8th Lecture Computer Networks

Dr. Christian Baun

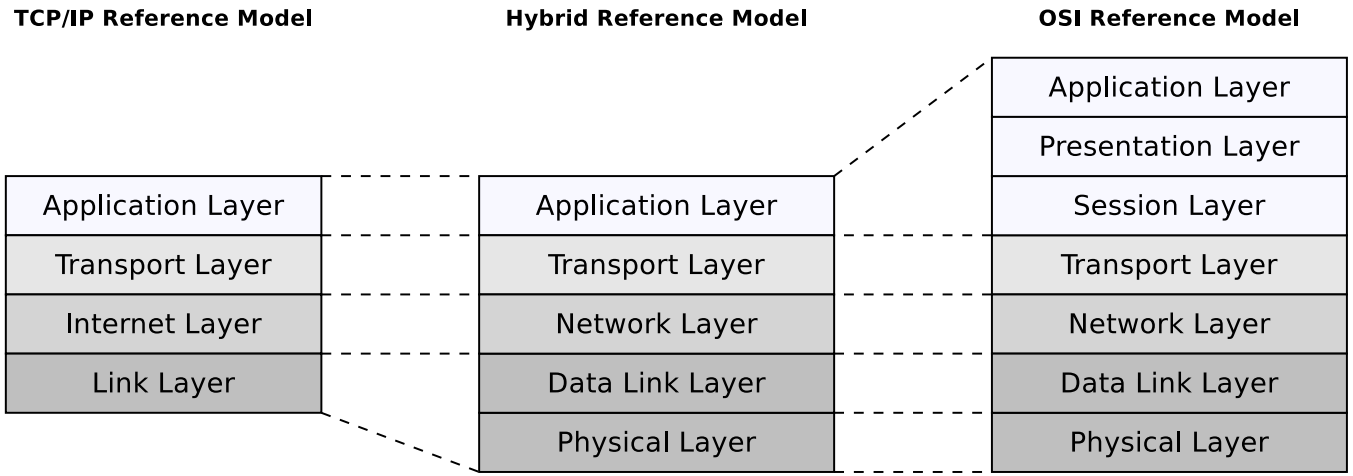
Fachhochschule Frankfurt am Main
University of Applied Sciences
Faculty of Computer Science and Engineering
wolkenrechnen@gmail.com

Agenda for Today

- Data link layer (part 3)
  - Media access control methods
    - Media access control method of Ethernet
    - Media access control method of WLAN
  - Address resolution with ARP

Data Link Layer

- Functions of the data link layer
  - Pack packets of the network layer into frames
  - Break the bit stream of the physical layer into frames
  - Ensure correct transmission of the frames inside a physical network from one network device to another one via error detection with checksums
  - Provide physical addresses (MAC addresses)
  - Control access to the transmission medium



- Devices: Bridge, Layer-2-Switch (Multiport-Bridge)
- Protocols: Ethernet, Token Ring, WLAN, Bluetooth

Media Access Control Methods

- With Ethernet and WLAN the network devices or stations use a shared transmission medium
- To coordinate media access and to avoid collisions, media access control methods are required
  - Ethernet uses the media access control method **CSMA/CD**
  - WLAN uses the media access control method **CSMA/CD**
- Bluetooth is not discussed here, because Bluetooth devices are organized in **piconets**
  - In each piconet, the master coordinates a media access

Media Access Control Method CSMA/CD

- In contrast to Token Ring, for Ethernet it's impossible to clearly predict the waiting time and amount of data that can be transmitted
- All participants are related to the medium access in direct competition
- The Waiting time and amount of data depend on the number of participants and the amount of data which is send by the individual participants
- Ethernet uses the media access control method „Carrier Sense Multiple Access / Collision Detection“ (CSMA/CD)

Meaning of CSMA/CD

- **Carrier Sense (CS) means:**
  - Each network device monitors the channel before transmitting, and it only transmits when the channel is free
  - This means that the network devices can distinguish between a free and a busy connecting cable
- **Multiple Access (MA) means:**
  - All network devices access the same transmission medium in a competitive way
- **Collision Detection (CD) means:**
  - Each network device also monitors the channel during transmission, in order to detect collisions as early as possible and to perform error handling when needed

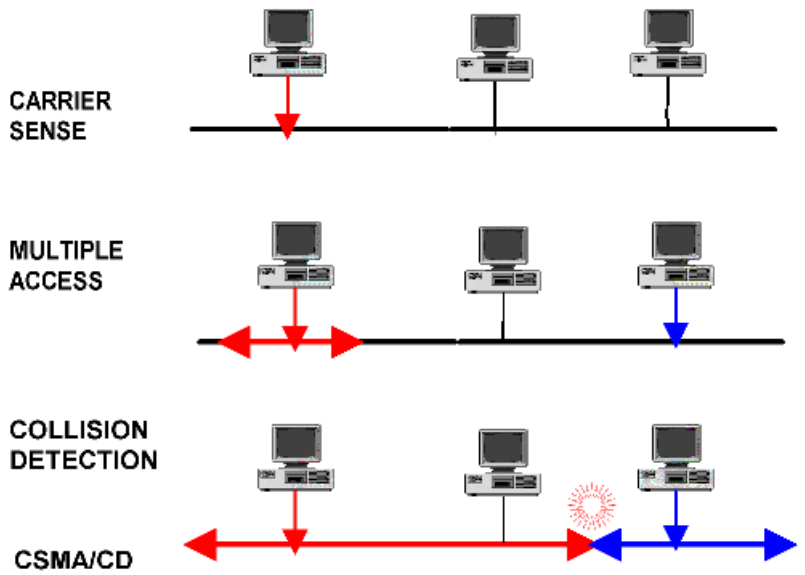


Image source: `http://www.payer.de/cmc/cmcs08.htm`

Functioning of CSMA/CD (1/2)

