6th Slide Set
Computer Networks

Prof. Dr. Christian Baun

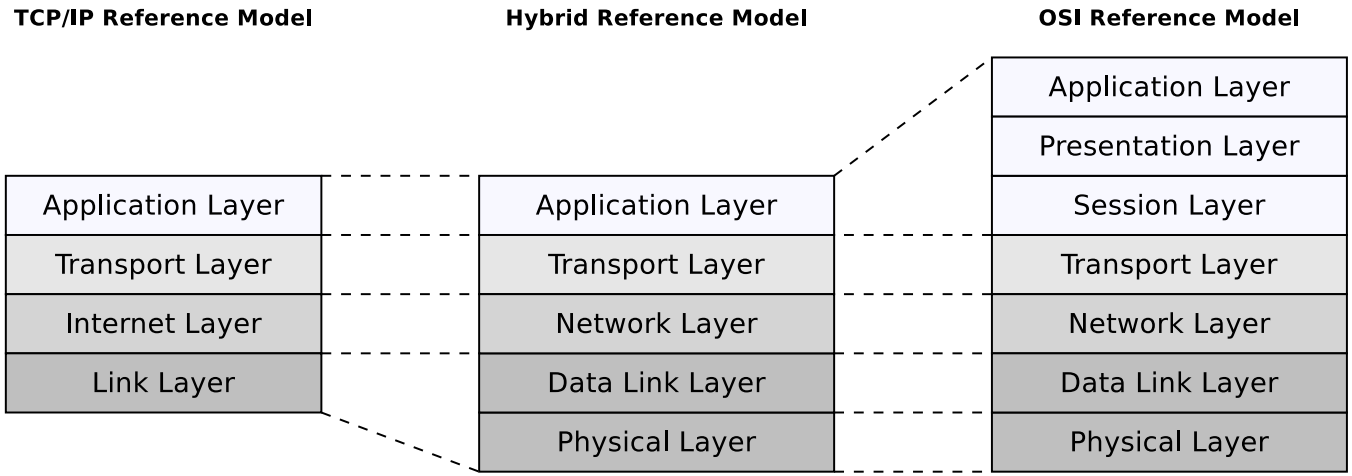
Frankfurt University of Applied Sciences
(1971–2014: Fachhochschule Frankfurt am Main)
Faculty of Computer Science and Engineering
christianbaun@fb2.fra-uas.de

Learning Objectives of this Slide Set

- 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
  - Sender: Pack packets of the Network Layer into frames
  - Receiver: Identify the frames in the bit stream from the Physical Layer
  - 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), Modem
- Protocols: Ethernet, Token Ring, WLAN, Bluetooth, PPP

Media Access Control Methods

- With Ethernet 10BASE2/5 and WLAN, the network devices or stations use a shared transmission medium
  - To coordinate the 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/CA**
- Bluetooth is not discussed here, because Bluetooth devices are organized in **piconets**
  - In each piconet, the master coordinates the media access

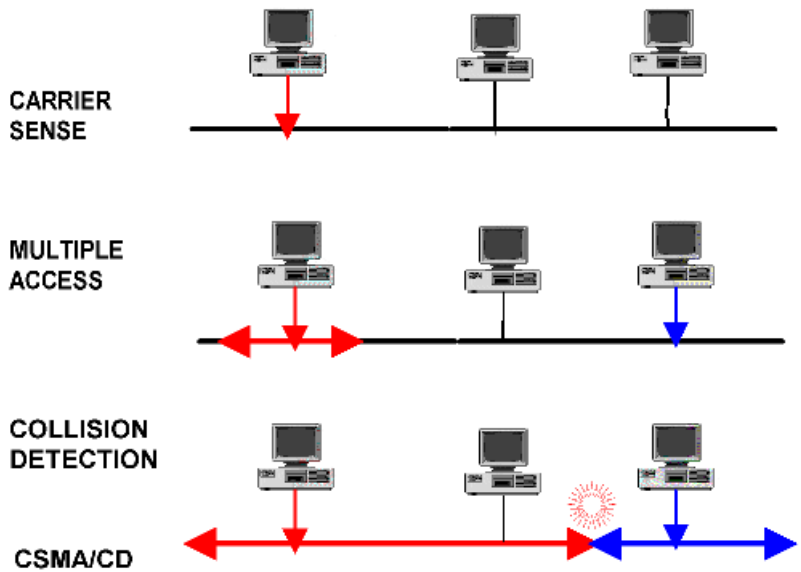
Media Access Control Method CSMA/CD

- In contrast to Token Ring, for Ethernet it is impossible to predict the **waiting time** and **amount of data**, that can be transmitted
- All participants are regarding the media 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

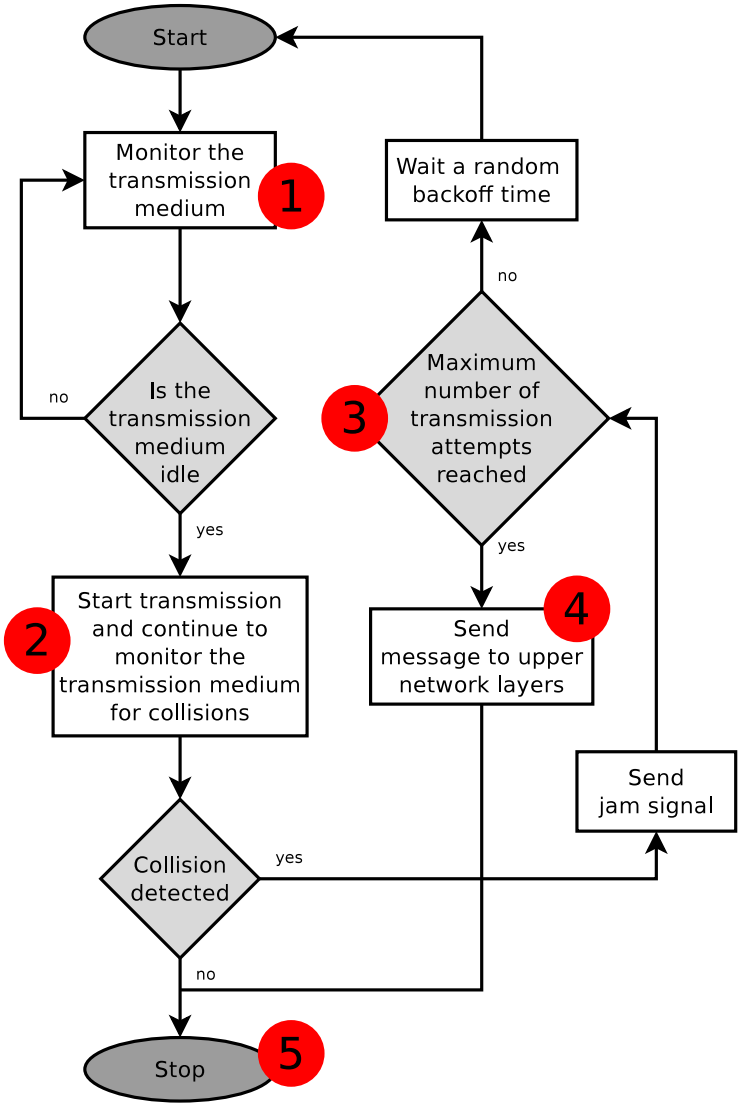
Image source: http://www.payer.de/cmc/cmcs08.htm

