Technische Universität Berlin

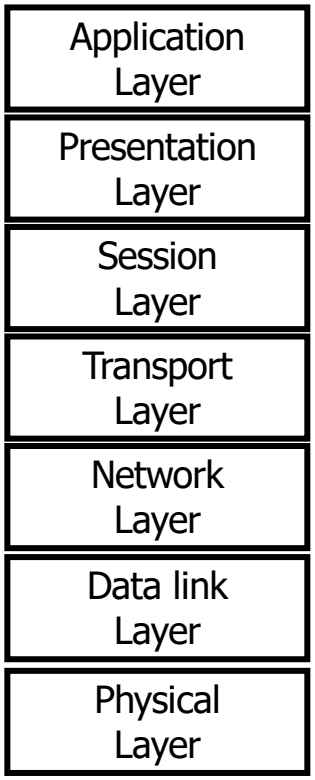
Computer Networks

WLAN

Chapter

1. Introduction
2. Protocols
3. Application layer
4. Web services
5. Distributed hash tables
6. Time synchronization
7. Error control
8. Transport layer
9. Network layer
10. Internet protocol
11. Data link layer
12. **WLAN**
    - **Architecture**
    - **Protocol**

Top-Down-Approach



Wireless LAN

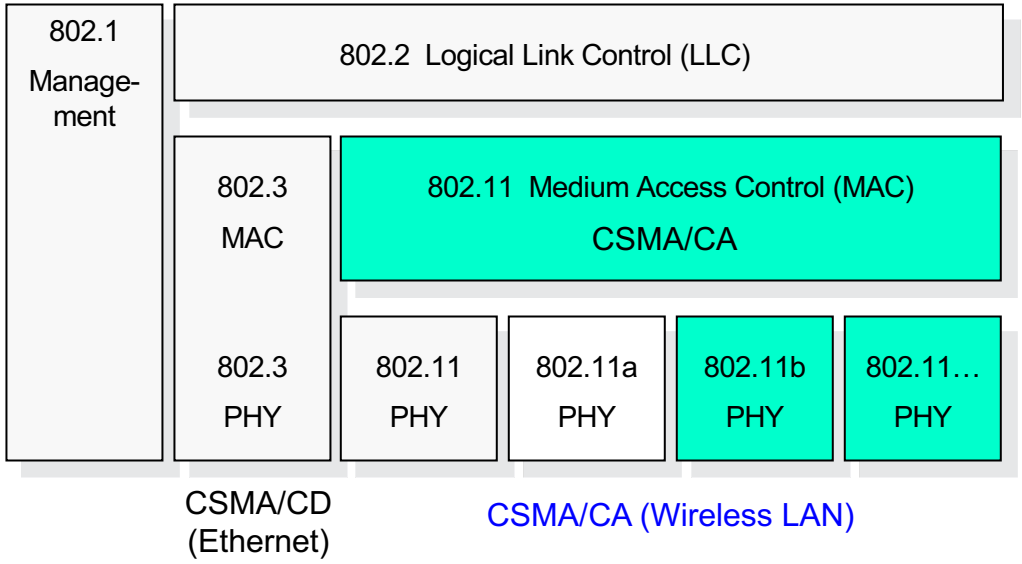
Wireless LAN

- Characteristics of wireless communications
  - Attenuation of the signal, at least quadratically with distance, strongly depending on environment → slow fading
  - Multi-path propagation: radio waves are reflected, phase shifted copied of the wave overlap, constructive or destructive interference → fast fading
  - Interference by other senders (many different wireless communication technologies, microwave oven, engines, …)
  - Higher error rates, usually in bursts

Wireless LAN

- WLAN according to IEEE 802.11
  - Initially 1-2 Mbps, radio (Direct Sequence Spread Spectrum, DSSS), also infrared
  - Continuous further development and standardization, e.g., 11b (11 Mbps), 11g (54 Mbps), 11i (security), 11e (quality-of-service), 11p (car-to-X), 11n (>54 Mbps), 11ac (>300 Mbps), 11ax (>1 Gbps), …
  - 3 operation modes: infrastructure network (access points, distribution service), ad hoc network, broadcast (OCB mode)
  - Medium access: CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
    - 2 Variants: Basic Access, RTS/CTS
  - Energy savings: sleep phases, synchronized wake-up

IEEE 802.x framework



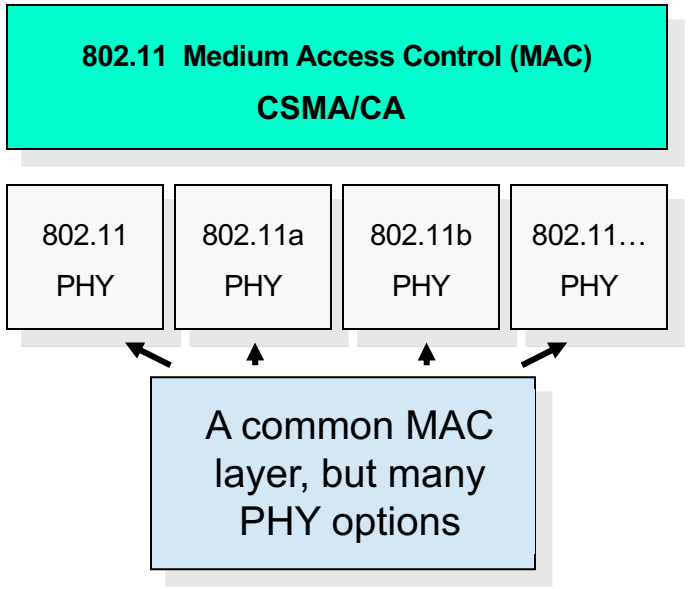
CSMA/CA Wireless LAN

CSMA/CA = Carrier Sense Multiple Access with Collision Avoidance

Unlike wired LAN stations, WLAN stations cannot detect collisions

→

avoid collisions (use "backoff procedure" as described later)

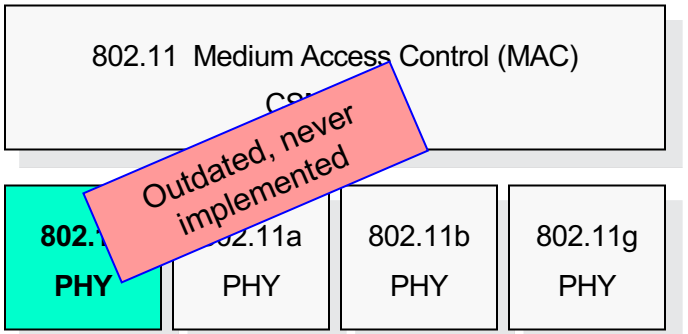


WLAN physical layer (1)

FHSS (Frequency Hopping Spread Spectrum)

DSSS (Direct Sequence Spread Spectrum)

Data rates supported:
1 and 2 Mbit/s.



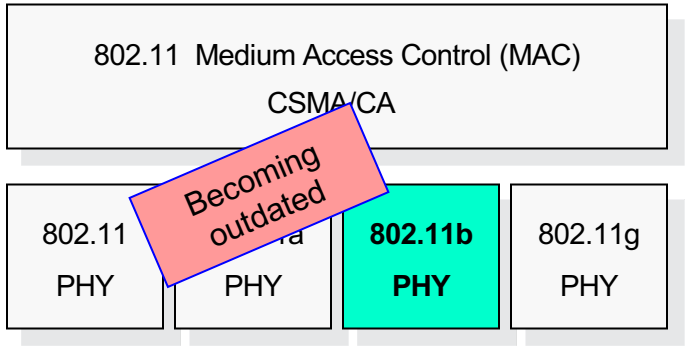
ISM band: 2.4 … 2.4835 GHz

WLAN physical layer (2)

The first widely implemented physical layer was 802.11b that uses:

DSSS (Direct Sequence Spread Spectrum) like in 802.11 but with larger bit rates:
1, 2, 5.5, 11 Mbit/s

Automatic fall-back to lower bitrates in case of bad radio channel.