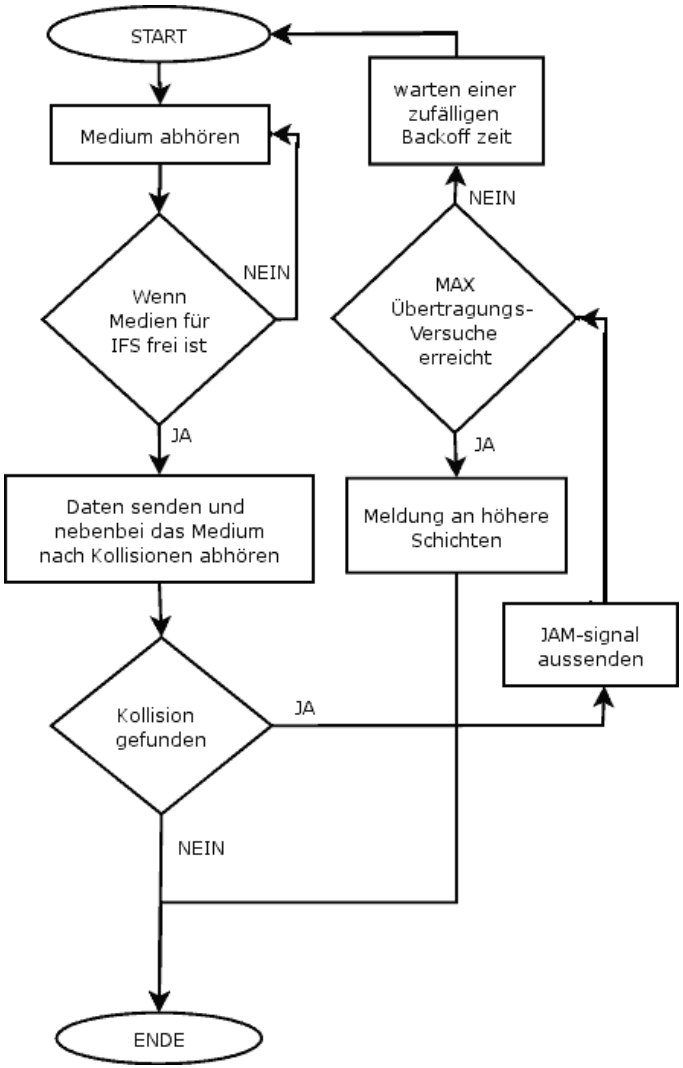


Image source: Wikipedia

- If a network device wants to transmit frames via Ethernet, it operates according to the following sequence

1. Monitor the transmission medium
   - Transmission medium is free $\Longrightarrow$ step 2
   - Transmission medium is busy $\Longrightarrow$ step 3
2. Start transmission and continue to monitor the transmission medium
   - Successful transmission
     - Send success message to upper network layers $\Longrightarrow$ step 5
   - Collision is detected
     - Stop frame transmission and send the 48 bit long (*jam signal*) to announce the collision $\Longrightarrow$ step 3

Functioning of CSMA/CD (2/2)

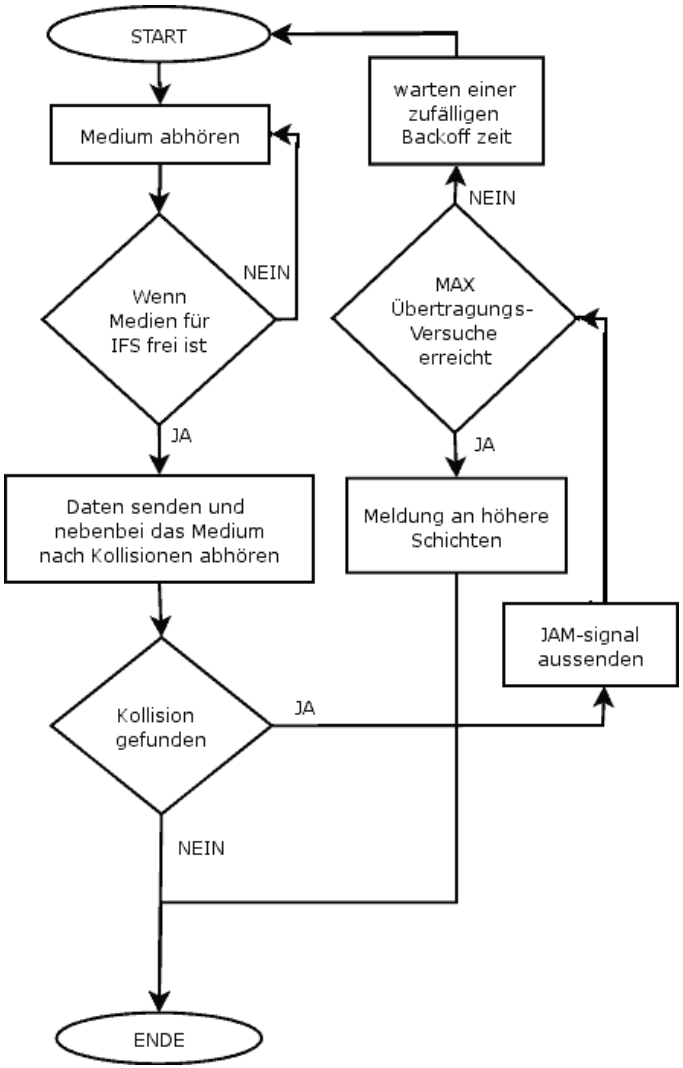


Image source: Wikipedia

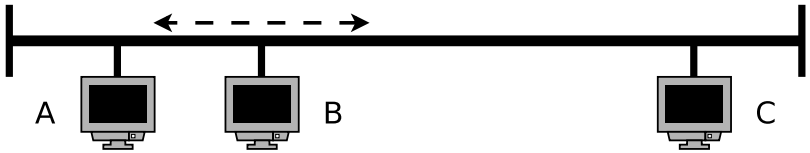
3. Transmission medium is busy. Check the number of transmission attempts:
   - Maximum not yet reached
     - Wait a random time $\Longrightarrow$ step 1
     - The random time is calculated using the backoff method
   - Maximum is reached $\Longrightarrow$ step 4
4. Error
   - Maximum number of transmission attempts reached
   - Send error message to upper network layers $\Longrightarrow$ step 5
5. Leave transmission mode

Example of CSMA/CD

1

B wants to transmit frames and monitors the transmission medium
From the perspective of B, the medium is free

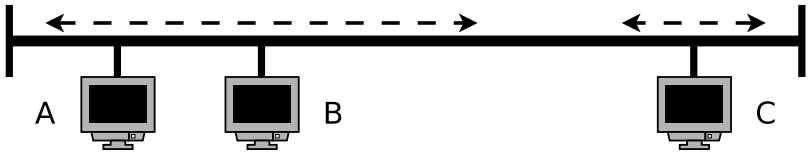
2



B begins the transmission and continues to monitor the medium

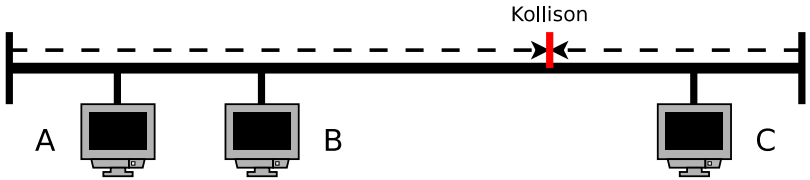
C wants to transmit frames and monitors the transmission medium
From the perspective of C, the medium is free