- **Carrier Sense (CS) means:**
  - Each network device monitors the channel before transmitting data, and it only transmits data when the channel is idle
  - Thus, the network devices can distinguish between an idle and a busy 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 and to perform error handling, when needed



Functioning of CSMA/CD (1/2)

Image Source: Wikipedia

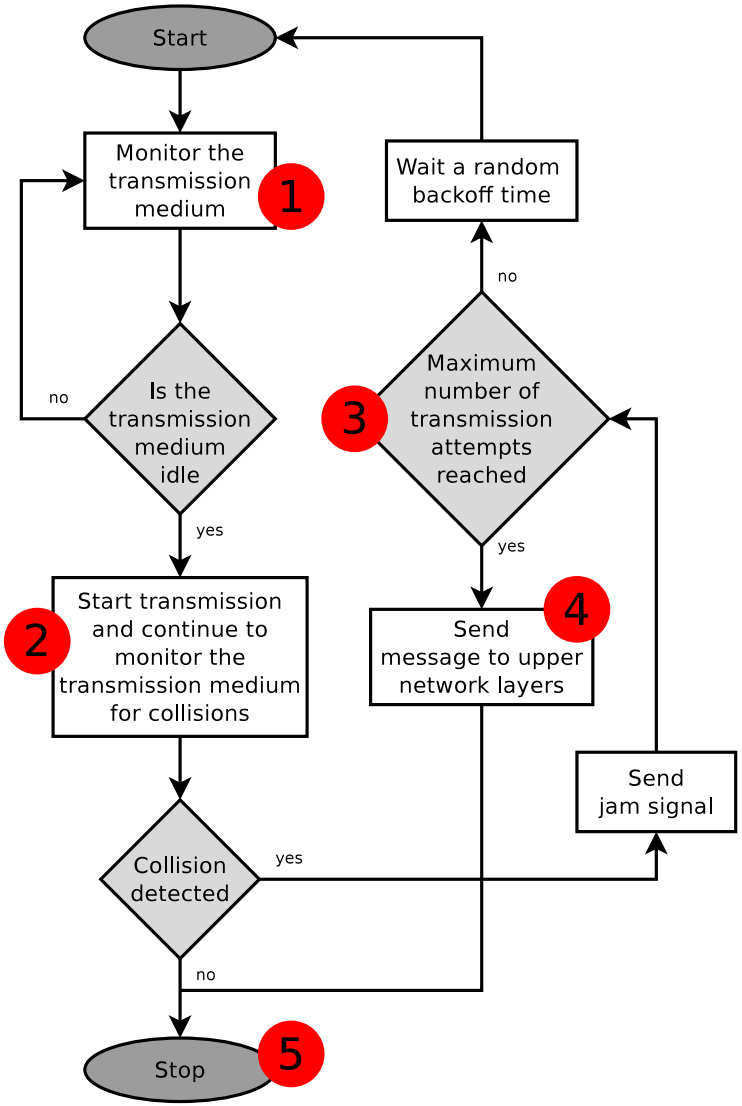


- If a network device wants to transmit frames via Ethernet, it operates according to the following sequence

1. Monitor the transmission medium
   - Transmission medium is idle $\Longrightarrow$ 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 bits long (*jam signal*) to announce the collision $\Longrightarrow$ step 3

Functioning of CSMA/CD (2/2)

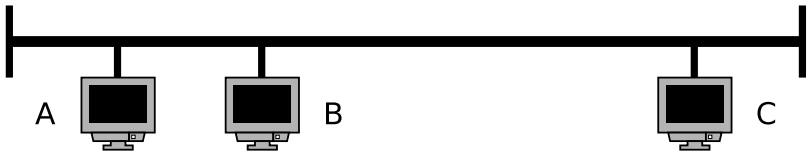
Image Source: Wikipedia



3. Transmission medium is busy. Check the number of transmission attempts:
   - Maximum number not yet reached
     - Wait a random time $\Longrightarrow$ step 1
     - The random time is calculated using the backoff method
   - Maximum number 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

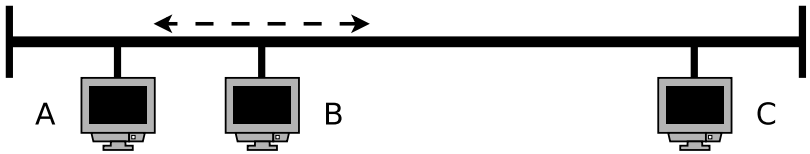
Example of CSMA/CD

1



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

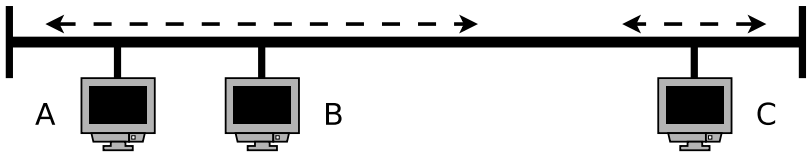
2



B begins the transmission and continues to monitor the medium

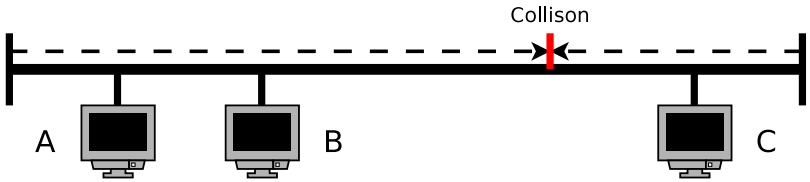
C wants to transmit frames and monitors the transmission medium
From the perspective of C, the medium is free