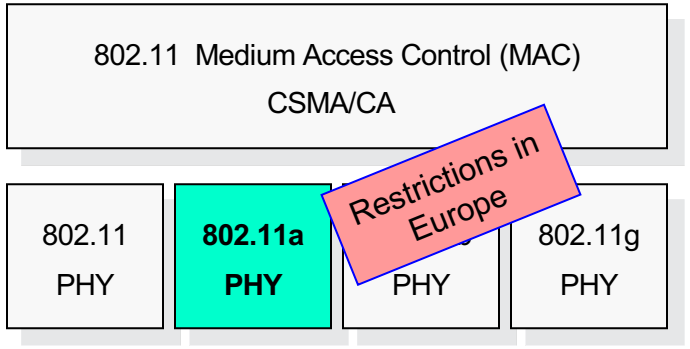
ISM band: 2.4 … 2.4835 GHz

WLAN physical layer (3)

802.11a operates in the 5.8 GHz band.

The signal format is OFDM (Orthogonal Frequency Division Multiplexing)

Data rates supported: Various bit rates from 6 to 54 Mbit/s.

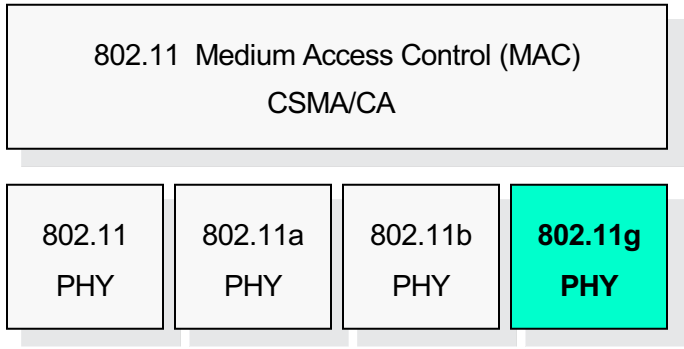


5 GHz frequency band

WLAN physical layer (4)

Starting with 802.11g, OFDM is the most recent physical layer, operating in different frequency bands

The signal format is OFDM (Orthogonal Frequency Division Multiplexing)



Wireless LAN

- Standardized variants

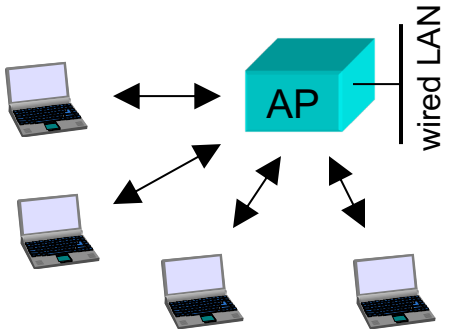
Standard	Frequenzband	Modulation	MIMO	Bandbreite	Datenrate
IEEE 802.11	2,4 GHz	FHSS, DSSS	–		2 Mbit/s
IEEE 802.11b	2,4 GHz	CCK, QPSK	–	22 MHz	11 Mbit/s
IEEE 802.11g	2,4 GHz	CCK, QAM64	–	20 MHz	54 Mbit/s
IEEE 802.11n	2,4 GHz oder 5 GHz	QAM64	4×4	40 MHz	600 Mbit/s
IEEE 802.11a	5 GHz	QAM64	–	20 MHz	54 Mbit/s
IEEE 802.11ac	5 GHz	QAM256	8×8	160 MHz	6,9 Gbit/s
IEEE 802.11ad	60 GHz	QAM64	–	2 GHz	6,7 Gbit/s
IEEE 802.11ax / Wi-Fi 6	5 GHz (and further license free bands 1-6 GHz)	QAM1024	8x8 + MU-MIMO	160 MHz	11 Gbit/s aggregated

IEEE 802.11 WLAN

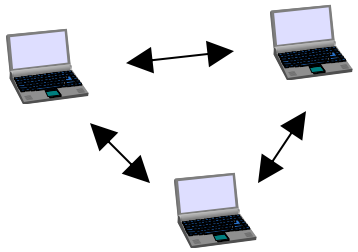
IEEE 802.11 WLAN Architecture

802.11 defines two BSS (Basic Service Set) options:

Infrastructure BSS



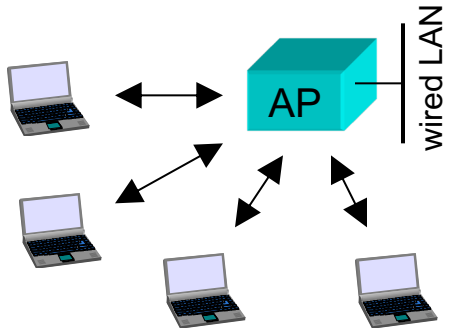
Independent BSS (Ad-Hoc network)



Infrastructure BSS

This is by far the most common way of implementing WLANs.

Infrastructure BSS



The base stations connected to the wired infrastructure are called access points (AP).

Wireless stations in an Infrastructure BSS must always communicate via the AP (never directly).

Before stations can use the BSS: Association.

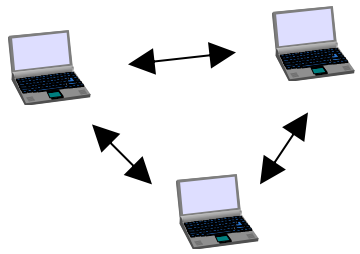
Independent BSS

Mainly of interest for military applications.

No access point is required, stations can communicate directly.

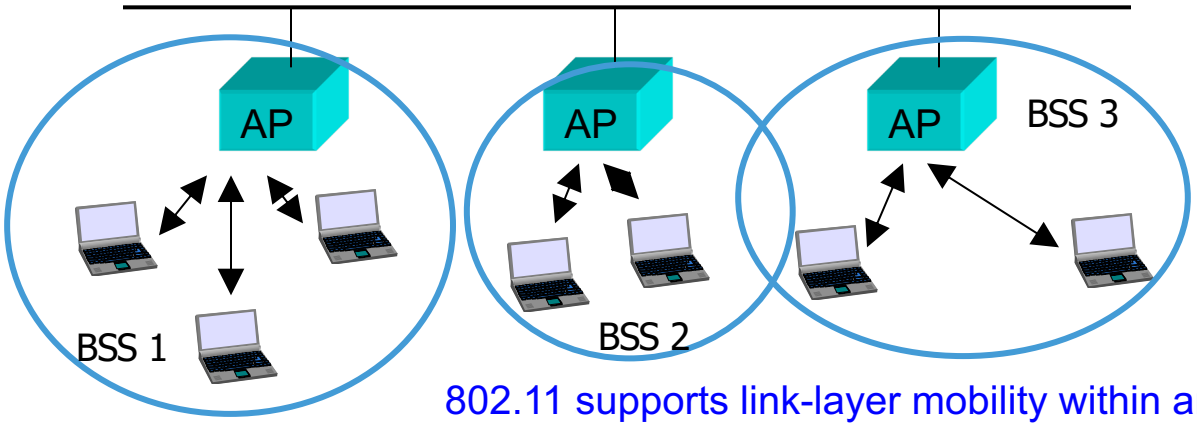
Efficient routing of packets is not a trivial problem (routing is not a task of 802.11).

Independent BSS (Ad-Hoc network)



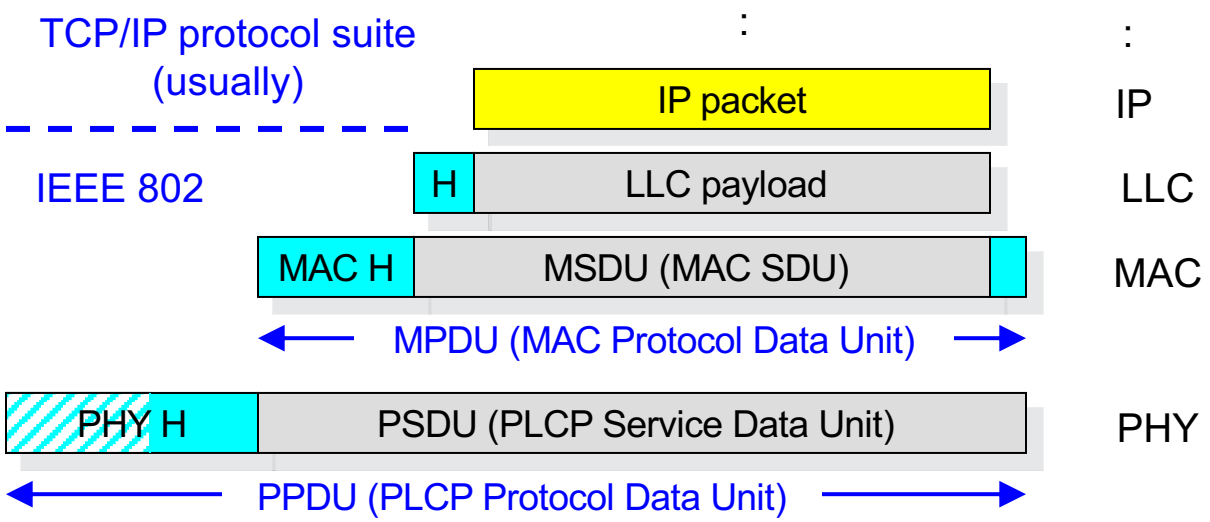
Extended Service Set (ESS)