3



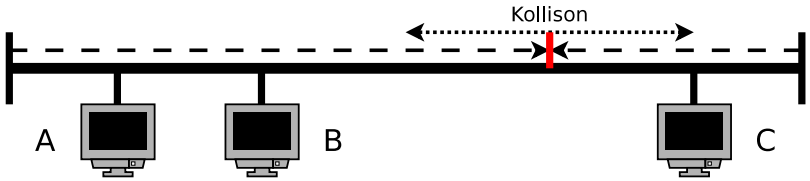
C begins the transmission and continues to monitor the medium

4



A collision occurs
The voltage on the cable changes
This leads to a sort senseless noise

5



The collision spreads out and reaches C first

6

C stops to transmit and sends the jam signal

As soon as the collision reaches B, this participant stops the transmission too and sends the jam signal

Network Size and Collision Detection

- A collision must be detected by the sender
- It is important that the transmission of a frame is **not completed** when a collision occurs
  - Otherwise, the network device might already be finished with the transmission and believes the transmission was successful
- Each frame must have a certain minimum length
  - It must be dimensioned in a way that the transmission duration for a frame with minimum length does not fall below the maximum RTDT (round trip delay time)
    - The RTDT is the time it takes for a frame to travel from one end of the network to the most distant end and return back
- This ensures that a collision reaches the sender before it's transmission is finished
  - If a sender detects a collision, it knows that it's frame has not arrived correctly at the receiver, and can try the transmission again later

Minimum Frame Length and Collision Detection (Example)

- For Ethernet, a maximum network size, and a minimum frame length is defined
- The **minimum frame length**, where collision detection is still possible, is calculated as follows:

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

P = Minimum frame length in bits
U = Data transmission speed of the transmission medium in bits per second (bps)
D = Network length in meters
V = Signal speed on the transmission medium in meters per second (mps)

- Calculation example for 10BASE5 with 10 Mbps and coaxial cables:
  - $U = 10\,\text{Mbps} = 10{,}000{,}000\,\text{bps}$
  - $D = 2,500$ meters (this is the maximum length for 10BASE5)
  - $V =$ speed of light $*$ velocity factor
    - Speed of light $c = 299{,}792{,}458\,\text{mps}$
    - Velocity factor $ABF = 0.77$ for coaxial cables
    - $V = c * ABF \approx 231,000,000$ mps

$$P = 2 * 10 * \frac{2500}{231} \approx 218 \text{ Bits} \approx 28 \text{ bytes}$$

- this means that the minimum frame length of 64 bytes for Ethernet is more than enough

Velocity Factor (Wave Propagation Speed)

- The velocity factor, also known as wave propagation speed, depends on transmission medium and is:
  - 1 for the vacuum
  - 0.60 for twisted pair cables
  - 0.67 for optical fiber
  - 0.60 for coaxial cables
- Describes the speed of a signal on a transmission medium relative to the speed of light

Network Size and Collision Detection (Example)

- The **maximum network size**, where collision detection is still possible, is calculated as follows:

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

S_{max} = Maximum network size with collision detection
V = Signal speed of the transmission medium in meters per second (mps)
t_{frame} = transmission duration of a frame in seconds

- Calculation example for 10BASE5 with 10 Mbps and coaxial cables:
  - $V = 231,000,000$ mps $= 231 * 10^6$ mps
  - Transmission duration t_{frame} = Transmission duration for a single bit multiplied with the number of bits in a frame ($\Longrightarrow$ 512 bit = 64 byte)
    - The transmission duration for a single bit at 10 mbps is 0.1 microseconds
    - A frame with the minimum frame length of 64 bytes needs requires 51.2μs for a complete transmission
  - A 51.2μs long signal travels in the coaxial cable the following distance: $231 * 10^6 * 51.2 * 10^{-6} = 11,827.20$ m $= 11.82$ km
  - A frame which is 64 bytes large needs for $2 * 2,500$ m $= 5,000$ m less than half the minimum transmission time of 51.2μs
    - The maximum network size of 2.5 km is dimensioned small enough

CSMA/CD nowadays

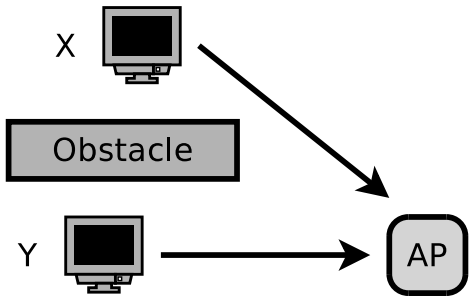
- The media access method CSMA/CD is absolutely necessary for computer networks that are based on the bus network topology, because at this topology, all network devices are directly connected with a common transmission medium
- Almost all Ethernet-based networks nowadays *fully switched* and therefore free from collisions

Media Access Control Method CSMA/CA of WLAN

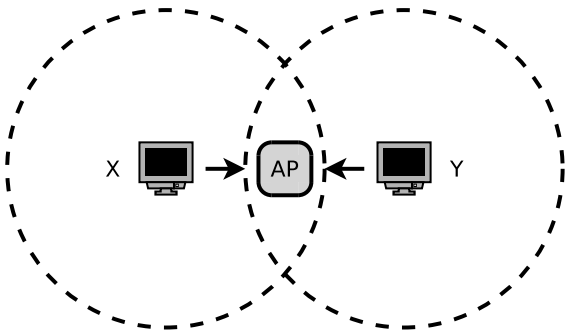
- CSMA/CD does not work with wireless networks
  - In contrast to wired computer networks based of Ethernet, it's not guaranteed that all collisions are detected in wireless networks
- With CSMA/CD, the sender detects occurring collisions
  - In wired networks with a common transmission medium, each participant receives the transmissions of all other participants
    - Therefore each participant detects any collision
  - For wireless networks such as WLAN, this is not always the case
    - For this reason, the media access methods *Carrier Sense Multiple Access / Collision Avoidance* (CSMA/CA) is used which tries to minimize the occurrence of collisions
- Two special characteristics of the transmission medium in wireless networks lead to undetected collisions at the receiver
  - **Hidden terminal problem**
  - **Fading**
- The hidden terminal problem and fading both make multiple access in wireless networks more complicated compared to wired networks