3



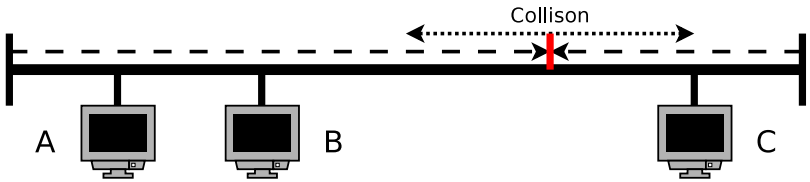
C begins the transmission and continues to monitor the medium

4



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

5



The collision spreads and reaches C first

6

C stops to transmit the frame 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 sending the frame and assumes 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 RTT (round trip time)
    - The RTT 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 its transmission is finished**
    - If a sender detects a collision, it knows that its frame has not arrived correctly at the receiver, and can try the transmission again later

Ethernet specifies a maximum network size and a minimum frame length

Minimum frame length for Ethernet: 64 Bytes
Maximum length of the physical network depends on the Ethernet standard used

Minimum Frame Length and Collision Detection (Example)

- Ethernet specifies a maximum network size and a minimum frame length
- 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 rate 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)

- 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 $= 299{,}792{,}458\,\text{m/s}$
    - Velocity factor $= 0.77$ for coaxial cables
    - $V = 299,792,458\,\text{m/s} * 0.77 \approx 231,000,000\,\text{m/s}$

$$P = 2 * 10 * 10^6\,\text{bps} * \frac{2{,}500\,\text{m}}{231{*}10^6\,\text{m/s}} \approx 217\ \text{bits} \approx 28\ \text{bytes}$$

- Outcome: The minimum frame length of 64 bytes for Ethernet is more than enough

Velocity Factor (Wave Propagation Speed)

- The **velocity factor**, also called wave propagation speed, depends on transmission medium and is:
  - 1 for vacuum
  - 0.64 for twisted pair cables Cat-5e
  - 0.66 for coaxial cables RG-58 ($\Longrightarrow$ Ethernet 10BASE2)
  - 0.67 for optical fiber
  - 0.77 for coaxial cables RG-8 ($\Longrightarrow$ Ethernet 10BASE5)
- 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:
  - $V = 231,000,000\,\text{m/s} = 231 * 10^6\,\text{m/s}$
  - Transmission duration t_{frame} = Transmission duration for a single bit, multiplied with the number of bits in a frame ($\Longrightarrow$ 512 Bits = 64 Bytes)
    - The transmission duration for a single bit at 10 Mbps is 0.1 microseconds
    - A frame with the minimum frame length of 64 Bytes requires 51.2μs for its complete transmission
  - A 51.2μs long frame travels in the coaxial cable the following distance: $231 * 10^6 \frac{\text{m}}{\text{s}} * 51.2 * 10^{-6}\text{s} = 11,827.20\,\text{m} = 11.83\,\text{km}$
    - Outcome: With a maximum network size of 2.5 km collision detection is possible

CSMA/CD nowadays

- The media access method **CSMA/CD is absolutely necessary** only for Ethernet networks, which implement the **bus network topology**
  - Reason: In a bus network topology, all network devices are directly connected to a shared transmission medium
- Almost all Ethernet-based networks nowadays are **fully switched networks** and therefore **collision-free**

Media Access Control Method CSMA/CA of WLAN

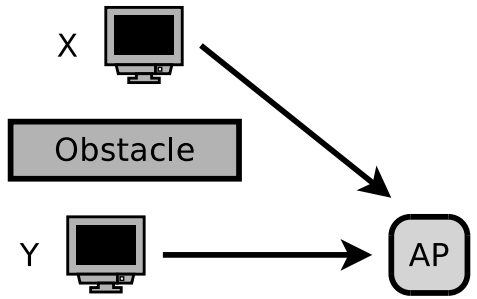
- CSMA/CD cannot be used with wireless networks
- With CSMA/CD, the sender detects occurring collisions
  - In wired networks with a shared transmission medium, each participant receives the transmissions of all other nodes
    - Therefore, each node detects any collision
  - For wireless networks like WLAN, this is not always the case
    - Therefore, the media access method *Carrier Sense Multiple Access / Collision Avoidance* (CSMA/CA) is used, which tries to **minimize** the occurrence of collisions
- Special challenges of the transmission medium in wireless networks cause undetected collisions at the receiver
  - **Hidden terminal problem**
  - **Fading**

LowerLAN / Powerline also uses CSMA/CA as media access method

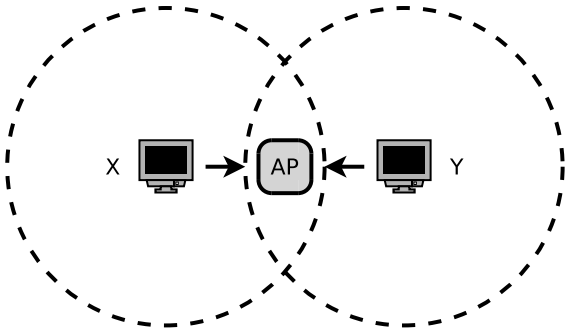
Source: Analysis of CSMA/CA used in Power Line Communication. *Martin Koutny, Petr Mlynek, Jiri Misurec*. IEEE (2013)

Special Characteristics of the Transmission Medium

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



- **Fading** (decreasing signal strength)
  - X and Y both send frames to the Access Point
  - The electromagnetic waves are weakened by obstacles and in free space
  - Caused by the positions of X and Y to each other, their signals are so weak, that the stations cannot 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 via random backoff time
   - Minimum spacing between frames, when a sequence of frames shall be transmitted
   - Acknowledgements – 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

