Fachhochschule
Dortmund
University of Applied Sciences and Arts

Communications and Computer Networks

Summer Term 2023

Prof. Dr. Daniel Spiekermann
Faculty of Computer Science

Recap of (a prior) lecture (1/1)

- What are the tasks of the physical layer?
- Which transmission media are there on this layer?
- What are TP cables? What categories are there?
- How do fiber optics work?
- What types of fiber optics are there? What is the difference between them?
- What are your advantages and disadvantages of these cables?
- What is the bandwidth of a transmission channel?
- What connection does Nyquist's sampling theorem describe?
- How to calculate the channel capacity of a channel (Shannon)?
- What types of encoding are there?
- What are typical properties of signal codes?
- How does the 4B5B code and pulse amplitude modulation (PAM-5) work?

Fachhochschule
Dortmund
University of Applied Sciences and Arts

Wireless Communication - Basics

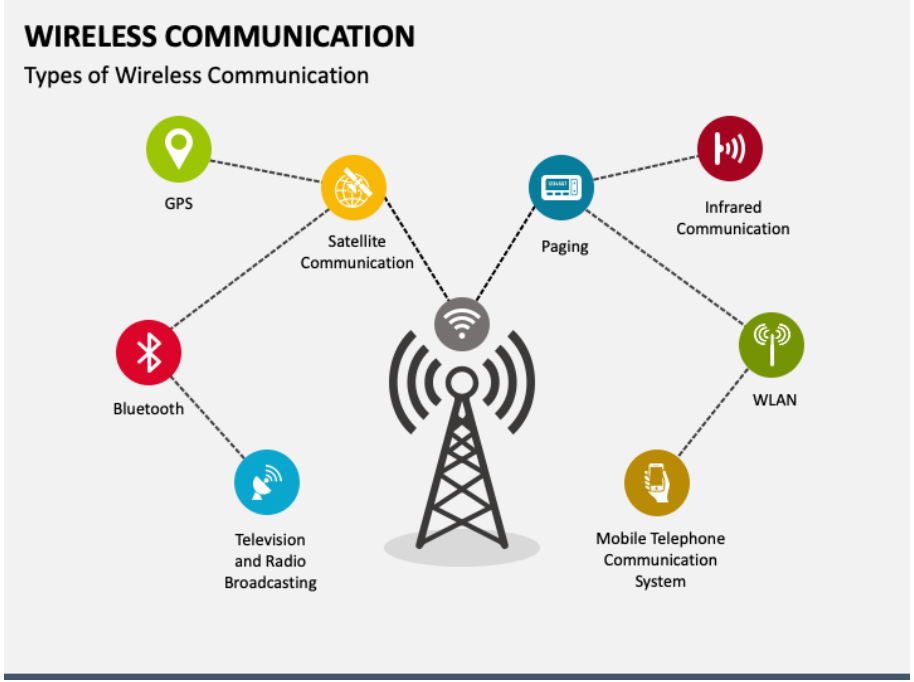
Prof. Dr. Daniel Spiekermann
Faculty of Computer Science

Learning Objectives

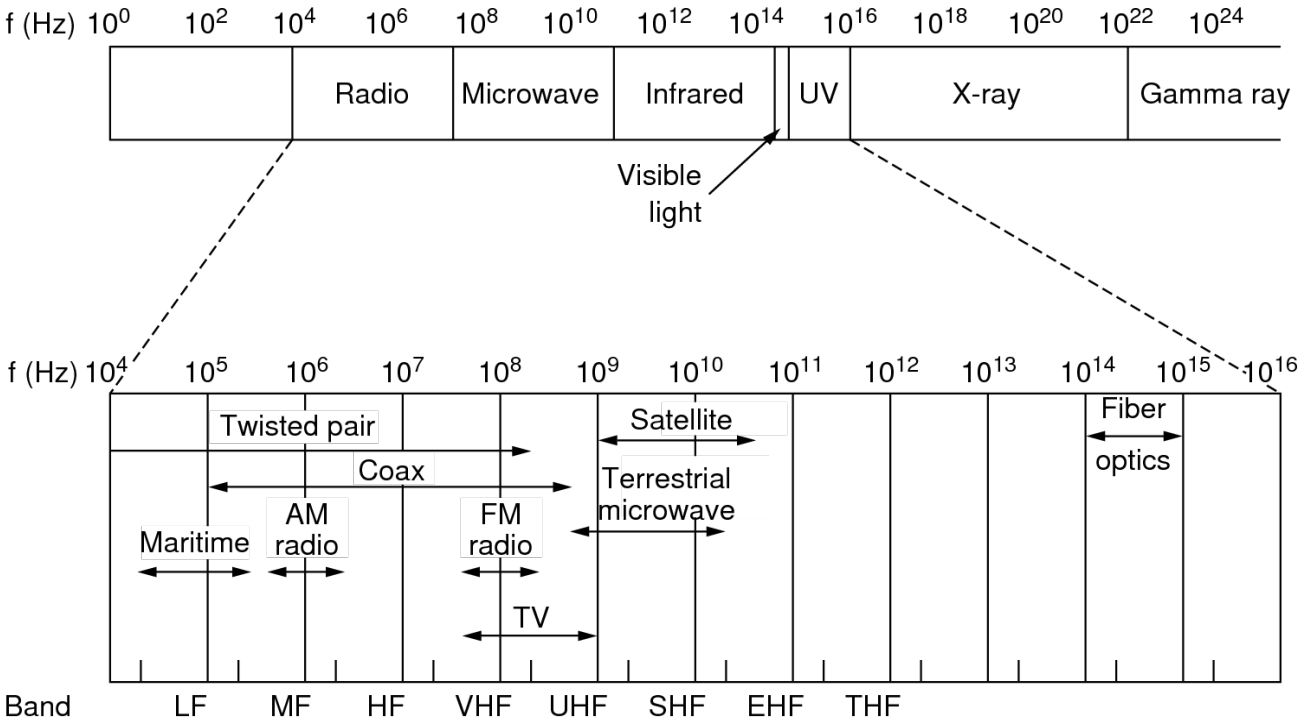
- You know the basic principle of wireless communication
- You are familiar with the different standards according to IEEE 802.11.
- You can explain the difference between ad hoc mode and infrastructure mode.
- You can explain the hidden station problem and the exposed station issue.
- You can explain CSMA/CA
- You know the basic structure of a framework for WLAN.
- You can explain the addressing of IEEE 802.11 with the 4 addresses