Zwei Spezielle Eigenschaften des Übertragungsmediums

- **Hidden terminal problem** (Problem caused by invisible or hidden terminal device)
  - X and Y both send frames to the Access Point
  - Because of obstacles the stations X and Y can not detect their transmissions, although they interfere each other at the Access Point



- **Fading** (decreasing signal strength)
  - X and Y both send frames to the Access Point
  - The electromagnetic waves of the wireless network are gradually weakened by obstacles and in free space
  - Caused by the positions of X and Y to each other stations, their signals are too weak that the stations can detect each others transmissions



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

WLAN (802.11) implements 3 different Media Access Control Methods

1. **CSMA/CA**
   - Strategy: *Listen before talk*
   - Collision avoidance through random backoff time
   - Minimum distance between frames
   - Receive acknowledgements via ACK (not for broadcast)
   - Default method which is implemented in all WLAN devices
2. **CSMA/CA RTS/CTS** (**R**equest **T**o **S**end/**C**lear **T**o **S**end)
   - Solves the problem of hidden terminals
   - Optional method and implemented in most WLAN devices
3. **CSMA/CA PCF** (**P**oint **C**oordination **F**unction)
   - Access Point controls the access to the transmission medium
   - Optional method and seldom implemented

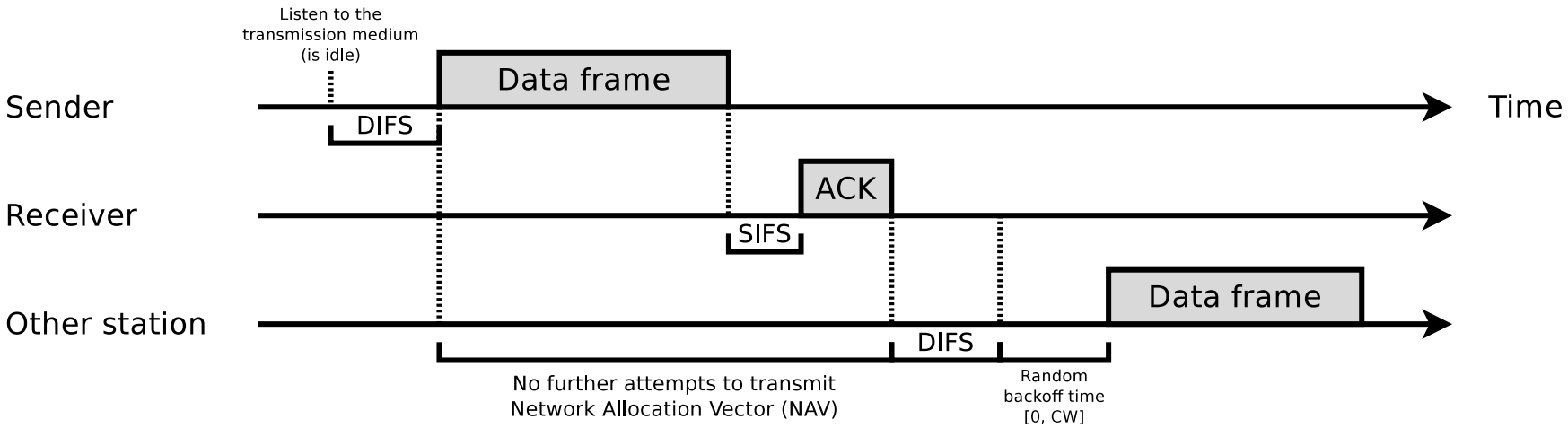
Source: Lecture slides of Prof. Dr. Michael Massoth and Wikipedia

Transmission of Frames

- 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
    - Es gibt also kein Zurück mehr, wenn eine Station einmal mit dem Senden begonnen hat
  - Der Sender muss darum erkennen können, wenn ein Rahmen nicht korrekt beim Empfänger angekommen ist

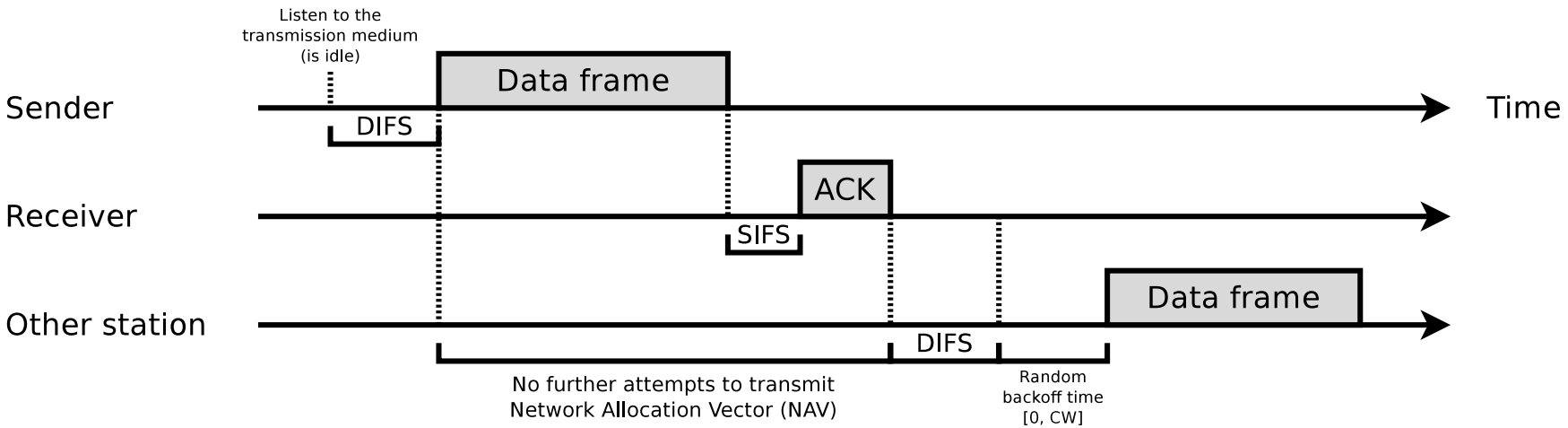
Functioning of CSMA/CA – 1/5

- At first, the sender *listens* to the transmission medium (carrier sense)
- The transmission medium needs to be idle for a short period
  - This period is called **Distributed Interframe Spacing (DIFS)** $\approx 50\mu s$
- If the transmission medium is free for the duration of one DIFS, the station can send start to transmit a frame



