächt
  - Durch die Positionen der Stationen X und Y zueinander sind deren Signale zu schwach, als dass sie ihre Übertragungen gegenseitig wahrnehmen können





# WLAN (802.11) kennt drei verschiedene Medienzugriffsverfahren

## ❶ CSMA/CA

- Vorgehensweise: „erst hören, dann sprechen“ (*listen before talk*)
- Kollisionsvermeidung durch zufällige Backoffzeit
- Mindestabstand zwischen aufeinanderfolgenden Rahmen
- Empfangsbestätigung durch ACK (nicht bei Broadcast)
- Standardmäßiges Medienzugriffsverfahren bei WLAN und bei allen WLAN-Geräten implementiert

## ❷ CSMA/CA RTS/CTS (Request To Send/Clear To Send)

- Vermeidung des Problems versteckter Endgeräte
- Optional und meistens implementiert

## ❸ CSMA/CA PCF (Point Coordination Function)

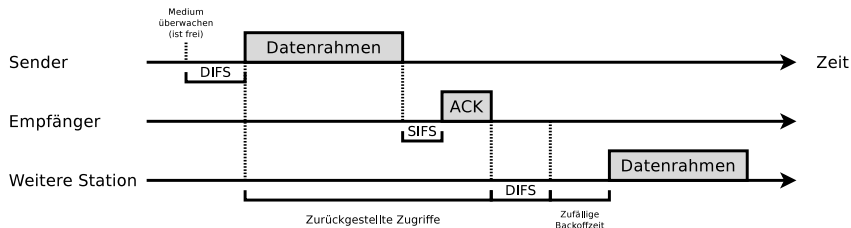
- Access Point steuert den Medienzugriff zentral
- Optional und selten implementiert

# Übertragung von Rahmen

- Erkennt bei CSMA/CD (Ethernet) ein sendender Teilnehmer eine Kollision, bricht er das Senden des Rahmens ab
- WLAN verwendet aber keine Kollisionserkennung, sondern mit CSMA/CA eine **Kollisionsvermeidung** (eigentlich ist es nur eine **Kollisionsminimierung**)
  - Hat eine Station mit dem Senden eines Rahmens begonnen, überträgt sie den vollständigen Rahmen in jedem Fall
    - Hat eine Station einmal mit dem Senden begonnen gibt kein Zurück
  - Der Sender muss darum erkennen können, wenn ein Rahmen nicht korrekt beim Empfänger angekommen ist
    - Lösung: Der Empfänger bestätigt den korrekten Empfang des Rahmens mit **ACK**

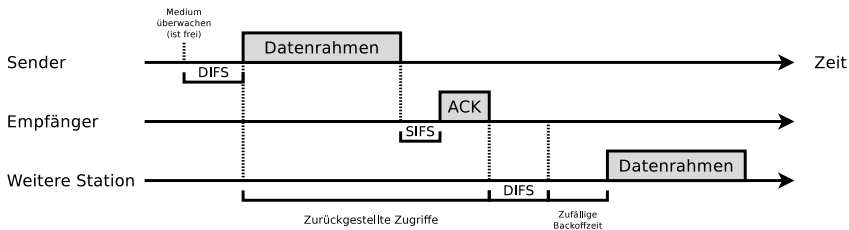
# Ablauf von CSMA/CA – 1/5

- Zuerst *horcht* der Sender am Übertragungsmedium ( $\implies$  Carrier Sense)
- Das Medium muss für einen kurzen Zeitraum frei sein
  - Der Zeitraum heißt **Distributed Interframe Spacing (DIFS)**  $\approx 50\mu s$
- Ist das Medium einen DIFS lang frei, kann der Sender einen Rahmen aussenden