Basic principle of wireless transmission

- Various implementations exists, but have a similar basic principle
- Data exchange is based on the transmission of electromagnetic waves.
- A wave type converter (**antenna**) converts the conducted wave into a **free space** wave (transmit side) and back again (receive side).
- For transmission, the user information is modulated to a carrier frequency.
- Different carrier frequencies have different propagation characteristics.



The electromagnetic spectrum



Spectral ranges and communication systems (selection)

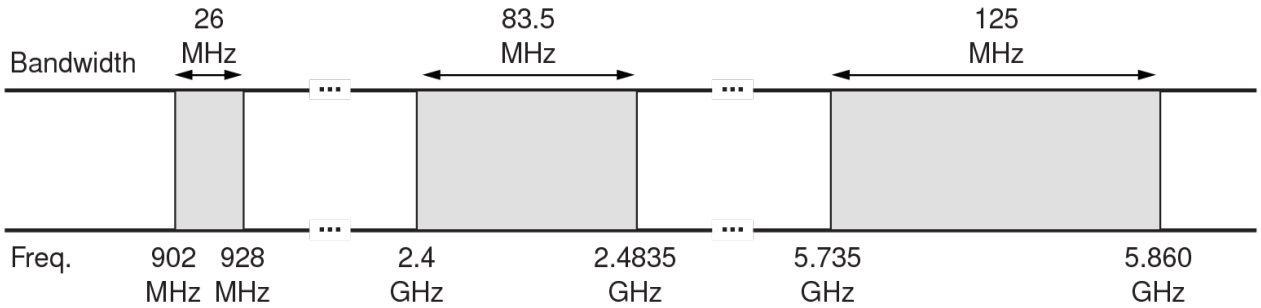
MHz frequency band	System	Category
703-733	LTE/5G (E-UTRA Band 28 Uplink)	Mobile
758-788	LTE/5G (E-UTRA Band 28 Downlink)	
791-821	LTE (E-UTRA Band 20 Downlink)	
832-862	LTE (E-UTRA Band 20 Uplink)	
890-915	GSM (GSM 900)	
935-960	GSM (GSM 900)	
1227,6	GPS	Position
1575,42	GPS	
1710-1785	GSM (DCS 1800)	Mobile
1805-1880	GSM (DCS 1800)	
1880-1900	DECT	Cordless telephony
1920-1980	UMTS (UTRA-FDD), ab ~2021 5G Uplink	Mobile
2110-2170	UMTS (UTRA-FDD), ab ~2021 5G Downlink	
2400-2483,5	WLAN 802.11b,g,n Bluetooth, 802.15.4	wireless local networks
5150-5725	WLAN 802.11a,n,ac	
5725-5875	WLAN 802.11a,n	

Frequency allocation

- Garage door openers, alarm systems, etc. – 40MHz
- Baby monitors: 49MHz
- Cell phones: 824-849MHz, 869-894MHz, 1850-1990MHz
- Global Positioning System: 1.227-1.575MHz
- WiFi/802.11b/g and Bluetooth: 2.4GHz
- Zigbee/802.15.4: 868MHz, 915MHz, 2.4GHz
- Microwave ovens: 2.4Ghz
- TV: 54-216 (VHF 2-13), 470-806MHz (UHF 14-69)
- ISM (industrial, scientific, medical): 900MHz, 1.8GHz, 2.4GHz, 5.8GHz