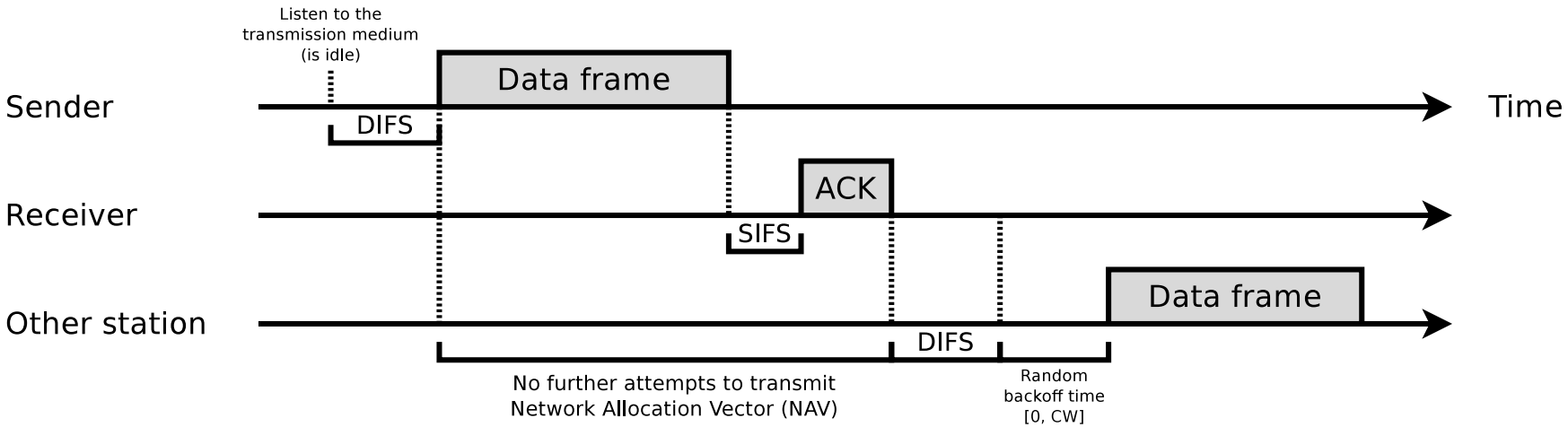
Functioning of CSMA/CA – 2/5

- If a station receives a frame which passes the CRC check, them it waits for a short period
  - This period is called **Short Interframe Spacing (SIFS)** $\approx 10\mu s$
  - Then the receiver sends an **acknowledgement frame (ACK)**
    - Die Empfangsbestätigung durch ACK erfolgt nicht bei einem Broadcast
- DIFS und SIFS garantieren bei CSMA/CA einen Mindestabstand zwischen aufeinanderfolgenden Rahmen



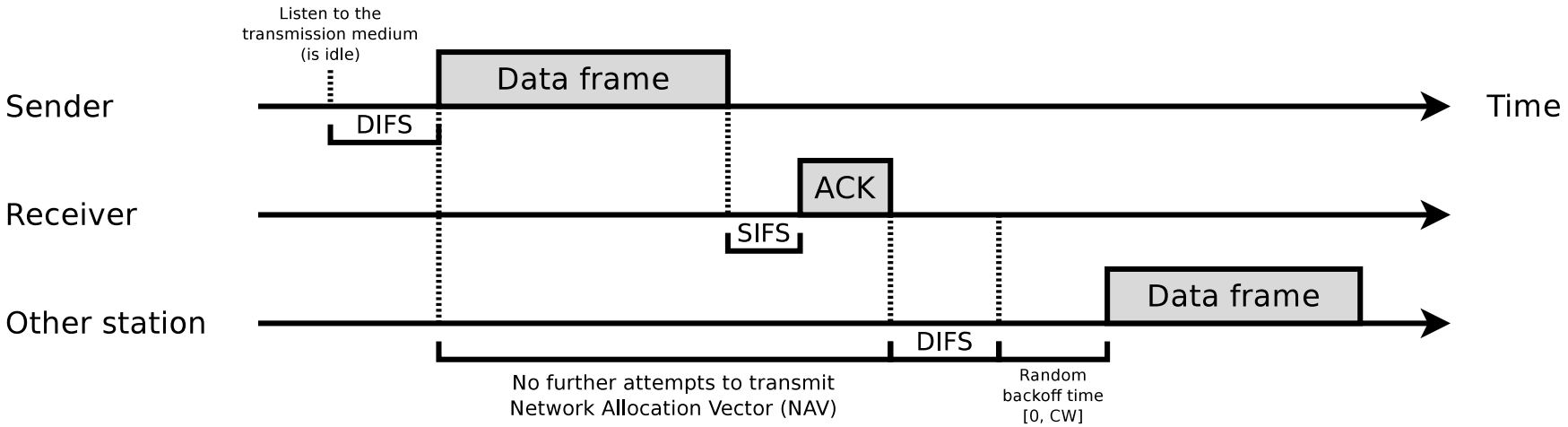
Functioning of CSMA/CA – 3/5

- 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 von jeder Station selbst verwaltet wird
  - Verringert die Kollisionen bei CSMA/CA
  - Enthält die Zeit, die das Übertragungsmedium voraussichtlich belegt sein wird