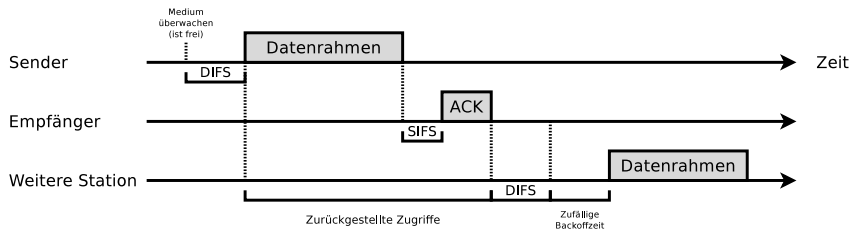
## Ablauf von CSMA/CA – 2/5

- Empfängt eine Station einen Rahmen, der die CRC-Prüfung besteht, wartet sie einen kurzen Zeitraum ab
  - Der Zeitraum heißt **Short Interframe Spacing (SIFS)**  $\approx 10\mu s$
  - Danach sendet der Empfänger einen **Bestätigungsrahmen (ACK)**
- DIFS und SIFS garantieren bei CSMA/CA einen Mindestabstand zwischen aufeinanderfolgenden Rahmen



# Ablauf von CSMA/CA – 3/5

- Nach Ablauf eines weiteren DIFS mit freiem Übertragungsmedium wird eine **Backoffzeit** berechnet
  - Die Backoffzeit wird berechnet, indem ein zufälliger Wert zwischen minimalem und maximalem Wert des **Contention Window** bestimmt wird, und dieser zufällige Wert wird mit der **Slot Time** multipliziert
    - Nach dem Ablauf der Backoffzeit wird der Rahmen gesendet



Quelle: Grundkurs Computernetzwerke, Jürgen Scherff, Vieweg + Teubner (2010)

Belegt während der Backoffzeit eine andere Station das Übertragungsmedium, wird der Zähler so lange angehalten, bis das Medium mindestens ein DIFS lang wieder frei ist.

# Ablauf von CSMA/CA – 4/5

- Der minimale und maximale Wert des CW sowie die Slot Time hängen vom verwendeten Modulationsverfahren ab und sind fest vorgegeben

Modulationsverfahren	SIFS	DIFS <sup>1</sup>	Slot Time	Minimales CW	Maximales CW
FHSS (802.11)	28 $\mu$ s	128 $\mu$ s	50 $\mu$ s	15	1023
DSSS (802.11b)	10 $\mu$ s	50 $\mu$ s	20 $\mu$ s	31	1023
OFDM (802.11a/h/n/ac)	16 $\mu$ s	34 $\mu$ s	9 $\mu$ s	15	1023
OFDM (802.11g) <sup>2</sup>	16 $\mu$ s	34 $\mu$ s	9 $\mu$ s	15	1023
OFDM (802.11g) <sup>3</sup>	10 $\mu$ s	50 $\mu$ s	20 $\mu$ s	15	1023

<sup>1</sup> DIFS = SIFS + 2 \* Slot Time

<sup>2</sup> Mit Unterstützung für Übertragungsraten 1-54 Mbit/s

<sup>3</sup> Mit ausschließlicher Unterstützung für Übertragungsraten > 11 Mbit/s

- Die untere und obere Schranke des CW sind immer Zweierpotenzen, wobei vom Ergebnis der Wert 1 abgezogen wird
  - Verwendet ein WLAN z.B. das Modulationsverfahren OFDM ist beim...
    - 1. Sendeversuch das CW ein Wert  $\geq 15$  und  $\leq 31$
    - 2. Sendeversuch das CW ein Wert  $\geq 31$  und  $\leq 63$
    - 3. Sendeversuch das CW ein Wert  $\geq 63$  und  $\leq 127$

# Ablauf von CSMA/CA – 5/5

Modulationsverfahren	SIFS	DIFS <sup>1</sup>	Slot Time	Minimales CW	Maximales CW
FHSS (802.11)	28 $\mu$ s	128 $\mu$ s	50 $\mu$ s	15	1023
DSSS (802.11b)	10 $\mu$ s	50 $\mu$ s	20 $\mu$ s	31	1023
OFDM (802.11a/h/n/ac)	16 $\mu$ s	34 $\mu$ s	9 $\mu$ s	15	1023
OFDM (802.11g) <sup>2</sup>	16 $\mu$ s	34 $\mu$ s	9 $\mu$ s	15	1023
OFDM (802.11g) <sup>3</sup>	10 $\mu$ s	50 $\mu$ s	20 $\mu$ s	15	1023