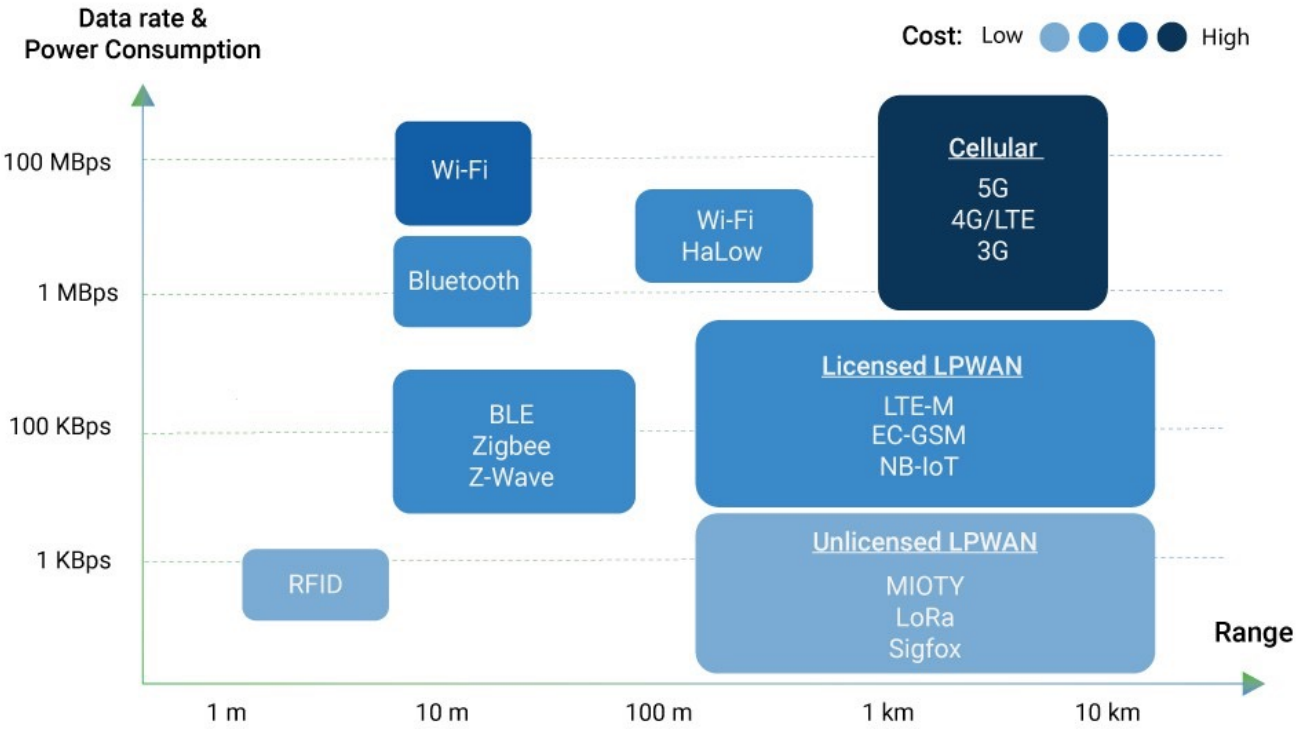
The ISM Band

ISM: Industrial, Scientific, Medical; reserved for unlicensed use

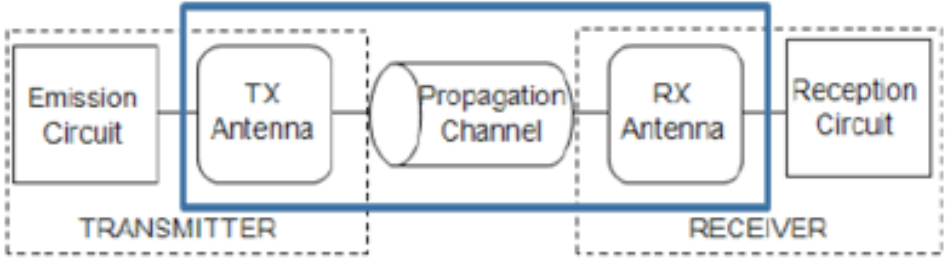


ISM bands in the USA (up to 1 watt transmission power free)

Wireless Networks Overview – Distance, Bandwidth and Cost



Components



- Transmitter
  - Initial component in the creation of wireless communication
  - Transmitter starts generating an AC signal (e.g. 2,4 GH = oscillating 2.4billion times per sec)
  - Data is send over the channel with the transmission method (DSSS, OFDM)
- Antenna
  - Collects RF signal (on receiver side)
  - Transmits data like an isotropic radiator
  - Structure depends on the used communication technique (depends on wavelength)
- Receiver
  - Takes the signal received by the antenna and translates this signal into 1 and 0