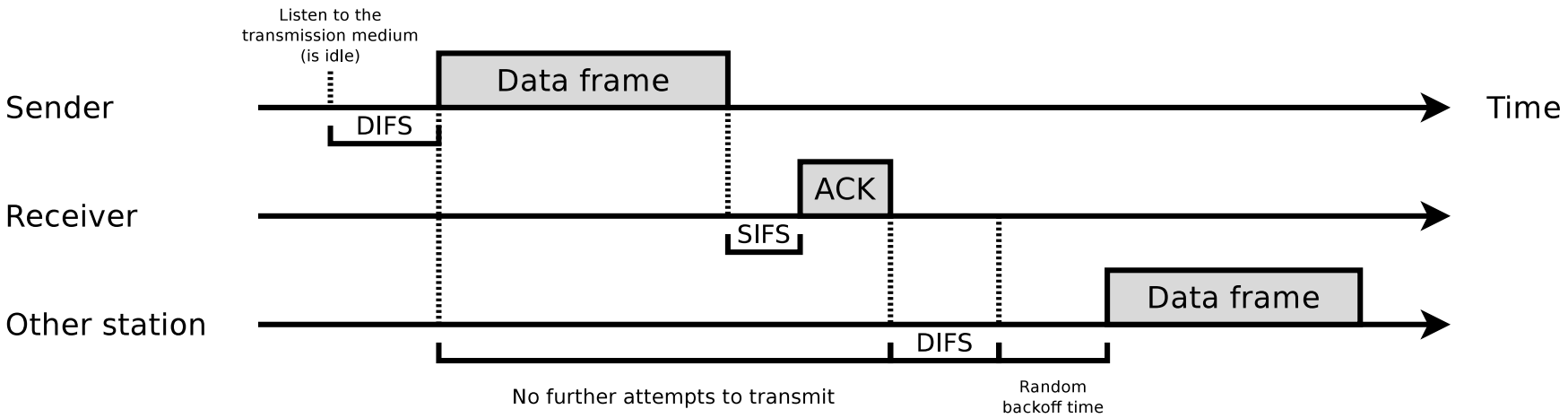
Source: Lecture slides of Prof. Dr. Michael Massoth and Wikipedia

Transmission of Frames

- If a node, which transmits frames, detects a collision via CSMA/CD (Ethernet), it aborts the transmission of the frame
- WLAN does not use collision detection, but with CSMA/CA it makes use of **collision avoidance** (actually it is just a **collision minimization**)
  - If a station started to transmit a frame, it will transmit the entire frame in any case
    - Once a station has started transmitting, there is no turning back
  - The sender must therefore be able to detect if a frame has not arrived correctly at the receiver
    - Solution: The receiver confirms by **ACK** that the frame was received correctly

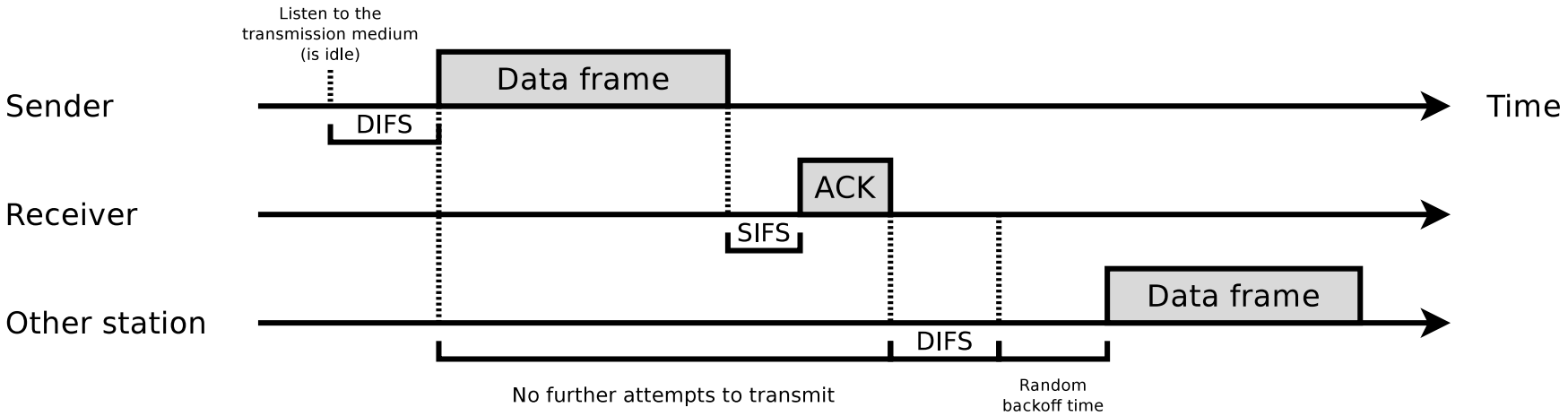
Functioning of CSMA/CA – 1/5

- First, the sender *listens* to the transmission medium ($\Longrightarrow$ 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 idle for the duration of 1 DIFS, the station can send start to transmit a frame