This is a larger WLAN network consisting of a number of BSS networks interconnected via a common backbone

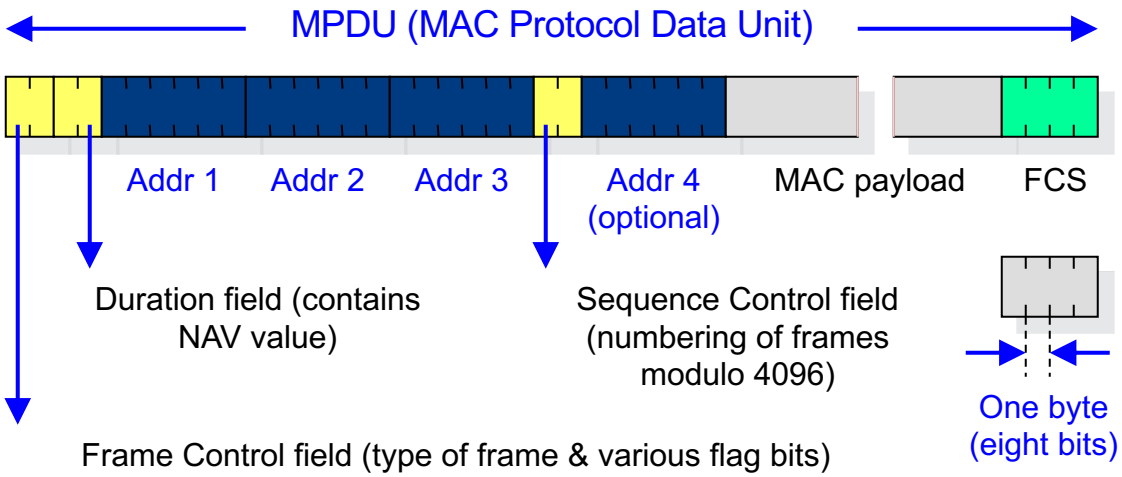


802.11 supports link-layer mobility within an ESS (but not outside the ESS)

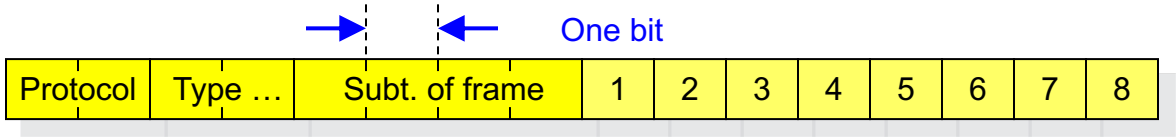
IEEE 802.11 frame structure



MAC header structure



Content of Frame Control Field

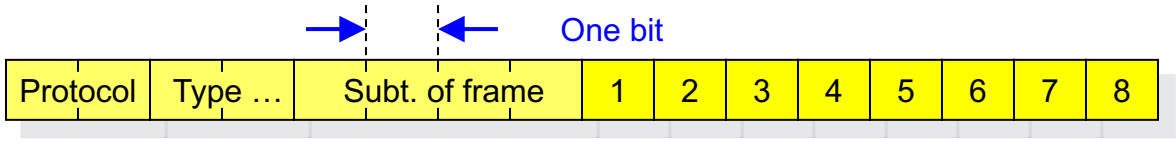


Protocol: Indicates IEEE 802.11 MAC

Type: 00 (Management frames)
01 (Control frames)
10 (Data frames)

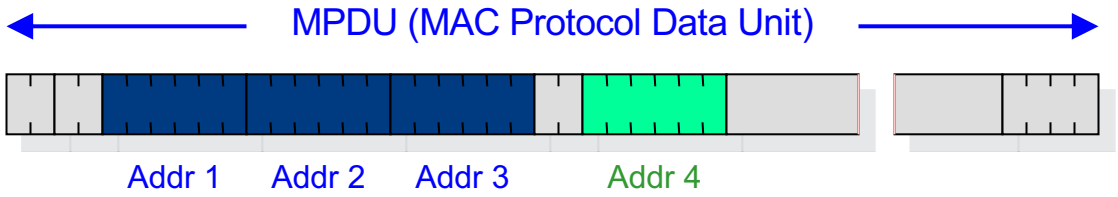
Subtype of frame: Describes type of management, control, or data frame in more detail (e.g. ACK => 1101)

Flags in Frame Control field



1: Bit is set if frame is sent to AP
2: Bit is set if frame is sent from AP
3: Used in fragmentation
4: Bit is set if frame is retransmitted
5: Power management bit (power saving operation)
6: More data bit (power-saving operation)
7: Bit is set if WEP is used
8: Strict ordering of frames is required

Usage of MAC address fields

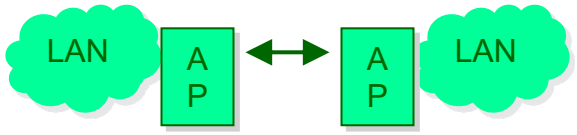


Address 1: Receiver (wireless station or AP)

Address 2: Sender (wireless station or AP)

Address 3: Ultimate source/destination (router in DS)

Address 4: Only used in Wireless Bridge solutions:

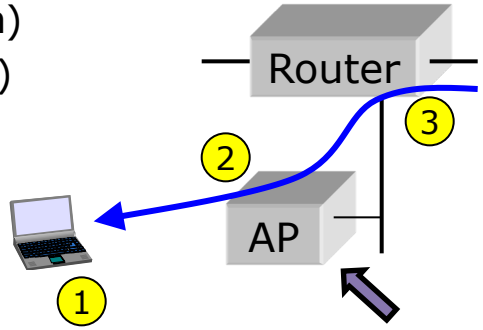


Direction: AP → wireless station

Frame created at AP:

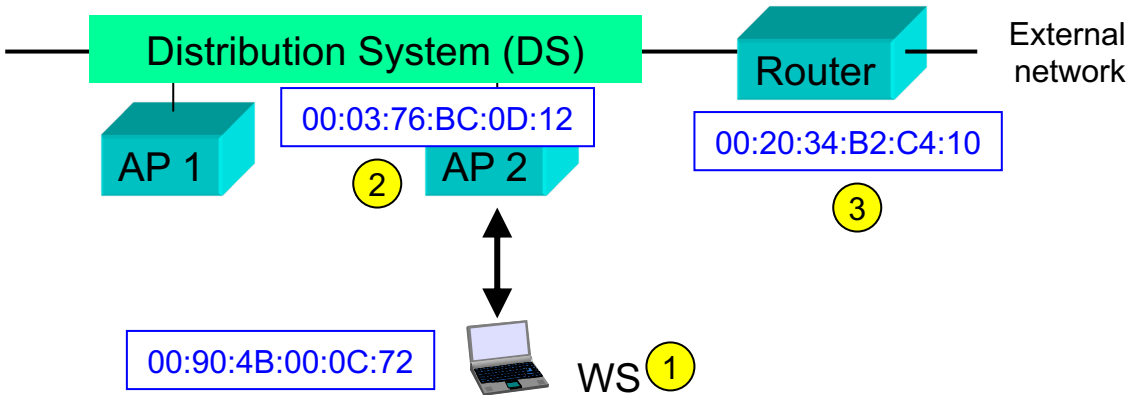
Addr 1: Receiver (wireless station)
Addr 2: Transmitter = BSSID (AP)
Addr 3: Ultimate source (router)

BSSID: MAC address of AP
SSID: Alphanumeric name of AP (or BSS)



MAC addressing example

Frames to the WS must also include the MAC address of the ”ultimate source” to which return frames should be routed (then ”ultimate destination”).