Fachhochschule
Dortmund
University of Applied Sciences and Arts

Wireless Communication - Wi-Fi

Prof. Dr. Daniel Spiekermann
Faculty of Computer Science

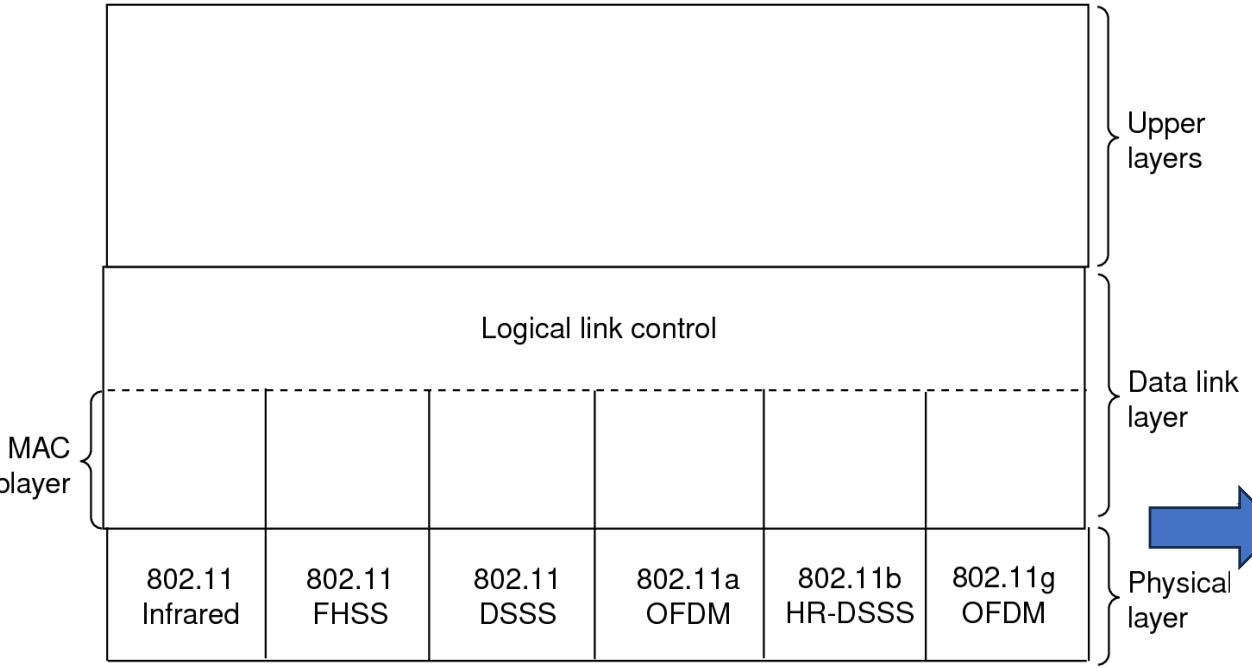
Overview of IEEE 802 standards with a focus on wireless

Name	Description
802.1	Overview, Architecture, Management, MAC Bridging
802.2	Logical Connection Control (LLC)
802.3	Ethernet and CSMA/CD access methods
802.11	Wireless LAN (WLAN) / Wireless networks
802.15	Wireless Personal Area Networks (WPAN)
802.15.1	Bluetooth
802.15.3a	High Rate WPAN, Ultra Wideband (UWB)
802.15.4	Low Rate WPAN, Wireless Sensor Networks
802.15.4a	Wireless Sensor Networks with Ranging
802.15.6	Wireless Body Area Network (WBAN)
802.16	Worldwide Interoperability for Microwave Access, WiMAX
802.20	Mobile Broadband Wireless Access
802.22	Wireless Regional Area Network (WRAN)

IEEE 802.11

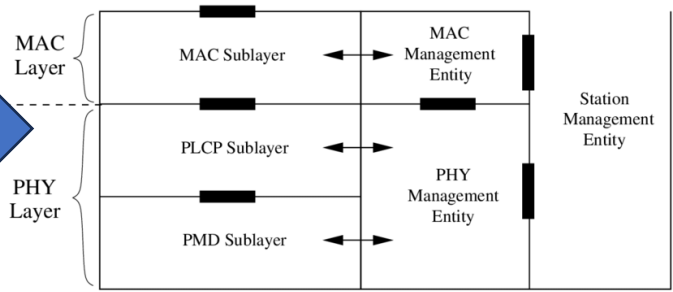
- IEEE 802.11, data rate: 1 or 2 Mbps in the 2.4 GHz band (FHSS, DSSS)
- IEEE 802.11b, data rate: 11 Mbps in the 2.4 GHz band (HR-DSSS)
- IEEE 802.11a, data rate: 54 Mbps in the 5 GHz band (OFDM, 64-QAM)
- IEEE 802.11g, data rate: 54 Mbps in the 2.4 GHz band (OFDM, 64-QAM)
- IEEE 802.11n, data rate: 600 Mbps, 40 MHz channel bandwidth, (OFDM, 64-QAM), 2.4 GHz and 5 GHz bands, Multiple Input Multiple Output (MIMO)
- IEEE 802.11p, Wireless Access in vehicular environments, 5.85 - 5.925 GHz
- IEEE 802.11ac, data rate: 1 Gbps, 80 MHz and 160 MHz channel bandwidth
- IEEE 802.11ad, data rate: 7 Gbps, 2.4, 5, 6 GHz band
- IEEE 802.11ah, WiFi HaLow, used for IoT
- IEEE 802.11ax, WiFi 6, data rate up to 9Gbps, 2.4, 5, 6 GHz
- IEEE 802.11be, WiFi 7, 2.4, 5, 6 GHz data rate up to (theoretical max.) 46Gbps