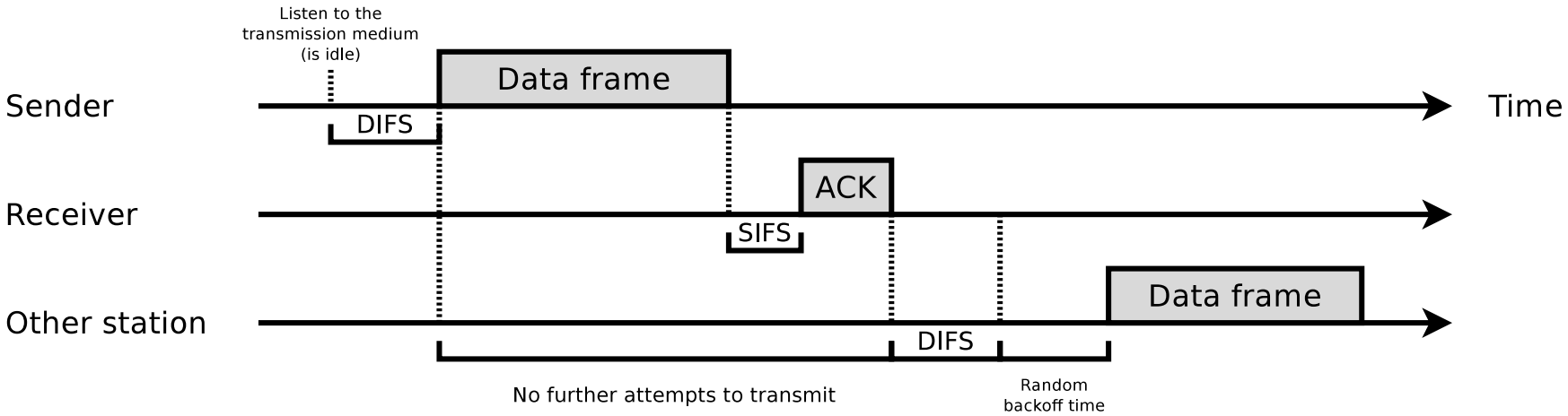
Functioning of CSMA/CA – 2/5

- If a station receives a frame, which passes the CRC check, it waits for a short period
  - This period is called **Short Interframe Spacing (SIFS)** $\approx 10\mu s$
  - Next, the receiver sends an **acknowledgement frame (ACK)**
- DIFS and SIFS guarantee for CSMA/CA a minimum spacing, when a sequence of frames shall be transmitted



Functioning of CSMA/CA – 3/5

- If another DIFS with an idle transmission medium has expired, a **backoff time** is calculated
  - The backoff time is calculated by using a random value between the minimum and maximum **contention window** and multiplying this random value with the **slot time**
    - After the backoff time has expired, the frame is transmitted



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

If during the backoff time period, another station occupies the transmission medium, the counter variable is stopped until the transmission medium is idle again for the duration of at least one DIFS.

Functioning of CSMA/CA – 4/5

- Minimum CW, maximum CW and slot time depend on the modulation method used and are fixed

Modulation method	SIFS	DIFS[1]	Slot Time	Minimal CW	Maximum CW
FHSS (802.11)	28 μs	128 μs	50 μs	15	1023
DSSS (802.11b)	10 μs	50 μs	20 μs	31	1023
OFDM (802.11a/h/n/ac)	16 μs	34 μs	9 μs	15	1023
OFDM (802.11g)[2]	16 μs	34 μs	9 μs	15	1023
OFDM (802.11g)[3]	10 μs	50 μs	20 μs	15	1023

[1] DIFS = SIFS + 2 * Slot Time
[2] Supports data rates 1-54 Mbps
[3] Supports only data rates > 11 Mbps

- The minimum and maximum CW values are always a power of 2, and from the result, value 1 is subtracted
  - If a WLAN uses e.g. the modulation method OFDM...
    - at the 1st attempt to transmit, the CW is ≥ 15 and ≤ 31
    - at the 2nd attempt to transmit, the CW is ≥ 31 and ≤ 63
    - at the 3rd attempt to transmit, the CW is ≥ 63 and ≤ 127

Functioning of CSMA/CA – 5/5

Modulation method	SIFS	DIFS[1]	Slot Time	Minimal CW	Maximum CW
FHSS (802.11)	28 μs	128 μs	50 μs	15	1023
DSSS (802.11b)	10 μs	50 μs	20 μs	31	1023
OFDM (802.11a/h/n/ac)	16 μs	34 μs	9 μs	15	1023
OFDM (802.11g)[2]	16 μs	34 μs	9 μs	15	1023
OFDM (802.11g)[3]	10 μs	50 μs	20 μs	15	1023

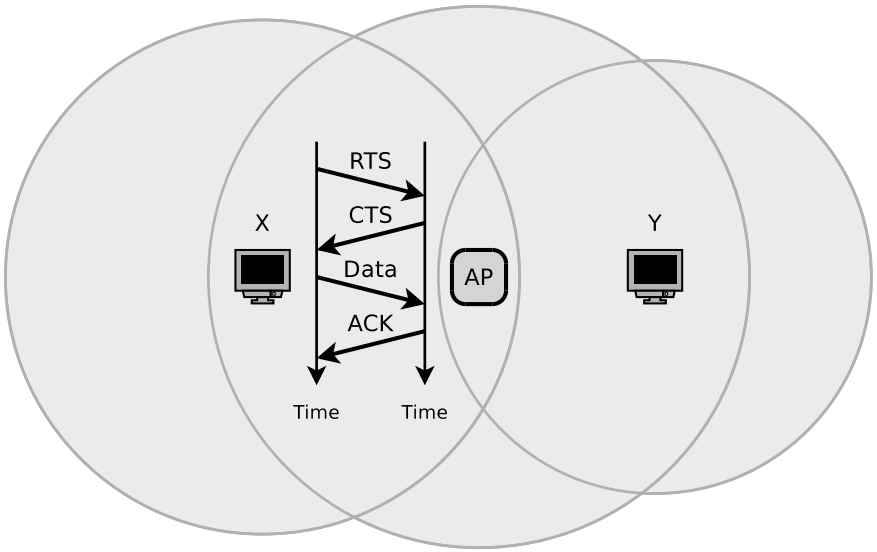
[1] DIFS = SIFS + 2 * Slot Time
[2] Supports data rates 1-54 Mbps
[3] Supports only data rates > 11 Mbps

- Further transmission attempts cause the CW to rise exponentially until the maximum value is reached
- As soon as a transmission of a frame was successful and the frame has been acknowledged via ACK, the lower bound of the CW is set to the minimum CW value in the table

Source: Wireless LANs, *Jörg Rech*, Heise (2012)

CSMA/CA RTS/CTS

- CSMA/CA reduces the number of collisions
  - But it cannot avoid all collisions
- A **better collision avoidance** implements CSMA/CA RTS/CTS
  - Concept: Sender and receiver exchange **control frames** first
    - This way, all stations in the network learn that a transmission will start soon
  - Control frames: **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 (see slides 28 + 29)