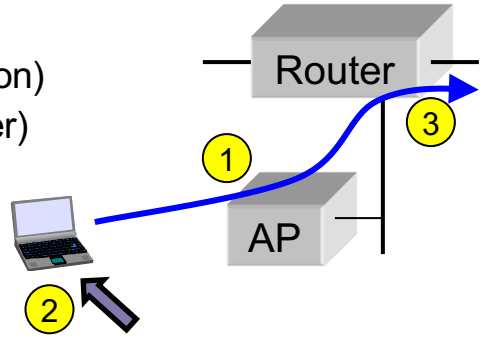
Direction: Wireless station → AP

Frame created at station:

Addr 1: Receiver = BSSID (AP)

Addr 2: Transmitter (wireless station)

Addr 3: Ultimate destination (router)



Management frames

- In addition to the data frames (containing the user data to be transported over the 802.11 network) and control frames (e.g., acknowledgements), there are a number of management frames.
- Note: that these management frames compete for access to the medium in equal terms (using CSMA/CA) with the data and control frames.
- Some of these management frames are presented on the following slides.

Beacon frames

- Beacon frames are **broadcast** (meaning that all stations shall receive them and read the information) at regular intervals from the Access Point. These frames contain (among others) the following information:
  - Timestamp (8 bytes) is necessary, so that stations can synchronise to the network
  - Beacon interval (2 bytes) in milliseconds
  - Capability info (2 bytes) advertises network capabilities
  - SSID (0 ... 32 bytes), alphanumeric “network name”
  - The channel number used by the network (optional).

Probe request & response frames

- A **probe request** frame is transmitted from a wireless station during **active scanning**. Access points within reach respond by sending **probe response** frames.
- Probe request frames contain the following information:
  - SSID (0 ... 32 bytes), alphanumeric “network name”
  - Bit rates supported by the station. This is used by APs to see if the station can be permitted to join the network.
- Probe response frames actually contain the same kind of “network information” as beacon frames.

Association request & response frames

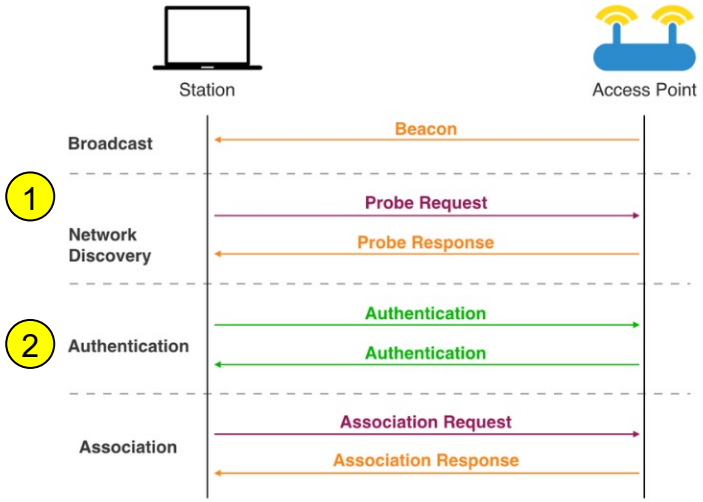
- Before a station can join an 802.11 network, it must send an **association request** frame. The AP responds with an **association response** frame.
- Association request frames contain (among others):
  - SSID, capability info, bit rates supported.
- Association response frames contain (among others):
  - Capability info, bit rates supported
  - Status code (success or failure with failure cause)
  - Association ID (used for various purposes)

Passive and active scanning

- Wireless stations can find out about 802.11 networks by using passive or active scanning.
- During **passive scanning**, the station searches beacon frames, moving from channel to channel through the complete channel set (802.11b => 13 channels).
- During **active scanning**, the station selects Channel 1 and sends a probe request frame. If no probe response frame is received within a certain time, the station moves to Channel 2 and sends a probe request frame, and so on.

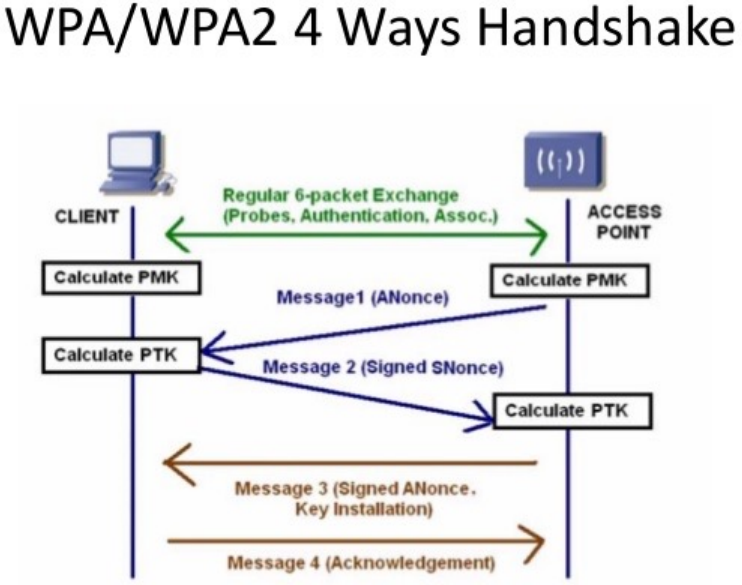
Station connecting to a WLAN

- When a station moves into the coverage area of a WLAN, the following procedures take place:
  1. **Scanning**: the station searches for a suitable channel over which subsequent communication takes place
  2. **Authentication**: open-system or shared key (WEP) - optional
  3. **Association**: the station associates with an AP
  4. **IP address allocation**: the station gets an IP address, for instance from a DHCP server



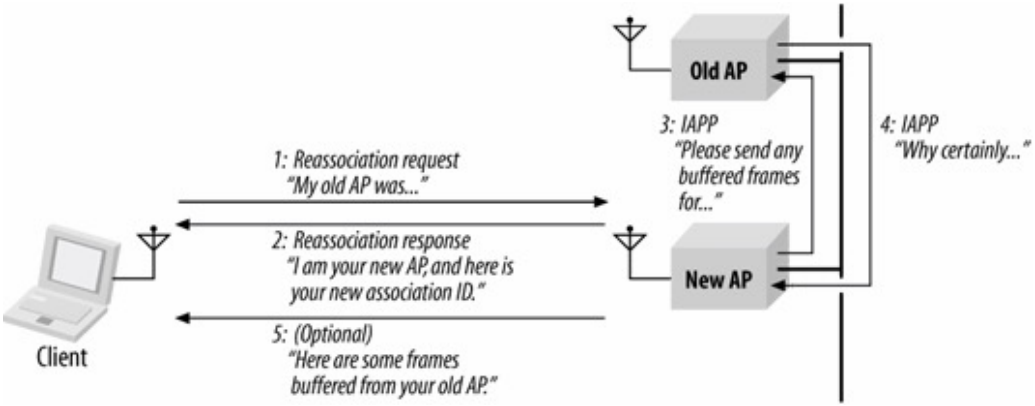
Optional WPA2 4 Way Handshake

- WPA2 (Wi-Fi Protected Access 2) is a network security technology commonly used on WLAN wireless networks.
- Used since 2006 and is based on the IEEE 802.11i technology standard for **data encryption**.



Handover to another AP

- When a station has noticed that the radio connection to another AP is a better than the existing connection:
  - **Reassociation**: the station associates with another AP
  - No new IP address is needed; however, the WLAN must be able to route downlink traffic via the new AP
  - **Authentication**: this security option, if required, will result in a substantially increased handover delay (complete procedure sequence: deauthentication, disassociation, reassociation, authentication).



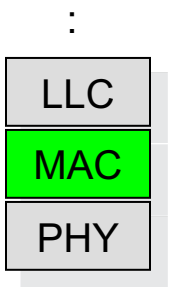
WLAN Medium Access Control

Medium Access Control (MAC)

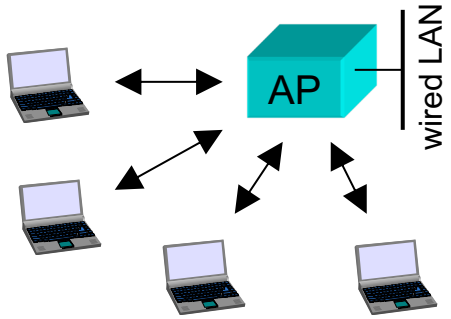
Medium access control: Different nodes must gain access to the shared medium (for instance a wireless channel) in a controlled fashion (otherwise there will be collisions).