Layers of IEEE 802.11



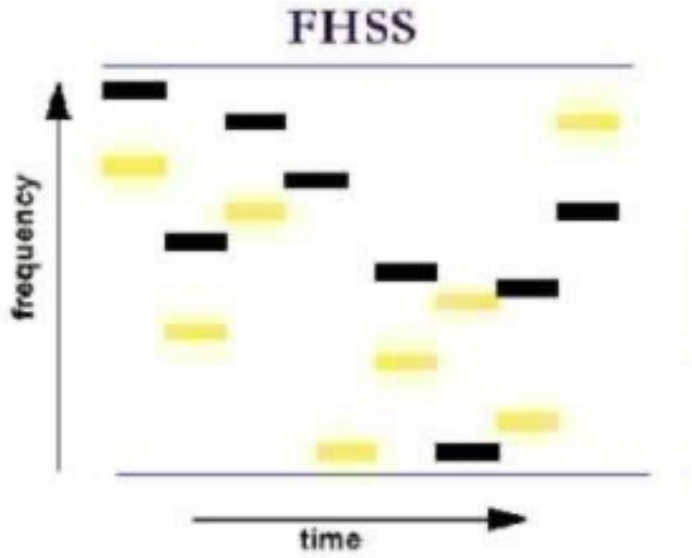
PLCP (Physical Layer Convergence Protocol): Translates between MAC and PMD

PMD (Physical Medium Dependent): Modulation / Demodulation, is interfaced with medium



FHSS - Frequency Hopping Spread Spectrum

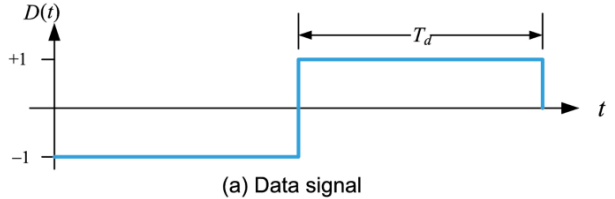
- Available frequency band is divided into smaller sub-bands
- Signals change (hop) their frequencies
- High resistance to interferences on specific frequencies
- Use in 802.11:
  - Frequency change at least 2.5 times per second
  - 1 or 2 Mbps in the 2.4 GHz band



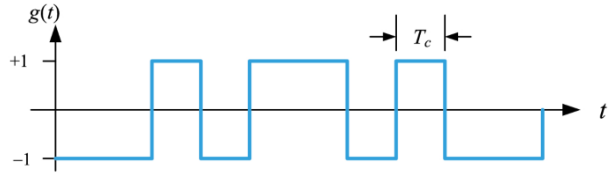
DSSS - Direct Sequence Spread Spectrum

- Signal is multiplexed with spread spectrum signal
- CDMA:
  several transmitters can send information simultaneously over a single communication channel.

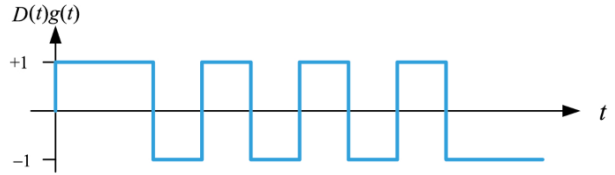
- Use in 802.11
  - DSSS, 802.11: 1 or 2 Mbps in the 2.4 GHz band
  - HR-DSSS, 802.11b: 11 Mbps in the 2.4 GHz band



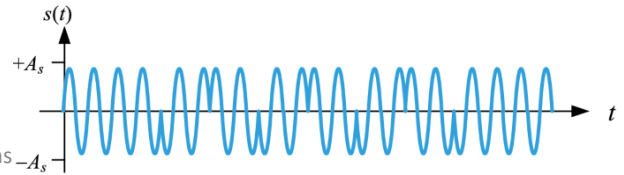
(a) Data signal



(b) Baseband spread-spectrum signal



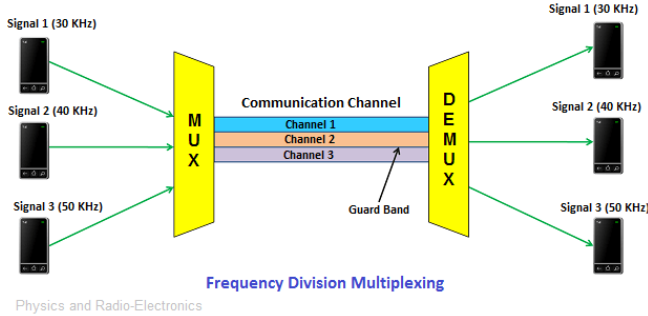
(c) Product signal

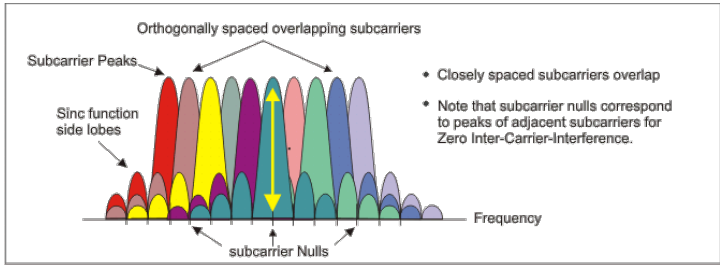


(d) Transmitted signal

OFDM - Orthogonal Frequency Division Multiplexing

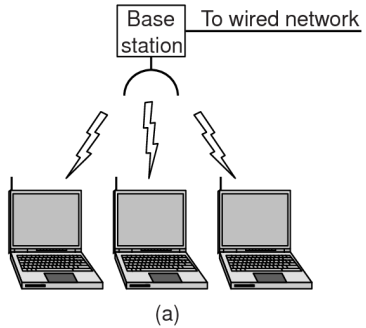
- Transfer of data on multiple carrier frequencies
  - Symbols are transmitted in parallel on 52 frequencies
- Based on FDM (Lecture PhysicalLayer)
- Bitstream is divided in multiple streams
- Each stream is transmitted in closely spaced orthogonal subcarrier signals
- Carriers have overlapping spectra
- Signal with peak has adjacent signals transferring 0
- Use in 802.11
  - 802.11a, 802.11g, 802.11n in the 2.4 GHz and 5 GHz bands