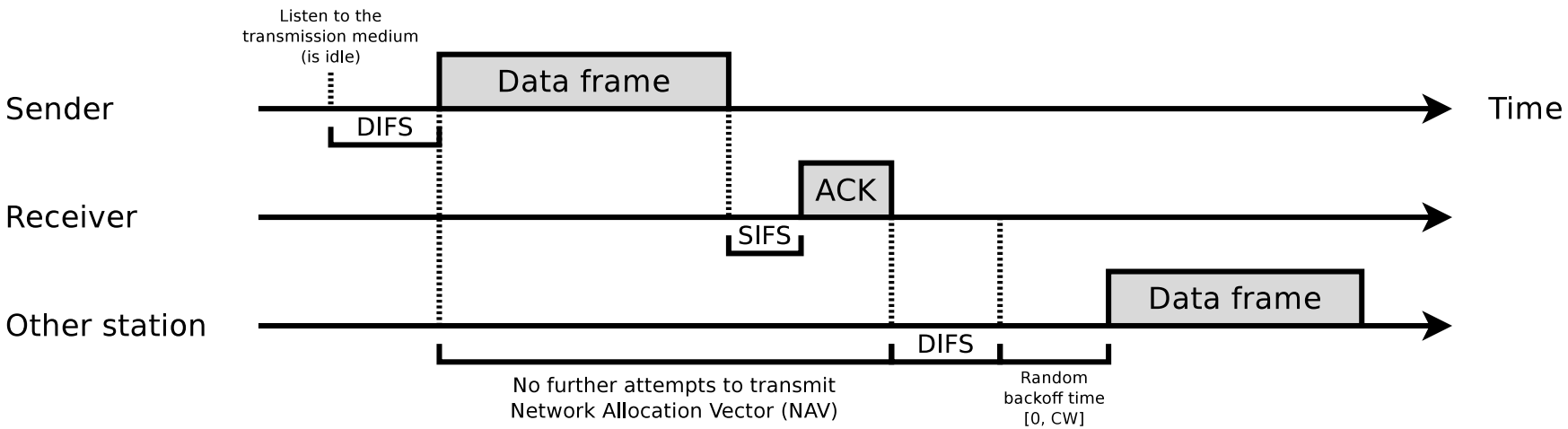
Functioning of CSMA/CA – 4/5

- Empfängt eine Station zum Beispiel die Information „*Das Übertragungsmedium ist für die nächsten x Datenrahmen belegt*“, trägt sie die erwartete Belegungszeitspanne in ihren NAV ein
- Der NAV wird mit der Zeit dekrementiert, bis er den Wert 0 erreicht
- Solange der NAV > 0 ist, unternimmt eine Station keine Sendeversuche
  - Dabei ist es egal, ob das Übertragungsmedium frei oder belegt ist



Functioning of CSMA/CA – 5/5

- Nach Ablauf des NAV und einem weiteren DIFS mit freiem Übertragungsmedium wird eine **Backoffzeit** aus dem **Contention Window** (CW) erzeugt
  - Das CW ist ein Wert, den jeder IEEE 802.11 Rahmen enthält
  - Mit dem CW wird eine zufällige Zeitspanne als Backoff definiert
  - Die CW-Zeitspanne liegt zwischen einem minimalen und einem maximalen Wert
  - Die CW-Zeitspanne wird bei jeder auftretenden Kollision verdoppelt
- Nach dem Ablauf der Backoffzeit wird der Rahmen gesendet

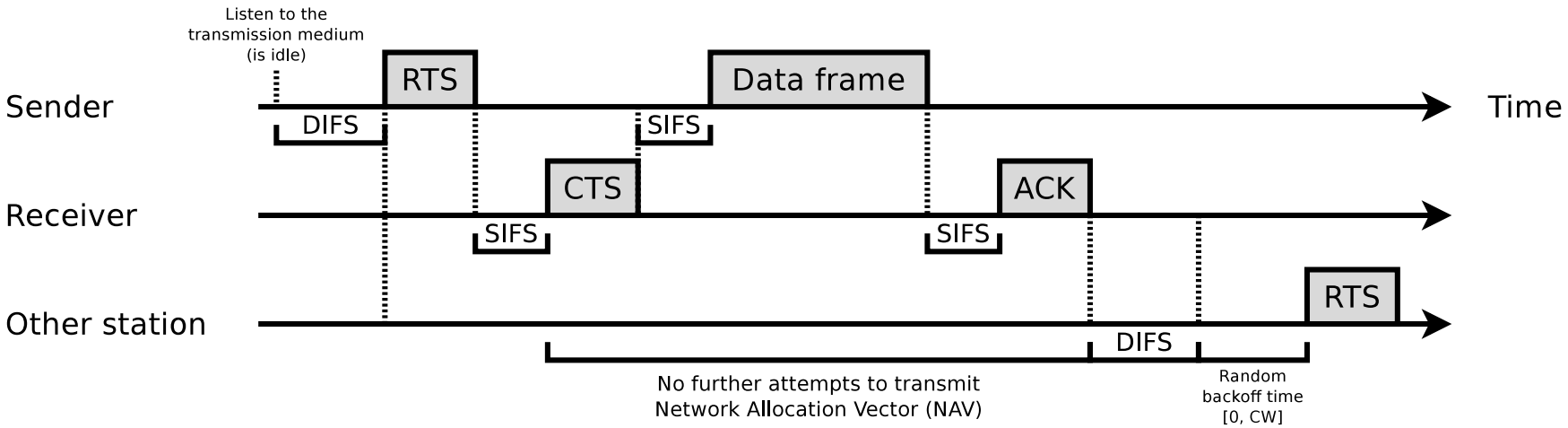


CSMA/CA RTS/CTS

- The media access control method CSMA/CA reduces the number of collisions
  - But it can not avoid all collisions
- An improved collision avoidance provides CSMA/CA RTS/CTS
  - Sender and receiver exchange with this method **control frames** before the sender begins to transmit
    - This way, all available stations know that a transmission will start soon
  - The control frames are **Request To Send (RTS)** and **Clear To Send (CTS)**
  - both control frames contain a field which indicates how long the transmission medium (the channel) will be occupied

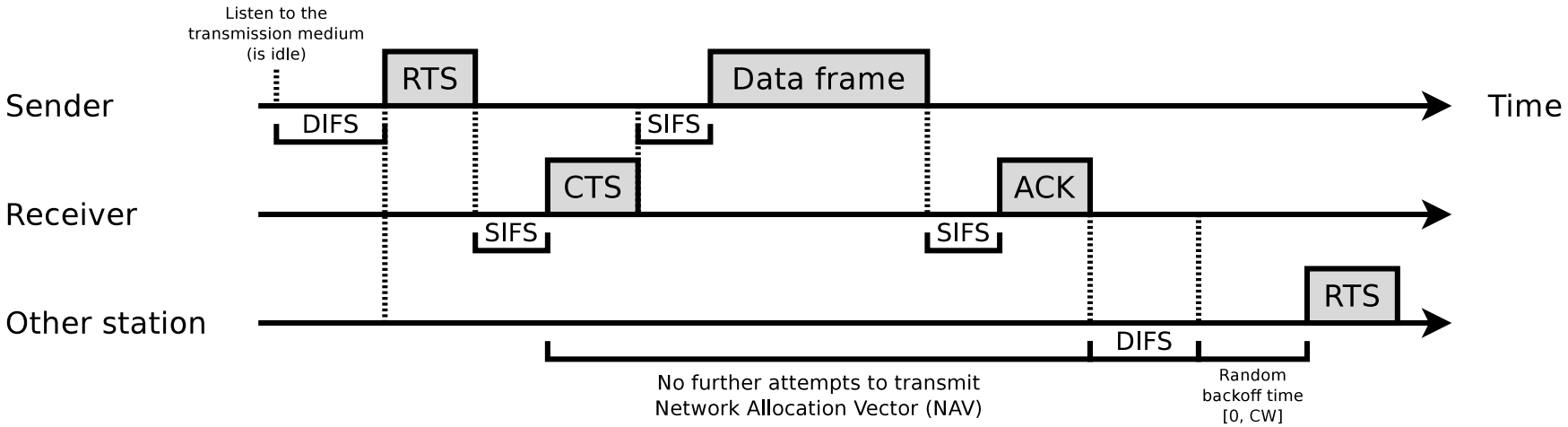
Functioning of CSMA/CA RTS/CTS – 1/4

- After the DIFS, the sender transmits a **RTS** frame to the receiver
  - The RTS frame contains a field that specifies the period, the sender wants to reserve (use) the transmission medium (the channel)
    - In the RTS frame, the sender specifies the length of data frame to be transmitted