Access methods:

FDMA	Assigning channels in frequency domain
TDMA	Assigning time slots in time domain
CDMA	Assigning code sequences in code domain
CSMA	Assigning transmission opportunities in time domain on a statistical basis



Basic wireless medium access



CSMA:
One packet at a time

We shall next investigate Infrastructure BSS only.

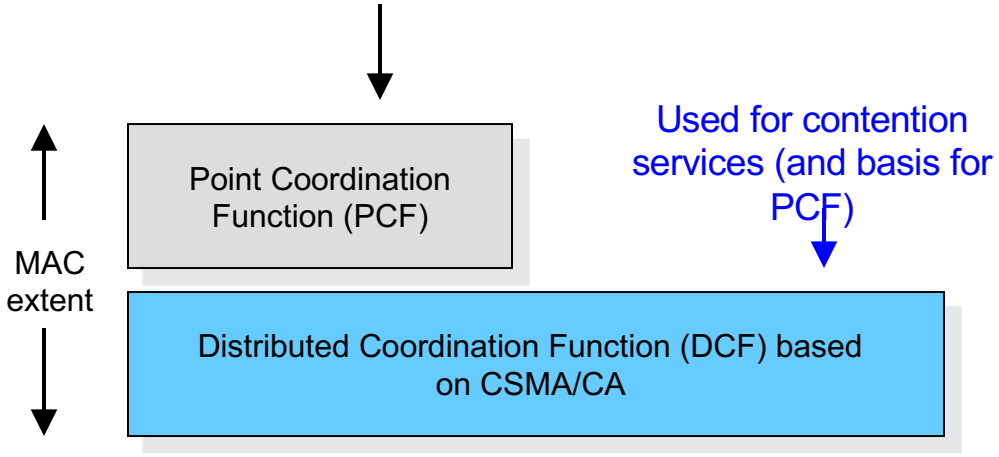
As far as medium access is concerned, all stations and AP have equal priority

⇔

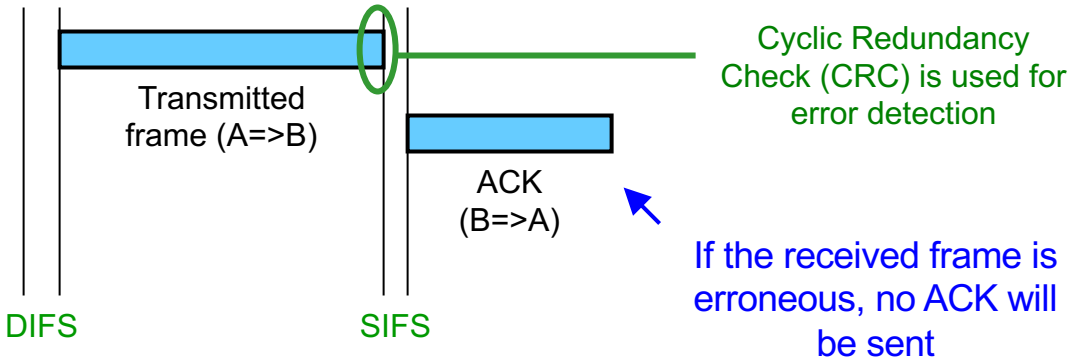
transmission in downlink (from the AP) and uplink (from a station) is similar.

DCF (CSMA/CA) vs. PCF

Designed for contention-free services (delay-sensitive real-time services such as voice transmission), but has not been implemented (yet)

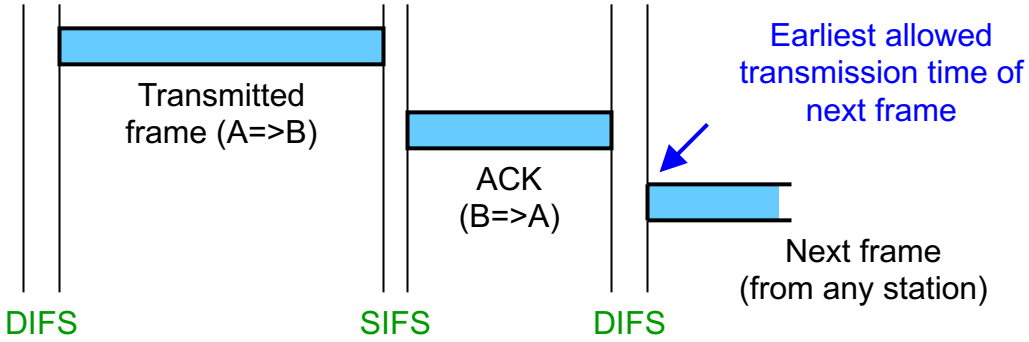


Wireless medium access



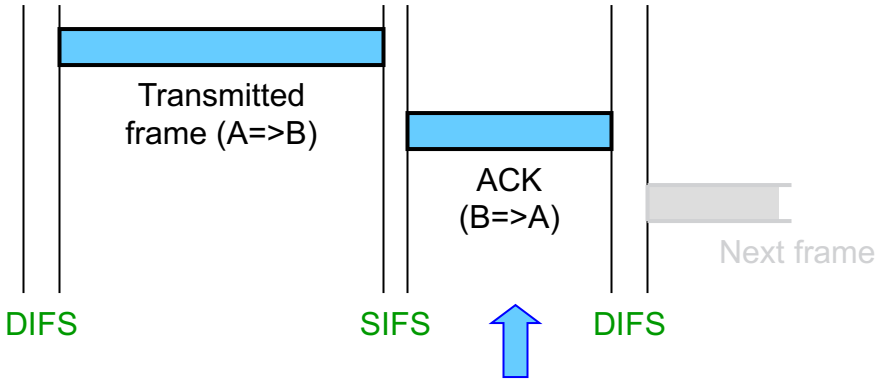
When a frame is received without bit errors, the receiving station (B) sends an Acknowledgement (ACK) frame back to the transmitting station (A).

Wireless medium access (2)



During the transmission sequence (Frame + SIFS + ACK) the medium (radio channel) is reserved. The next frame can be transmitted at earliest after the next DIFS period.

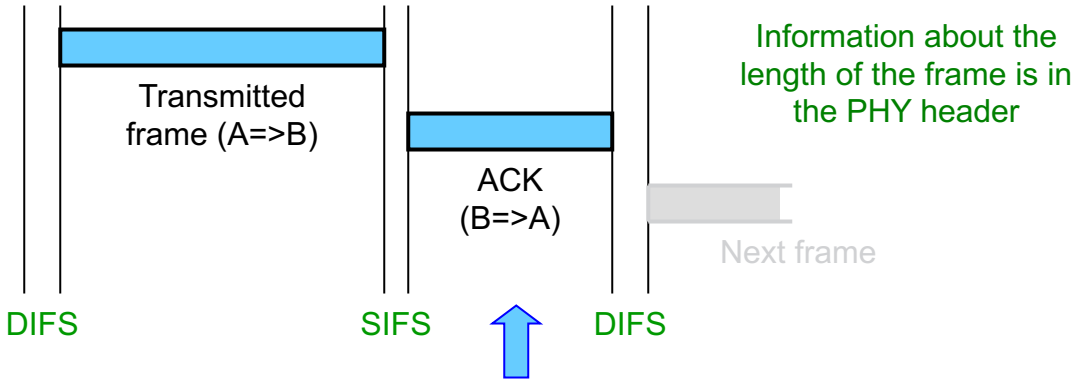
Wireless medium access (3)



There are two mechanisms for reserving the channel:

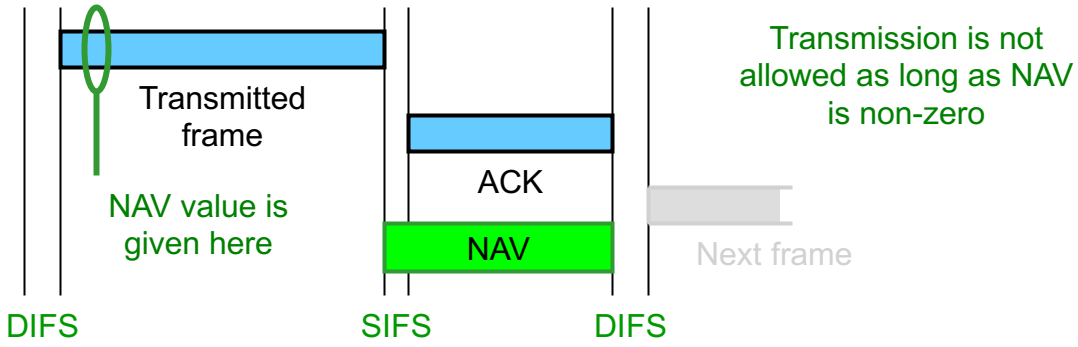
Physical carrier sensing and Virtual carrier sensing using the so-called Network Allocation Vector (NAV).