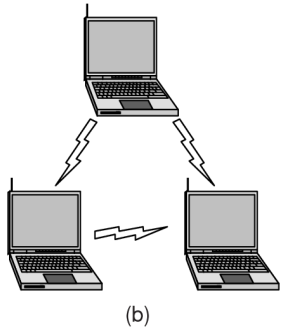


OFDM Signal Frequency Spectra

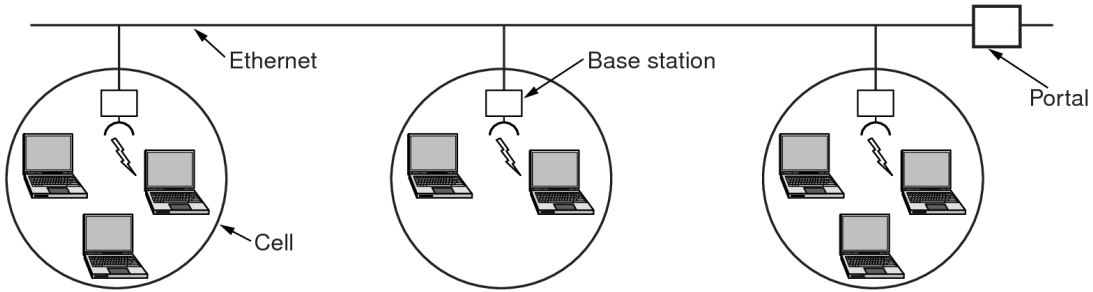
Ad hoc mode and infrastructure mode



(a) Infrastructure mode



(b) Ad hoc mode



Infrastructure mode

Ad hoc mode and infrastructure mode

- **Infrastructure mode**

Even when sitting right next to each other, the stations are not communicating directly. Instead, the stations are communicating indirectly through the **wireless access point**. Any station send packets to the access point — probably a wireless router — and the AP sends the packets back to the other station(s). Infrastructure mode requires a central access point that all devices connect to. Infrastructure mode is ideal if you're setting up a more permanent network. Wireless routers that function as access points generally have higher-power wireless radios and antennas so they can cover a wider area.

Most Wi-Fi networks function in infrastructure mode.

- **Ad hoc mode**

Ad-hoc mode is also known as "peer-to-peer" mode. Ad-hoc networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other. If you set up the two stations in ad-hoc wireless mode, they could connect directly to each other without the need for a centralized access point. If you're setting up a temporary wireless network between a handful of devices, ad-hoc mode is probably fine.

Ad-hoc mode can be easier to set up if you just want to connect two devices to each other without requiring a centralized access point.

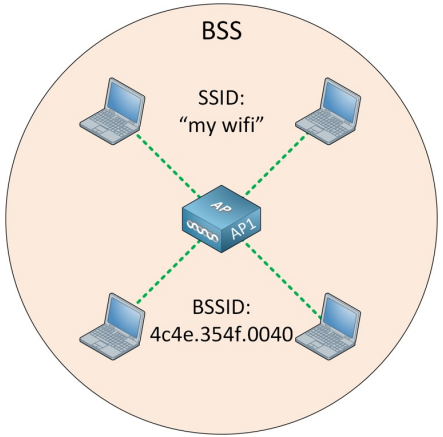
Many devices (like wireless printers, Google's Chromecast) don't support ad-hoc mode.

Service Set

- A service set is a group a wifi devices the same logical network
- Either basic service set (BSS) or an extended service set (ESS)
- The **service set identifier** (**SSID**) defines a service set
  - SSIDs can be **zero to 32 octets** long
  - A **null SSID** (the SSID element's 'length' field is set to zero) prompts an associated access point to send the station a list of supported SSIDs.
- Once a device has associated with a basic service set, for efficiency, the SSID is not sent within packet headers; only **BSSIDs** are used for addressing.

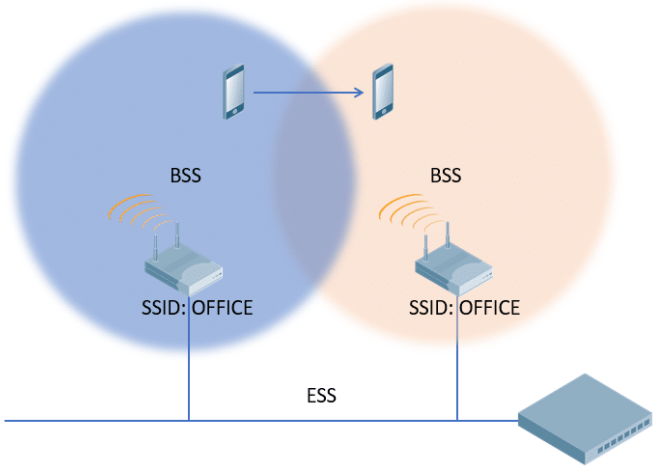
Service Set – Basic Service Set

- An infrastructure BSS is created by an **access point** (**AP**) for other devices to join.
- The **operating parameters** of the infrastructure BSS are **defined by the AP**.
- Each basic service set has a unique identifier, a **BSSID**, which is a 48-bit number that follows MAC address conventions. Is usually non-configurable.
- Basic service set types
  - **BSS**: infrastructure BSS (infrastructure)
  - **IBSS**: Independent BSS (ad hoc)
  - **MESH**: Mesh BSS