<sup>1</sup> DIFS = SIFS + 2 \* Slot Time

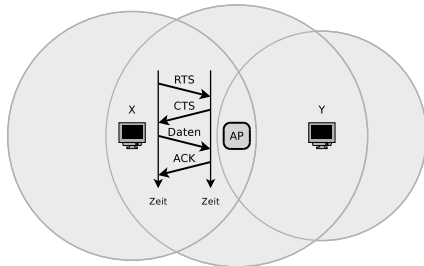
<sup>2</sup> Mit Unterstützung für Übertragungsraten 1-54 Mbit/s

<sup>3</sup> Mit ausschließlicher Unterstützung für Übertragungsraten > 11 Mbit/s

- Weitere Sendeversuche lassen den Wert von CW weiter exponentiell ansteigen, bis der maximale Wert erreicht ist
- Wurde ein Rahmen durch ACK bestätigt ( $\implies$  erfolgreiche Übertragung), wird die untere Schranke des CW wieder auf den Wert des minimalen CW in der Tabelle zurückgesetzt

# CSMA/CA RTS/CTS

- CSMA/CA verringert die Anzahl der Kollisionen
  - Es kann aber nicht alle Kollisionen vermeiden
- Eine **bessere Kollisionsvermeidung** ermöglicht CSMA/CA RTS/CTS
  - Sender und Empfänger tauschen zuerst **Kontrollrahmen** aus
    - Das informiert alle erreichbaren Stationen, dass demnächst eine Übertragung beginnt
  - Kontrollrahmen: **Request To Send (RTS)** und **Clear To Send (CTS)**
    - Beide Kontrollrahmen beinhalten ein Datenfeld, das die Belegungsdauer des Übertragungsmediums (des Kanals) angibt  $\Rightarrow$  siehe Folien 28 + 29



- Kollisionen sind nur während dem Senden von RTS- und CTS-Rahmen möglich
  - Wegen des Hidden-Terminal-Problems

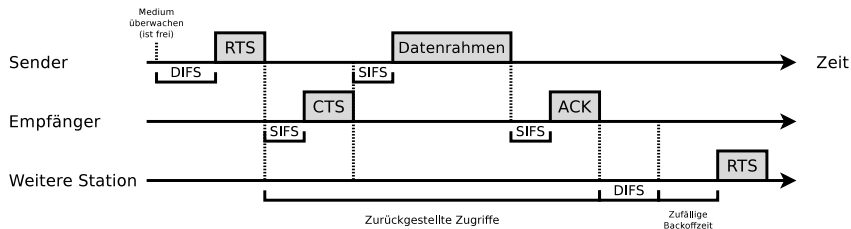
Abbildung auf der linken Seite. . .

Station Y kann nicht den RTS-Rahmen von X empfangen, aber den CTS-Rahmen der Basisstation (Access Point)



# Ablauf von CSMA/CA RTS/CTS – 1/3

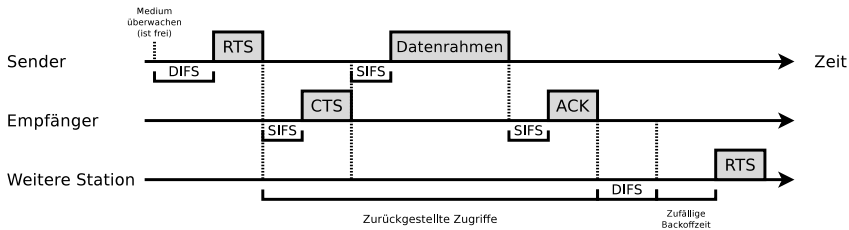
- Der Sender sendet nach dem DIFS einen **RTS**-Rahmen zum Empfänger
  - Der RTS-Rahmen enthält ein Feld, das angibt wie lange der Sender das Übertragungsmedium (den Kanal) zum Senden des Rahmens reservieren (benutzen) will



- Der Empfänger bestätigt die Reservierungsanfrage nach Abwarten des SIFS mit einem **CTS**-Rahmen, der ebenfalls die Belegungsdauer für das Übertragungsmedium enthält
  - Der Empfänger bestätigt somit die Belegungsdauer für den zu übertragenden Datenrahmen