Wireless medium access (4)



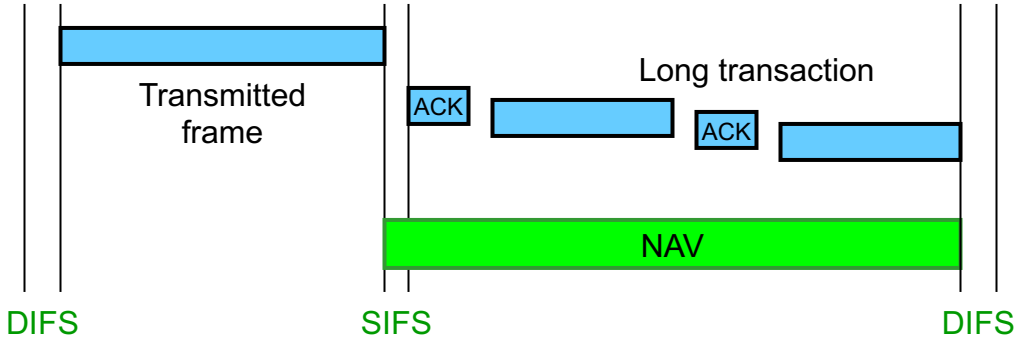
Physical carrier sensing means that the physical layer (PHY) informs the MAC layer when a frame has been detected. Access priorities are achieved through interframe spacing.

Wireless medium access (6)



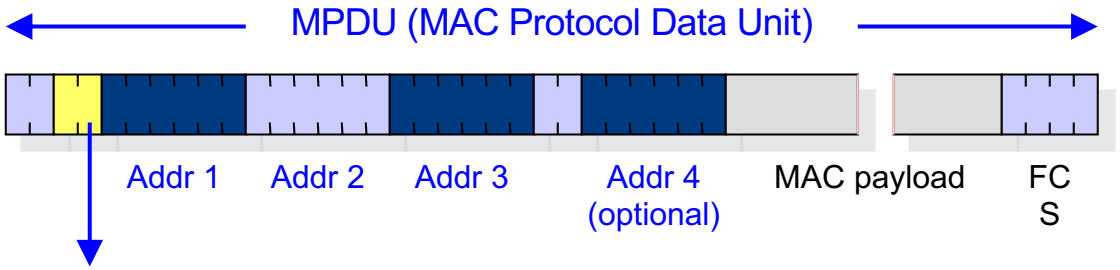
Virtual carrier sensing means that a NAV value is set in all stations that were able to receive a transmitted frame and were able to read the NAV value in this frame.

Wireless medium access (7)



Virtual carrier sensing using NAV is important in situations where the channel should be reserved for a ”longer time” (RTS/CTS usage, fragmentation, etc.).

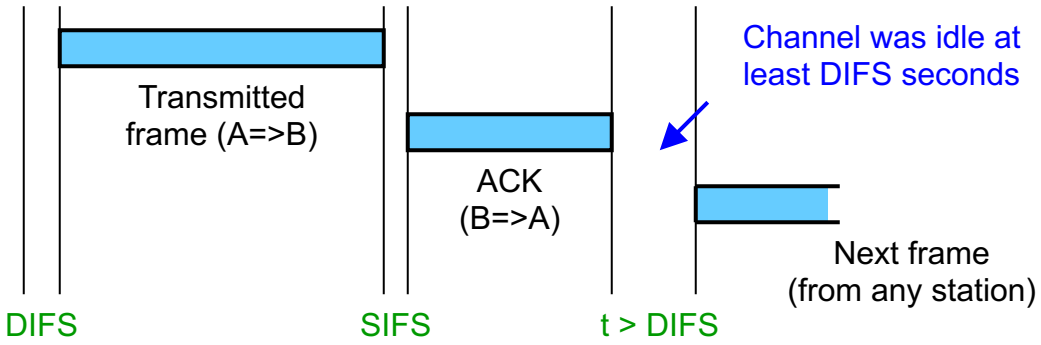
NAV value is carried in MAC header



Duration field: 15 bits contain the NAV value in number of microseconds. The last (sixteenth) bit is zero.

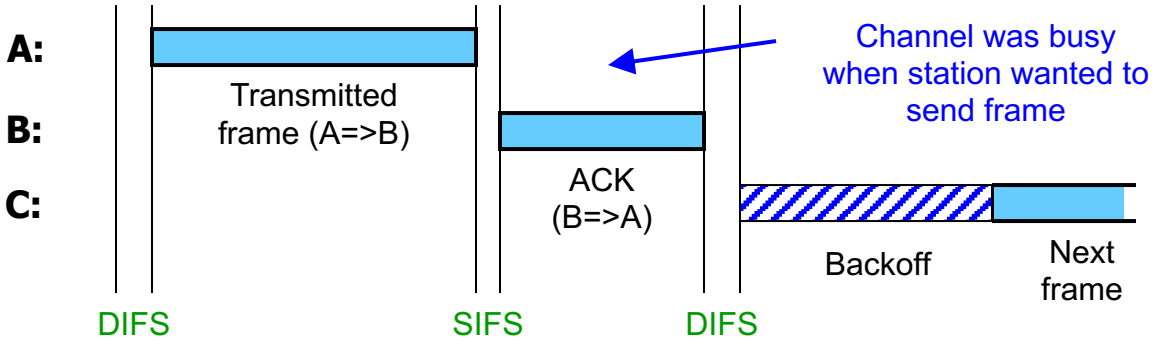
All stations must monitor the headers of all frames they receive and store the NAV value in a counter. The counter decrements in steps of one microsecond. When the counter reaches zero, the channel is available again.

Wireless medium access (8)



When a station wants to send a frame and the channel has been idle for a time > DIFS (counted from the moment the station first probed the channel) => can send immediately.

Wireless medium access (9)

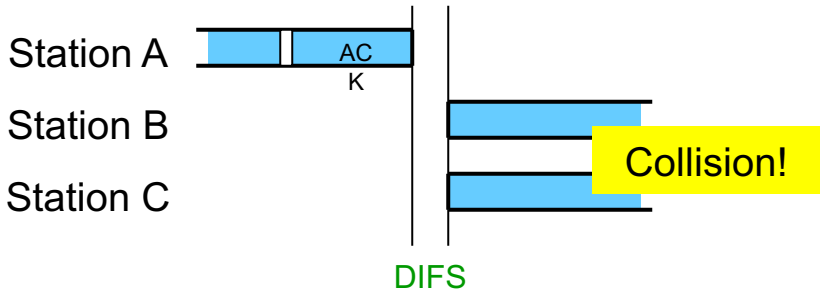


When a station wants to send a frame and the channel is busy => the station must wait a backoff time before it is allowed to transmit the frame. Reason? Next two slides…

No backoff → collision is certain

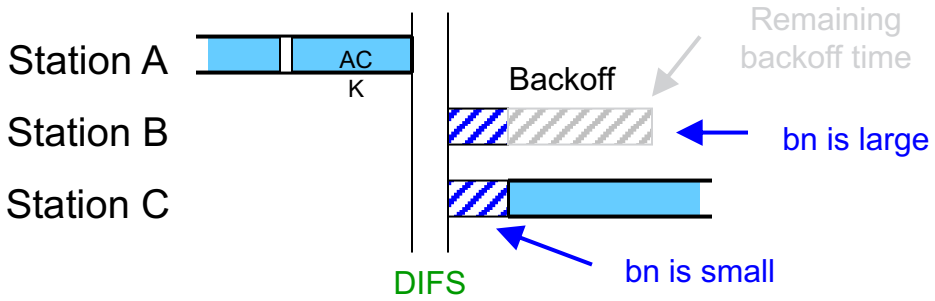
Suppose that several stations (B and C in the figure) are waiting to access the wireless medium.