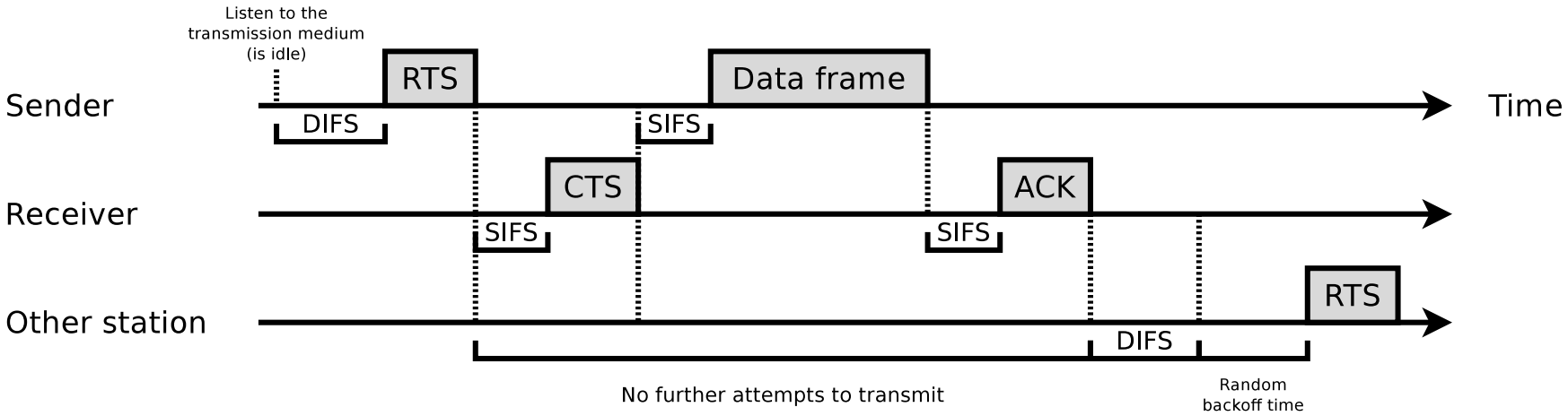
- Collisions can only occur during the transmission of RTS and CTS frames
  - Because of the hidden terminal problem

Figure on left side...

Station Y cannot receive the RTS frame from X, but the CTS frame from the Access Point

Functioning of CSMA/CA RTS/CTS – 1/3

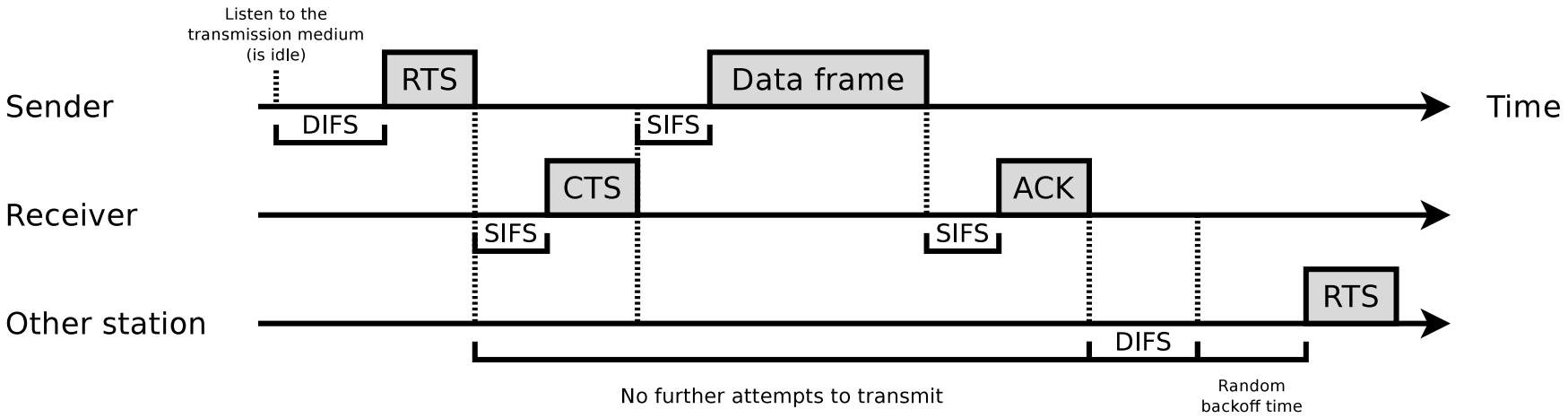
- After the DIFS, the sender transmits a **RTS** frame to the receiver
  - The RTS frame contains a field, which specifies the period, the sender wants to reserve (use) the transmission medium (the channel) to transmit the frame



- The receiver acknowledges the reservation request by waiting the SIFS and then transmitting a **CTS** frame, which also contains the period of time, the sender wants to reserve the transmission medium
  - The receiver confirms this way the period which is required to transmit the data frame