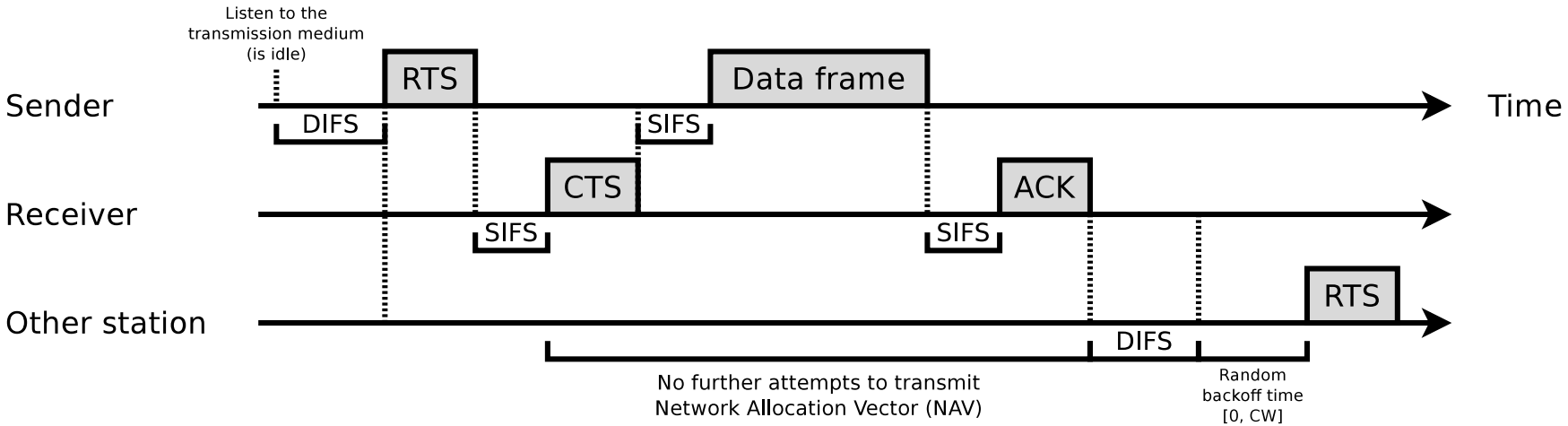
Functioning of CSMA/CA RTS/CTS – 2/4

- the receiver acknowledges this by waiting the SIFS and then transmitting a **CTS** frames, which also contains the period, the sender wants to reserve the transmission medium
  - The receiver sends the length field back to the sender and confirms this way the length of the data frame to be transmitted



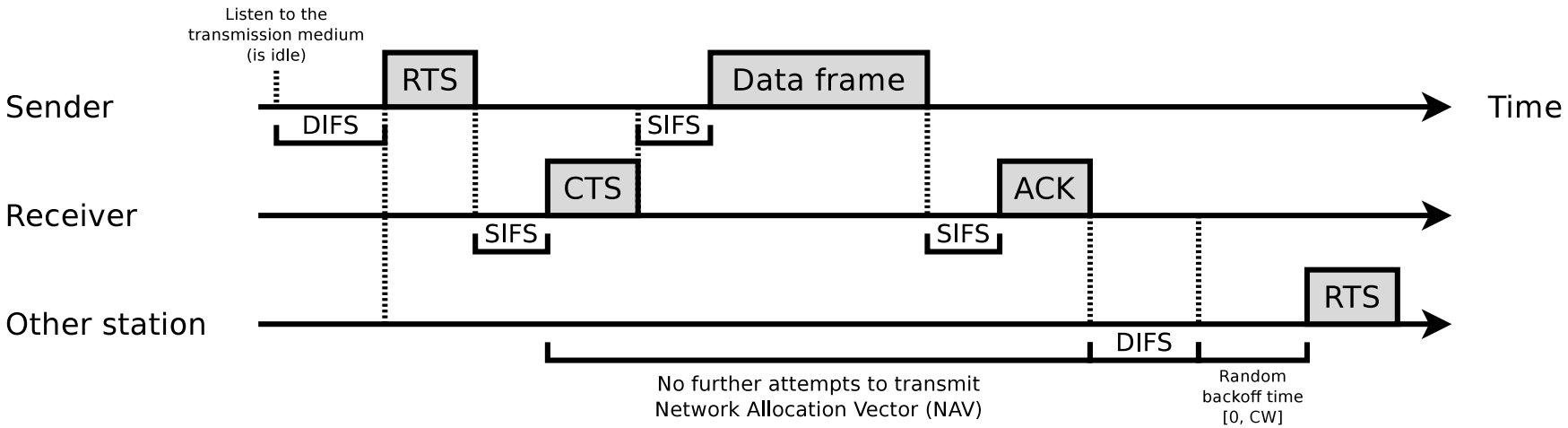
Functioning of CSMA/CA RTS/CTS – 3/4

- After the receiver successfully received the data frame, he waits a SIFS and transmits an ACK frame to the sender
- All other stations wait the time ($\Longrightarrow$ frame length) which is specified in the CTS frame
- Collisions can only occur during the transmission of RTS and CTS frames



Functioning of CSMA/CA RTS/CTS – 4/4

- Advantage: CSMA/CA RTS/CTS reduces collisions, because it solves the problem of hidden terminals
- Drawbacks:
  - Delays which are caused by the reservation of the transmission medium occur
  - The RTS and CTS frames which are used to reserve the transmission medium are overhead



CSMA/CA RTS/CTS in Practice

- CSMA/CA RTS/CTS is optional for WLAN and is mostly implemented
  - In practice, it is used for reserving channels for the transmission of big data frames
- For each station, a RTS threshold value can be set (driver?)
  - This way it can be defined that RTS/CTS is used only when a frame is bigger than the threshold value
- Often, the default threshold value is higher than the maximum frame length (2.346 byte) for IEEE 802.11
  - Then, the RTS/CTS sequence can be omitted for all transmitted data frames