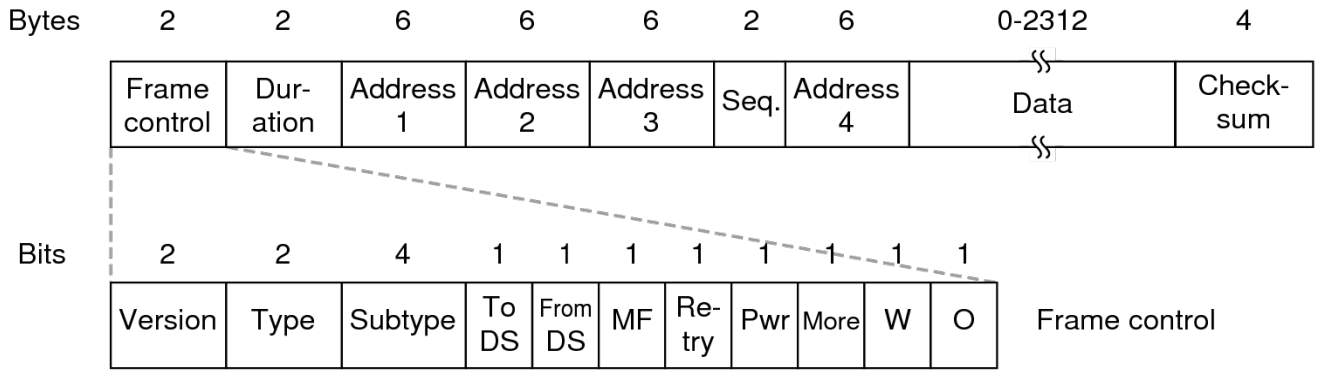
Service Set - Extended service set

- An ESS is a wireless network, created by **multiple APs**, which appears to users as a single, seamless network, such as a network covering a home or office that is too large for reliable coverage by a single AP.
- **One or more** infrastructure **BSS** on a common logical network segment (i.e. same IP subnet and VLAN).
- Easier centralization of services like authentication.
- An IBSS (ad hoc mode) cannot be part of an ESS.



Frame structure

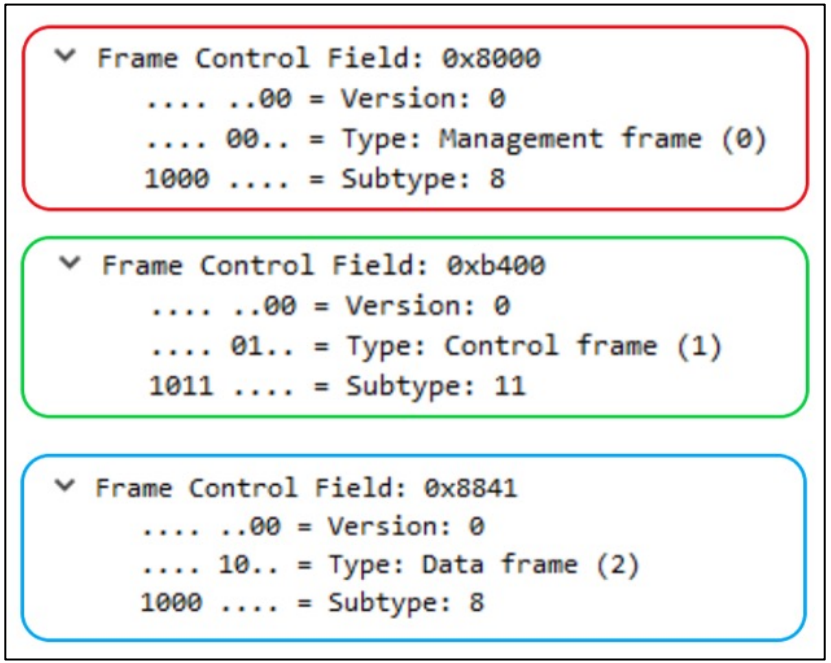
- A frame is constructed of common fields (present in all types of frames) and specific fields (present in certain cases)
- The specific fields depends on the type and subtype specified in the first octet of the frame



Fachhochschule Dortmund
University of Applied Sciences and Arts

Common fields

- Version: 00 (currently)
- Type: Management, Data, Contol
- 4 Addresses:
  - Various combination
  - Possible values:
    - BSSID of dest AP
    - BSSID of src AP
    - Source address
    - Destination address
- Sequence: fragment number and sequence number
- Data: Data
- Checksum: Checksum of Header and data



Management Frame

- Used to manage the BSS. This includes probing, associating, roaming, and disconnecting clients from the BSS.

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM (Announcement Traffic Indication Message)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved

Management Frames

- **Beacon**: Sent periodically from an **access point** to announce its presence and provide the **SSID**, and other parameters for wireless stations within range.
- **Probe request:** Requesting information of available AP
- **Probe response:** Reponse to the requests, contains BSSID and encryption parameters
- **Association request**: Sent from a station after authentication
- **Association response**: Sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such as an association ID and supported data rates.