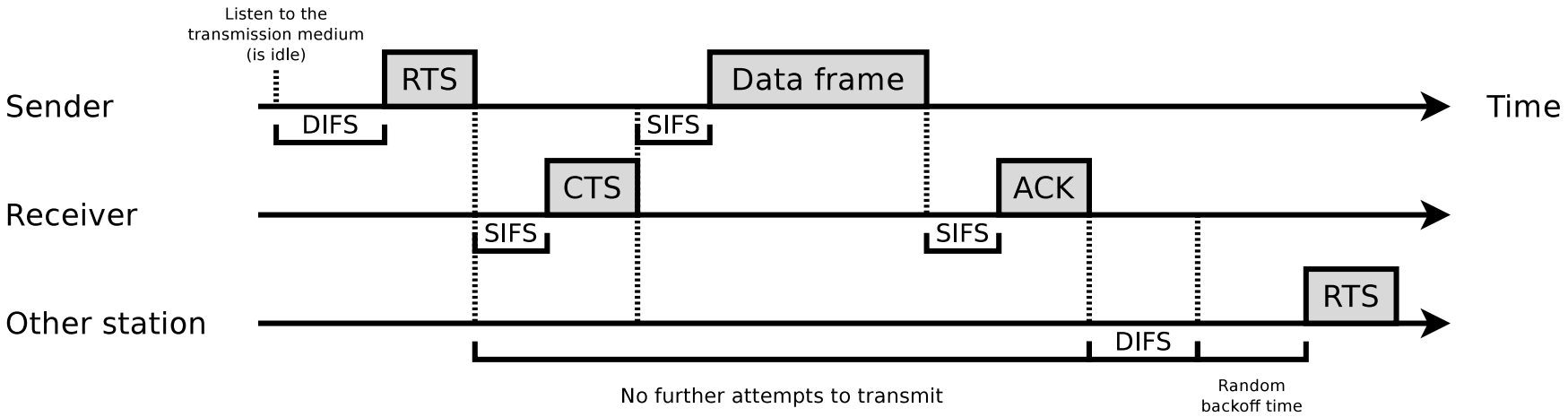
Functioning of CSMA/CA RTS/CTS – 2/3

- After the receiver successfully received the data frame, it waits for the period of a SIFS and transmits an ACK frame to the sender



- if the transmission medium (the channel) is occupied, no further station tries to transmit a frame, until the end of the **Network Allocation Vector (NAV)**
  - The NAV is a counter variable that each station manages by itself
    - Reduces the number of collisions
    - Contains the expected occupation time of the transmission medium
    - Is decremented over time, until it reaches value 0

Functioning of CSMA/CA RTS/CTS – 3/3



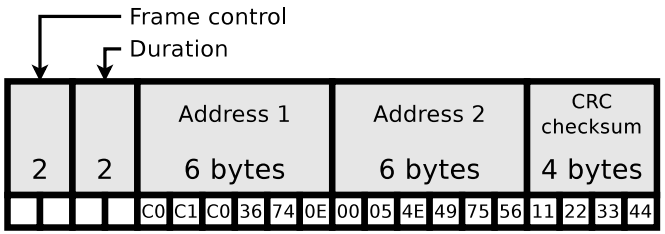
- Advantages
  - **Fewer collisions**, because it solves the problem of hidden terminals
  - **Less energy consumption**, because no transmission attempts during NAV
- Drawbacks:
  - The reservation of the transmission medium causes **delays**
  - The RTS and CTS frames are **overhead**

WLAN Control Frames (Special Frames) – RTS Frame

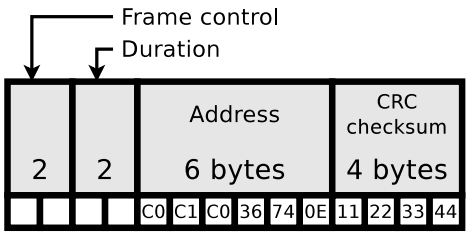
The control frames RTS, CTS and ACK have a different structure compared with data frames

- Length of **RTS frames**: 20 bytes
- With the RTS frame, a station, which wants to transmit frames, **sends a reservation request** for the transmission medium to the Access Point
- 1st address field = MAC address of the Access Point
- 2nd address field = MAC address of the station, which sends the request

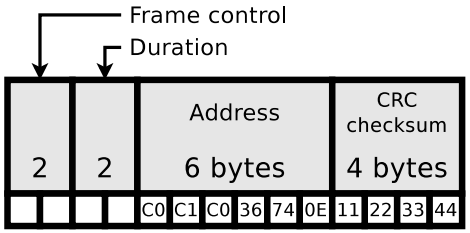
RTS frame



CTS frame



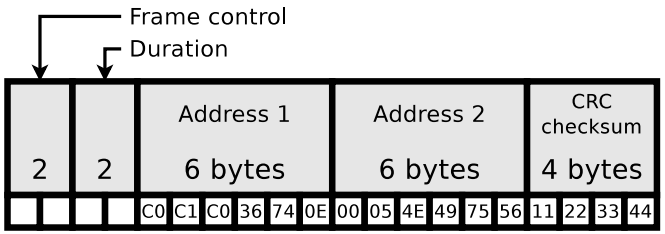
ACK frame



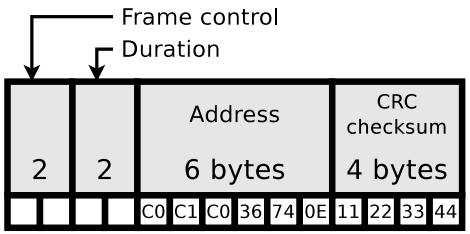
WLAN Control Frames (Special Frames) – CTS Frame

- Length of **CTS frames**: 14 bytes
- With a CTS frame, an Access Point **confirms the reservation request** for the transmission medium
- `address` = MAC address of the station, which sent the reservation request

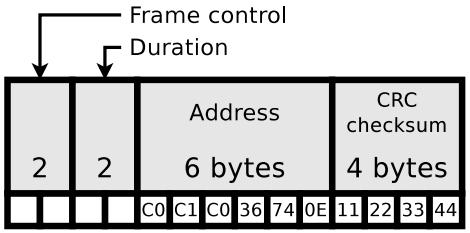
RTS frame



CTS frame



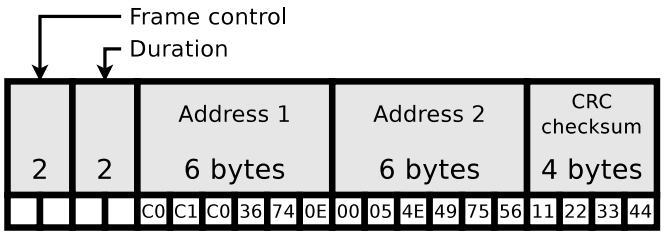
ACK frame



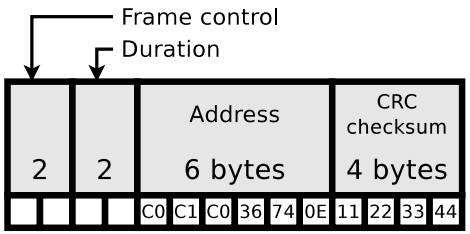
WLAN Control Frames (Special Frames) – ACK Frame