When the channel becomes idle, these stations start sending their packets at the same time → collision!



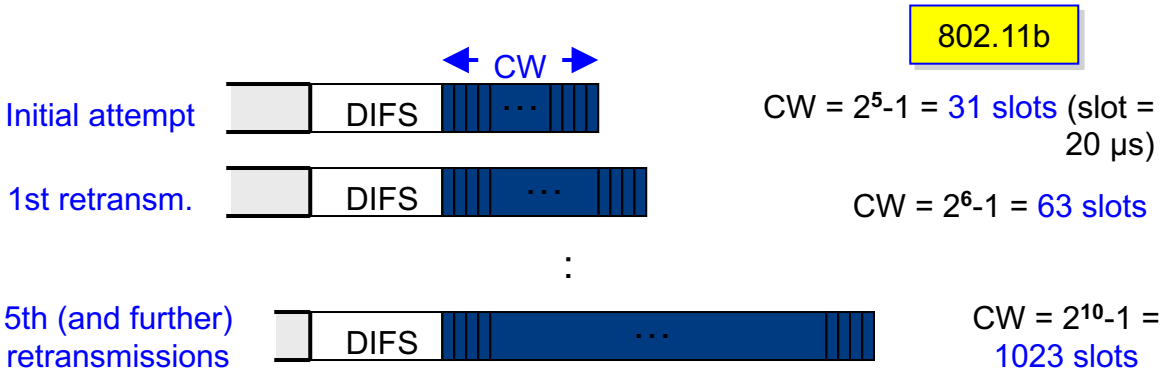
Backoff → collision probability is reduced

Contending stations generate random backoff values bn. Backoff counters count downwards, starting from bn. When a counter reaches zero, the station is allowed to send its frame. All other counters stop counting until the channel becomes idle again.



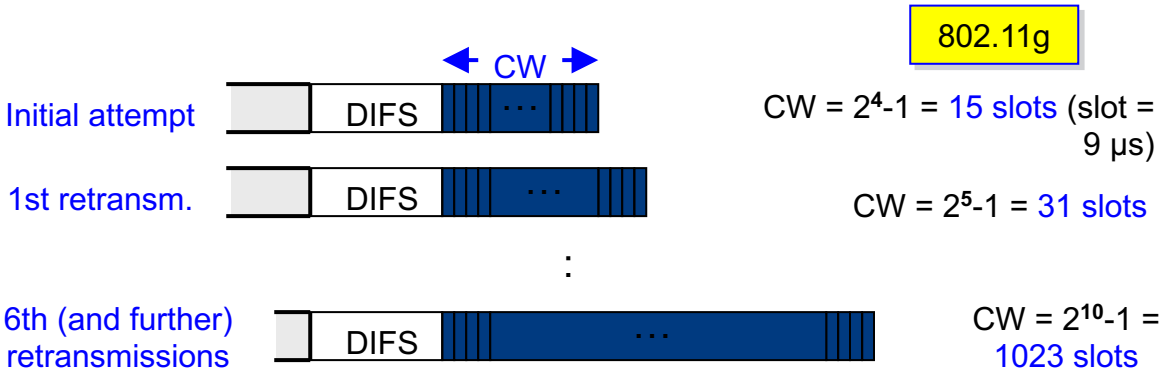
Contention window (CW) for 802.11b

If transmission of a frame was unsuccessful and the frame is allowed to be retransmitted, before each retransmission the Contention Window (CW) from which bn is chosen is increased.



Contention window (CW) for 802.11g

In the case of 802.11g operation, the initial CW length is 15 slots. The slot duration is 9 ms. The backoff operation of 802.11g is substantially faster than that of 802.11b.



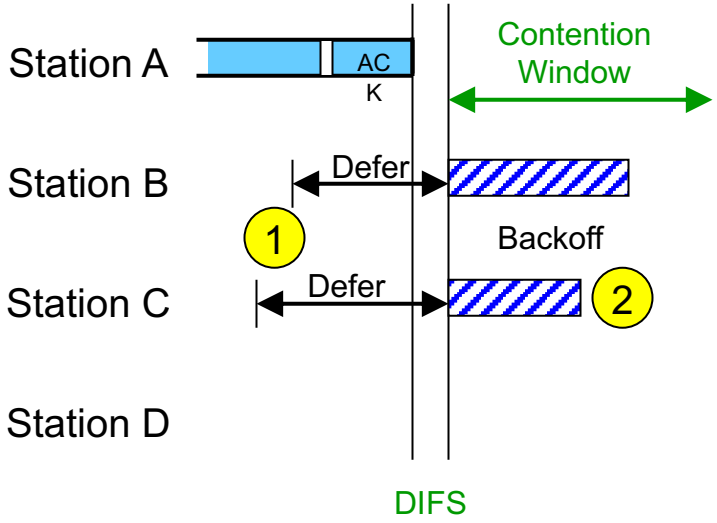
Selection of random backoff

From the number CW (= 15 / 31 … 1023 slots) the random backoff bn (in terms of slots) is chosen in such a way that bn is uniformly distributed between 0 … CW.

Since it is unlikely that several stations will choose the same value of bn, collisions are rare.

The next slides show wireless medium access in action. The example involves four stations: A, B, C and D. ”Sending a packet” means ”Data+SIFS+ACK” sequence. Note how the backoff time may be split into several parts.

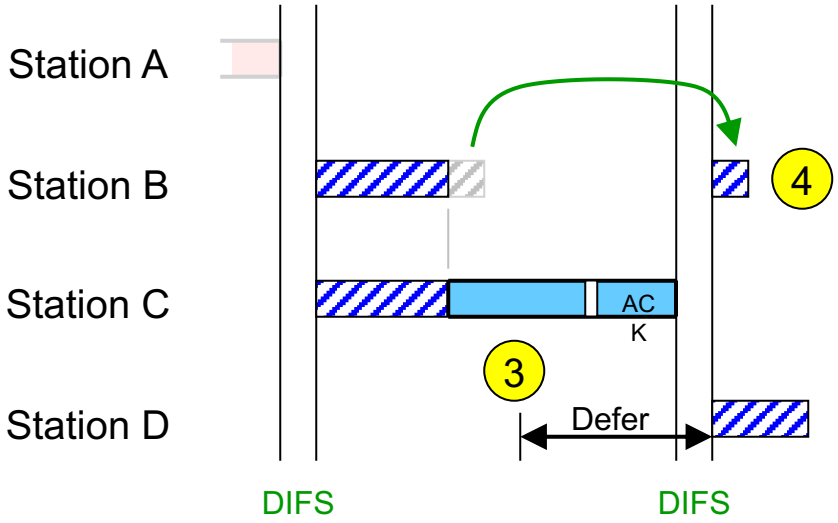
Wireless medium access



1) While station A is sending a packet, stations B and C also wish to send packets, but have to wait (defer + backoff)

2) Station C is ”winner” (backoff time expires first) and starts sending packet

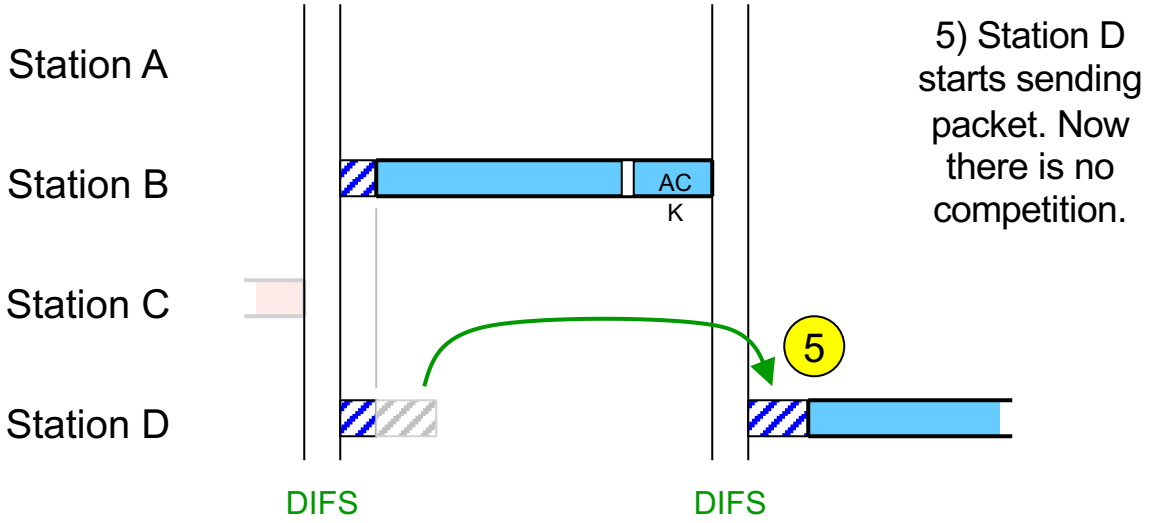
Wireless medium access (2)