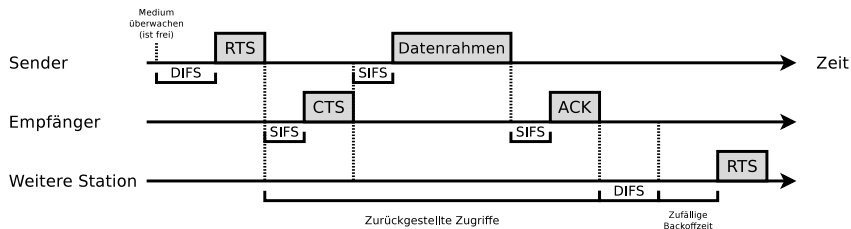
## Ablauf von CSMA/CA RTS/CTS – 2/3

- Nach dem erfolgreichem Erhalt des Datenrahmens, wartet der Empfänger ein SIFS und sendet ein ACK an den Sender



- Ist das Übertragungsmedium (der Kanal) belegt, finden bis zum Ablauf des Netzbelegungsvektors – **Network Allocation Vectors (NAV)** – keine weiteren Sendeversuche statt
  - Der NAV ist eine Zählvariable, die jede Station selbst verwaltet
    - Verringert die Anzahl der Kollisionen
    - Enthält die voraussichtliche Belegungszeit des Übertragungsmediums
    - Wird mit der Zeit dekrementiert, bis er den Wert 0 erreicht

# Ablauf von CSMA/CA RTS/CTS – 3/3



## • Vorteile:

- **Weniger Kollisionen**, weil es das Hidden-Terminal-Problem löst
- **Weniger Energieverbrauch**, weil keine Sendeveruche während des NAV

## • Nachteile:

- Reservierungen des Übertragungsmediums verursachen **Verzögerungen**
- RTS- und CTS-Rahmen sind **Overhead**

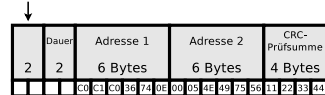


# WLAN Kontrollrahmen (Special Frames) – CTS-Rahmen

- Länge der **CTS-Rahmen**: 14 Bytes
- Mit einem CTS-Rahmen **bestätigt** eine Basisstation die **Reservierungsanfrage** für das Übertragungsmedium
- adresse = MAC-Adresse der Station, die die Reservierungsanfrage gesendet hatte

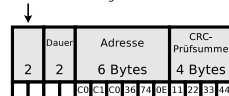
## RTS-Rahmen

Rahmensteuerung



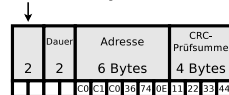
## CTS-Rahmen

Rahmensteuerung



## ACK-Rahmen

Rahmensteuerung

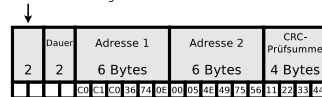


# WLAN Kontrollrahmen (Special Frames) – ACK-Rahmen

- Länge der **ACK-Rahmen**: 14 Bytes
- Mit einem ACK-Rahmen **bestätigt** der Empfänger die **erfolgreiche Übertragungen eines Rahmens** beim Sender
- adresse = MAC-Adresse der Station, die den Rahmen erfolgreich übertragen hat

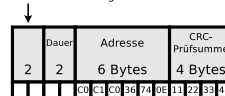
## RTS-Rahmen

Rahmensteuerung



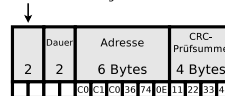
## CTS-Rahmen

Rahmensteuerung



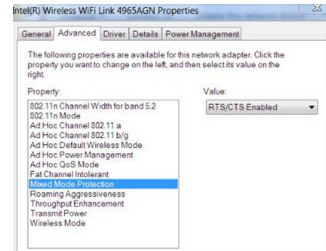
## ACK-Rahmen

Rahmensteuerung



# CSMA/CA RTS/CTS in der Praxis

- CSMA/CA RTS/CTS ist bei WLAN optional und meistens implementiert
  - Es wird in der Praxis zur Reservierung von Kanälen zur Übertragung langer Datenrahmen verwendet
- Man kann für jede Station einen RTS-Schwellenwert festlegen (Treiber?! )
  - So definiert man, dass RTS/CTS nur dann verwendet wird, wenn ein Rahmen länger ist, als der Schwellenwert groß ist
- Häufig ist der voreingestellte Schwellenwert größer als die maximale Rahmenlänge (2.346 Bytes) bei IEEE 802.11
  - Die RTS/CTS-Sequenz wird dann für alle gesendeten Datenrahmen weggelassen