- Length of **ACK frames**: 14 bytes
- With an ACK frame, the receiver **confirms the successful transmission of a frame** at the sender
- `address` = MAC address of the station, which transmitted the frame successfully

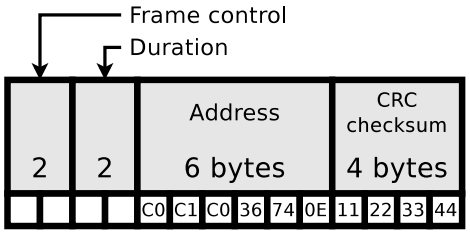
RTS frame



CTS frame



ACK frame



CSMA/CA RTS/CTS in Practice

- CSMA/CA RTS/CTS is optional for WLAN but mostly implemented
  - In practice, it is used for reserving channels for the transmission of large payload frames
- For each station, a RTS threshold value can be specified (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 left out for all transmitted payload frames

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

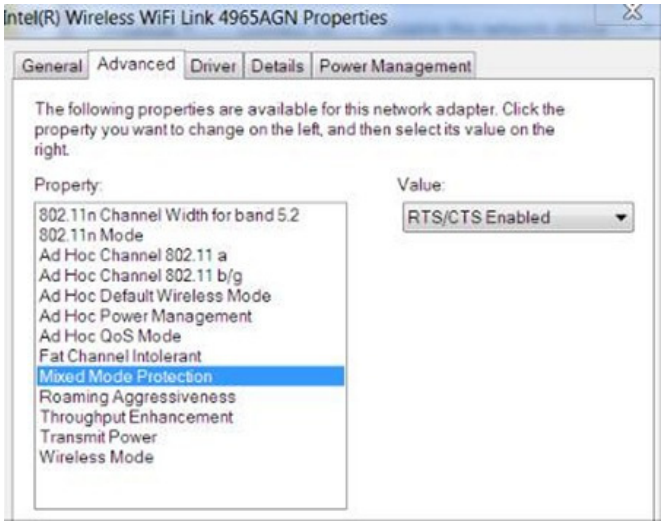
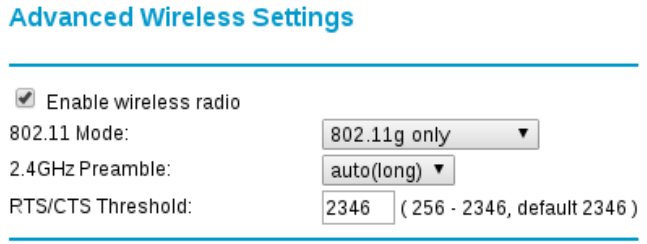


Image source: `http://www.itedge.net`



Screenshot from the web gui of a Netgear WGPS606 wireless router

CSMA/CA PCF

- **PCF** = **P**oint **C**oordination **F**unction
- The Access Point controls the media access
  - It requests the registered stations to transmit payload 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

Functioning of ARP (1/2)

- The **Address Resolution Protocol** (ARP) is used to resolve IP addresses of the Network Layer to MAC address of the Data Link Layer
- If a network device wants to transmit data to a receiver, it uses the receiver's IP address on the Network Layer
- But on the Data Link Layer, the MAC address is required
  - Therefore, **address resolution** must be carried out in the Data Link Layer
  - To find out the MAC address of a network device in the LAN, ARP sends a frame with the MAC broadcast address `FF-FF-FF-FF-FF-FF` as destination address
    - Each network device in the LAN receives and analyzes this frame
    - The frame contains the IP address of the searched network device
  - If a network device has this IP address, it sends an ARP response to the sender
    - The reported MAC address stores the sender in its local ARP cache

Functioning of ARP (2/2)

- The **ARP cache** is used to speed up the address resolution
  - It contains a table with these information for each entry:
    - Protocol type (IP)
    - Protocol address of the sender (IP address)
    - Hardware address of the sender (MAC address)
    - Time To Live (TTL)
  - The TTL is set by the operating system
  - If an entry in the table is used, the TTL is extended
- Modern Linux distributions discard entries after $\approx$ 5 minutes

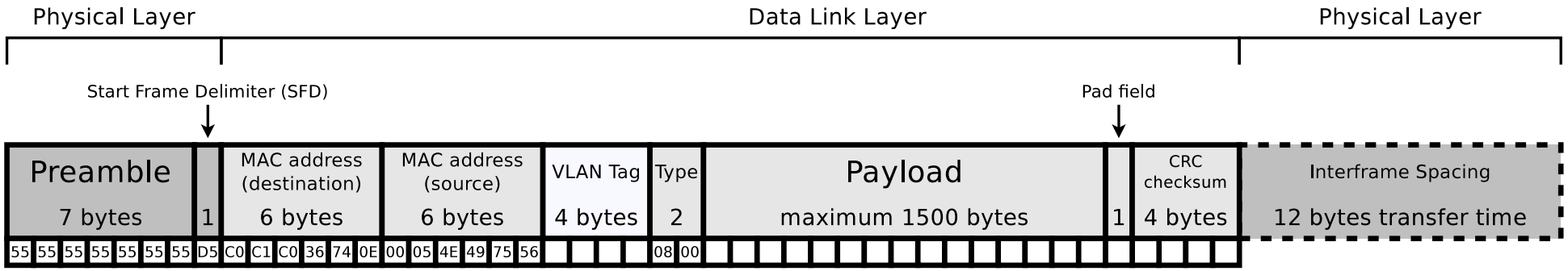
The ARP cache can be displayed via `arp -n` or `ip neighbour`

```
# 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
```

Address resolution requests can be send manually via `arping`

Structure of ARP Messages

- ARP messages are transmitted as payload via Ethernet frames
  - `type` = `0x0806` (for the ARP protocol)



- `HLEN` = hardware address (MAC address) length in bytes
  - For Ethernet: 6 bytes
- `PLEN` = IP address length in bytes
  - For IPv4: 4 bytes

32 bits (4 bytes)

Hardware type		Protocol type
HLEN	PLEN	Operation
MAC address (sender)		
MAC address (sender)		IP address (sender)
IP address (sender)		IP address (target)
IP address (target)		MAC address (target)
MAC address (target)		

In an ARP request is the content of the field `MAC address (target)` irrelevant