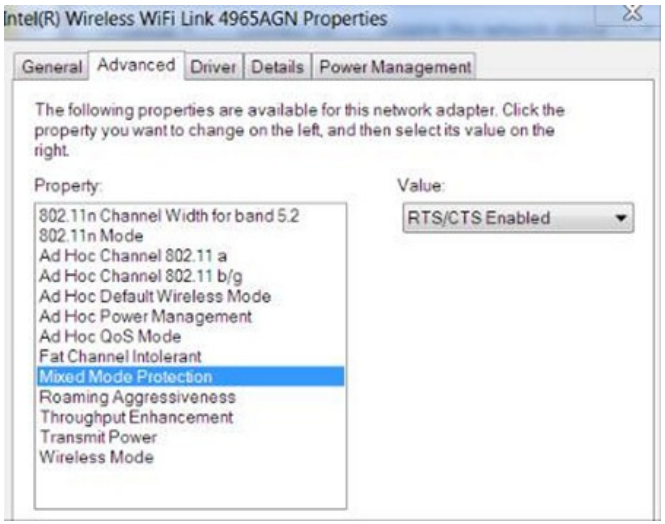


Image source: `http://www.itedge.net`

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

CSMA/CA PCF

- **PCF** = **P**oint **C**oordination **F**unction
- The access point controls the media access by requesting the registered stations to transmit data frames
  - The approach is called **polling**
- CSMA/CA PCF is an optional method and seldom implemented
  - For this reason it is not discussed here in detail

Arbeitsweise von ARP (1/2)

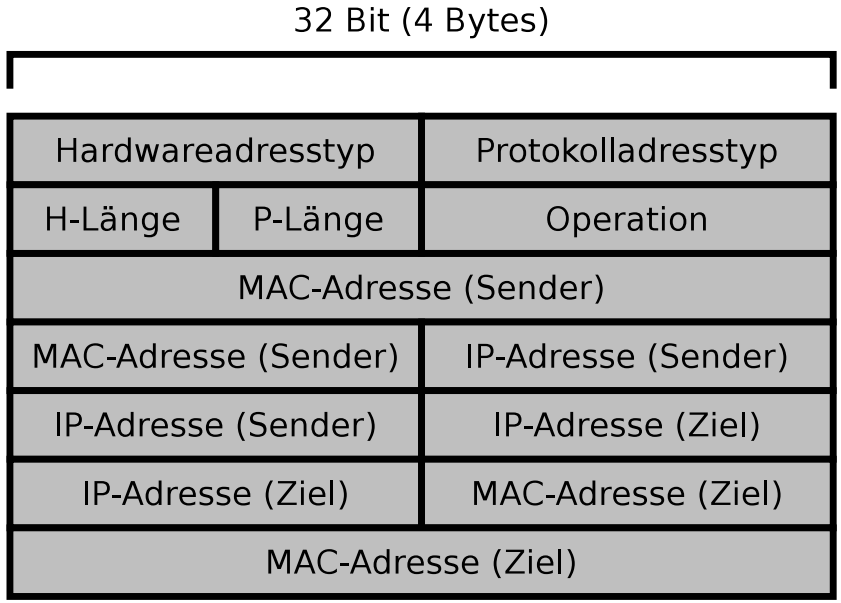
- Das **Address Resolution Protocol** (ARP) übersetzt IP-Adressen der Vermittlungsschicht in MAC-Adressen der Sicherungsschicht
- Will ein Netzwerkgerät Daten an einen Empfänger senden, gibt es auf der Vermittlungsschicht die IP-Adresse des Empfängers an
- Auf der Sicherungsschicht ist aber die MAC-Adresse nötig
  - Darum muss in der Sicherungsschicht die Adressauflösung erfolgen
  - Um die MAC-Adresse eines Netzwerkgeräts innerhalb des LAN zu erfahren, versendet ARP einen Rahmen mit der MAC-Broadcast-Adresse `FF-FF-FF-FF-FF-FF` als Zieladresse
    - Dieser Rahmen wird von jedem Netzwerkgerät entgegengenommen und ausgewertet
    - 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 wird im lokalen ARP-Cache des Senders gespeichert

Arbeitsweise von ARP (2/2)

- Der ARP-Cache dient zur Beschleunigung der Adressauflösung
  - Er enthält eine Tabelle mit vier Spalten
    - Protokolltyp (IP)
    - Protokolladresse des Senders (IP-Adresse)
    - Hardware-Adresse des Sender (MAC-Adresse)
    - Ablaufzeit – Time To Live (TTL)
  - Die TTL wird vom Betriebssystem festgelegt
  - Wird ein Eintrag in der Tabelle verwendet, verlängert sich die TTL
- Aktuelle Linux-Distributionen verwerfen Einträge im ARP-Cache nach ca. 5 Minuten
- Wird ein Eintrag in der Tabelle verwendet, wird die TTL verlängert
- Unter Linux kann der ARP-Cache mit `arp` angezeigt und verändert werden
- Mit `arping` kann man manuell Anforderungen zur Adressauflösung versenden

Aufbau von ARP-Nachrichten (1/2)

- ARP-Nachrichten werden im Nutzdatenteil von Ethernet-Rahmen übertragen
  - Das `Typ`-Datenfeld im Ethernet-Rahmen wird auf den Wert `0x0806` für das ARP-Protokoll gesetzt
- Das Datenfeld `H-Länge` enthält die Länge der Hardwareadressen (MAC-Adressen) in Bytes
  - Bei Ethernet sind MAC-Adressen 6 Bytes lang
- Das Datenfeld `P-Länge` enthält die Länge der Protokolladressen (IP-Adressen) in Bytes
  - Bei IPv4 sind IP-Adressen 4 Bytes lang



Aufbau von ARP-Nachrichten (2/2)

- Die Quell-MAC-Adresse ist die MAC-Adresse des Senders bei einer ARP-Anforderung und die MAC-Adresse des antwortenden Hosts bei einer ARP-Antwort
- Die Ziel-MAC-Adresse ist in einer ARP-Anforderung gleichgültig und enthält in einer ARP-Antwort die MAC-Adresse des anfragenden Hosts

- Die Quell-IP-Adresse ist bei einer ARP-Anforderung die IP des anfragenden Host und bei einer ARP-Antwort die IP des antwortenden Hosts
- Die Ziel-IP-Adresse ist bei einer ARP-Anforderung die IP-Adresse des gesuchten Hosts und bei einer ARP-Antwort die IP-Adresse des anfragenden Hosts