3) Station D also wishes to send a packet

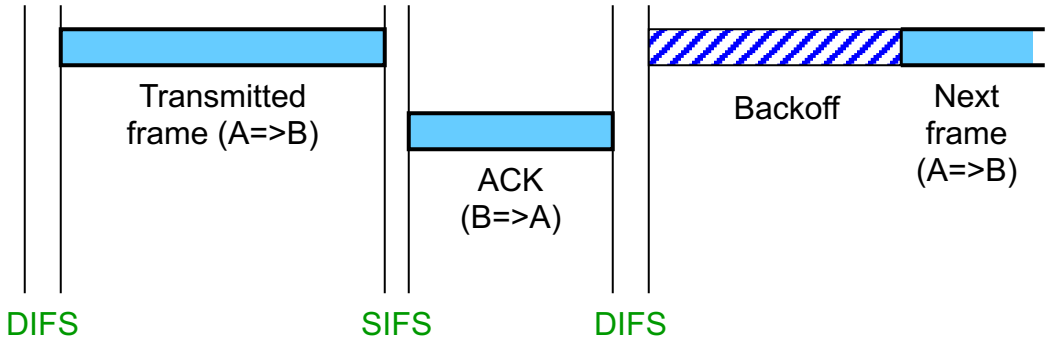
4) However, station B is ”winner” and starts sending packet

Wireless medium access (3)



5) Station D starts sending packet. Now there is no competition.

No shortcuts for any station…



When a station wants to send more than one frame, it has to use the backoff mechanism like any other station (of course it can ”capture” the channel by sending a long frame, for instance using fragmentation).

Hidden Node Problem

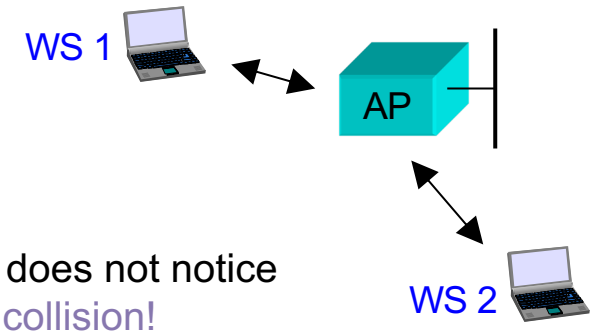
The RTS/CTS (Request/Clear To Send) scheme is used as a countermeasure against the "hidden node" problem:

Hidden node problem:

WS 1 and WS 2 can "hear" the AP but not each other

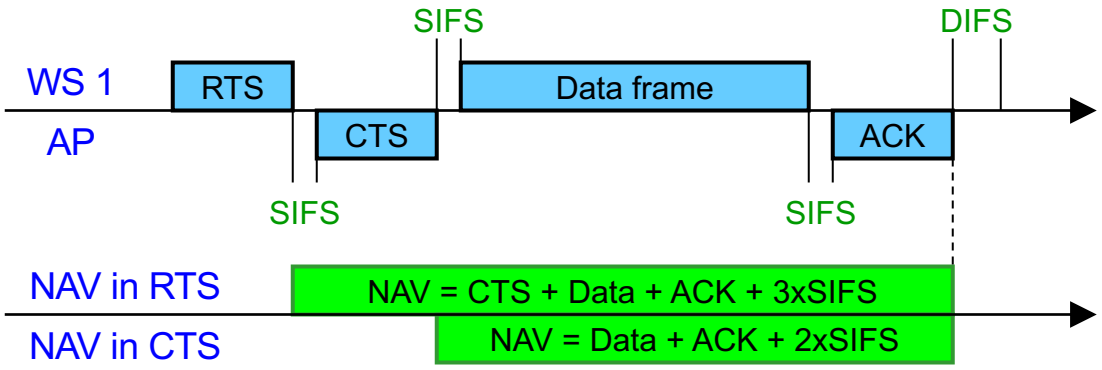
→

If WS 1 sends a packet, WS 2 does not notice this (and vice versa) → collision!



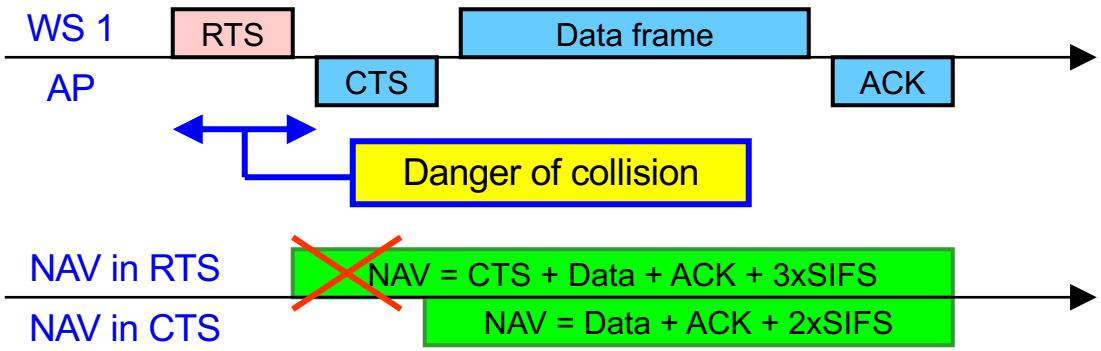
Reservation of medium using NAV

The RTS/CTS scheme makes use of “SIFS-only” and the NAV (Network Allocation Vector) to reserve the medium:



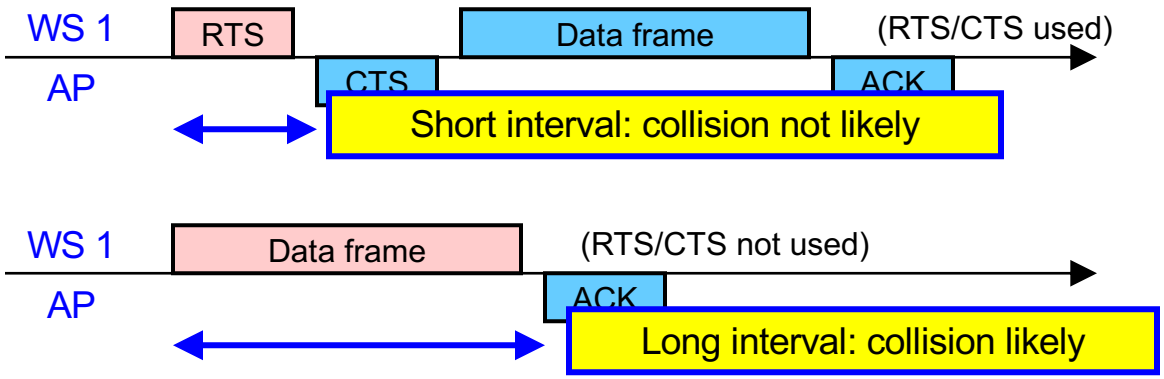
Danger of collision only during RTS

WS 2 does not hear the RTS frame (and associated NAV), but can hear the CTS frame (and associated NAV).



Discussion RTS & CTS

Usage of RTS/CTS offers an advantage if the data frame is very long compared to the RTS frame:



Discussion RTS & CTS (2)

- A long “collision danger” interval (previous slide) should be avoided for the following reasons:
  - **Larger probability of collision**
  - **Greater waste of capacity** if a collision occurs and the frame has to be retransmitted.
  - A threshold parameter (dot11RTSThreshold) can be set in the wireless station. Frames shorter than this value will be transmitted without using RTS/CTS.
- In modern 802.11 standards (802.11n and above), the time for RTS/CTS is comparably long
  - RTS/CTS are exchanged at min data rate
  - Frames are exchanges at max possible data rate
  - → mismatch and RTS/CTS is becoming obsolete