Bildquelle: <http://www.itedge.net>

## Advanced Wireless Settings

☒ Enable wireless radio

802.11 Mode: 802.11g only

2.4GHz Preamble: auto(long)

RTS/CTS Threshold: 2346 (256 - 2346, default 2346)

Screenshot from the web gui of a Netgear WGPS606 wireless router

Quelle: Computernetzwerke, James F. Kurose, Keith W. Ross, Pearson (2008)

# CSMA/CA PCF

- **PCF = Point Coordination Function**
- Die Basisstation (Access Point) steuert den Medienzugriff zentral
  - Sie fordert die angemeldeten Stationen zum Senden von Datenrahmen auf
    - Das Vorgehen heißt **Polling**
- CSMA/CA PCF ist ein optionales Verfahren und wird selten implementiert
  - Darum wird es an dieser Stelle nicht weiter näher beschrieben



## Arbeitsweise von ARP (1/2)

- Das **Address Resolution Protocol** (ARP) übersetzt IP-Adressen der Vermittlungsschicht in MAC-Adressen der Sicherungsschicht
- Will ein Netzwerkgerät Daten an einen Empfänger senden, gibt es auf der Vermittlungsschicht die IP-Adresse des Empfängers an
- Auf der Sicherungsschicht ist aber die MAC-Adresse nötig
  - Darum muss in der Sicherungsschicht die **Adressauflösung** erfolgen
  - Um die MAC-Adresse eines Geräts im LAN zu erfahren, sendet ARP einen Rahmen mit der MAC-Broadcast-Adresse FF-FF-FF-FF-FF-FF als Zieladresse
    - Diesen Rahmen nimmt jedes Netzwerkgerät entgegen und wertet ihn aus
    - Der Rahmen enthält die IP-Adresse des gesuchten Netzwerkgeräts
  - Fühlt sich ein Gerät mit dieser IP-Adresse angesprochen, schickt es eine ARP-Antwort an den Sender
    - Die gemeldete MAC-Adresse speichert der Sender im lokalen ARP-Cache

## Arbeitsweise von ARP (2/2)

- Der **ARP-Cache** dient zur Beschleunigung der Adressauflösung
  - Er enthält eine Tabelle mit folgenden Informationen für jeden Eintrag:
    - Protokolltyp (IP)
    - Protokolladresse des Senders (IP-Adresse)
    - Hardware-Adresse des Sender (MAC-Adresse)
    - Ablaufzeit – Time To Live (TTL)
  - Die TTL legt das Betriebssystem fest
  - Wird ein Eintrag in der Tabelle verwendet, verlängert sich die TTL
- Aktuelle Linux-Distributionen verwerfen Einträge nach  $\approx 5$  Minuten

ARP-Cache ausgeben: `arp -n` oder alternativ `ip neighbour`

```
# arp -n
Address HWtype HWaddress      Flags Mask    Iface
192.168.178.1 ether 9c:c7:a6:b9:32:aa C          wlan0
192.168.178.24 ether d4:85:64:3b:9f:65 C          wlan0
192.168.178.41 ether ec:1f:72:70:08:25 C          wlan0
192.168.178.25 ether cc:3a:61:d3:b3:bc C          wlan0
```

Mit `arping` kann man manuell Anforderungen zur Adressauflösung versenden

# Aufbau von ARP-Nachrichten

- ARP-Nachrichten werden als Nutzdaten in Ethernet-Rahmen übertragen (Typ = 0x0806 für das ARP-Protokoll)



- H-Länge = Länge der HW-Adressen (MAC-Adressen) in Bytes
  - Bei Ethernet: 6 Bytes
- P-Länge = Länge der IP-Adressen in Bytes
  - Bei IPv4: 4 Bytes

In einer ARP-Anfrage ist der Inhalt des Feldes MAC-Adresse (Ziel) egal