Control Frames

- Used to control access to the medium and are used for frame acknowledgement.
- Control frames only contain a header and trailer, no body.

Type Value	Type Description	Subtype Value	Subtype Description
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK

Control Frames

- Acknowledgement (**ACK**) frame: After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.
- Request to Send (**RTS**) frame: The RTS and CTS frames provide an optional collision reduction scheme for access points with hidden stations. A station sends an RTS frame as the first step in a two-way handshake required before sending data frames.
- Clear to Send (**CTS**) frame: A station responds to an RTS frame with a CTS frame. It provides clearance for the requesting station to send a data frame. The CTS provides collision control management by including a time value for which all other stations are to hold off transmission while the requesting station transmits.

Data frame

- Used to transfer information **or** trigger an event.
- Not all data frames contain a payload, some are “null data frames” and only contain a header and trailer

Type Value	Type Description	Subtype Value	Subtype Description
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Fachhochschule Dortmund
University of Applied Sciences and Arts

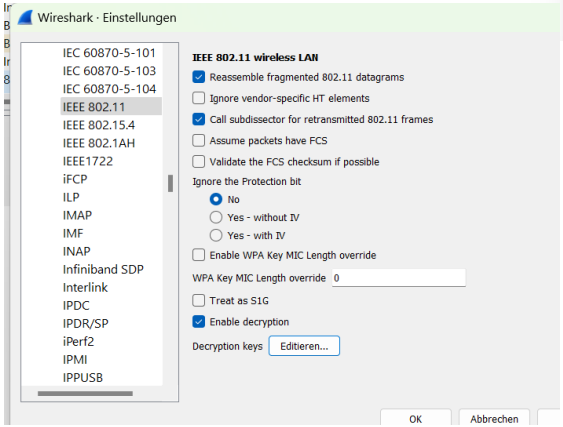
Processing

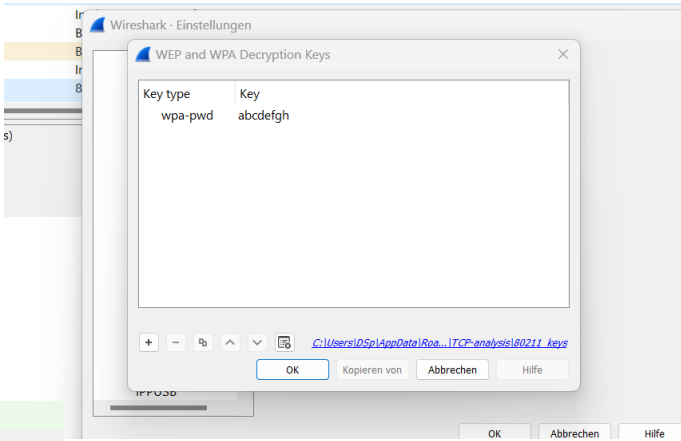
Pac...	Transmitter	Receiver	Flags	Ch...	Data ...	Size	Protocol	Size Bar
241	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	#+	149	24.0	24	802.11 BAR	802.11 BAR
242	84:38:38:5B:63:D5	Ethernet Broadcast	*	149	6.0	122	802.11 Probe Req	802.11 Probe Req
243	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*+	149	24.0	253	802.11 Probe Rsp	802.11 Probe Rsp
244		B8:38:61:99:1A:AF	#	149	24.0	14	802.11 Ack	
245		84:38:38:5B:63:D5	#	149	6.0	14	802.11 CTS	
246	B8:38:61:99:1A:AE	Ethernet Broadcast	*P	149	24.0	294	802.11 Beacon	802.11 Beacon
247	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	*	149	24.0	45	802.11 Auth	802.11 Auth
248		84:38:38:5B:63:D5	#	149	24.0	14	802.11 Ack	
249	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*	149	24.0	34	802.11 Auth	802.11 Auth
250		B8:38:61:99:1A:AF	#	149	24.0	14	802.11 Ack	
251	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	*	149	24.0	176	802.11 Assoc Req	802.11 Assoc Req
252		84:38:38:5B:63:D5	#	149	24.0	14	802.11 Ack	
253	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*	149	24.0	200	802.11 Assoc Rsp	802.11 Assoc Rsp
254		B8:38:61:99:1A:AF	#	149	24.0	14	802.11 Ack	
255	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	C	149	24.0	30	802.11 Null Data	802.11 Data
256		84:38:38:5B:63:D5	#	149	24.0	14	802.11 Ack	
257	B8:38:61:99:1A:AF	Ethernet Broadcast	*	149	24.0	259	802.11 Beacon	802.11 Beacon
258	B8:38:61:99:1A:AE	Ethernet Broadcast	*P	149	24.0	294	802.11 Beacon	802.11 Beacon
259	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	C	149	24.0	30	802.11 Null Data	802.11 Data
260		84:38:38:5B:63:D5	#	149	24.0	14	802.11 Ack	

Wireshark

- Wireshark is able to (capture and) analyze WiFi-traffic
- Interprets packets and types (mgmt, data, ctrl)
- Needs key to decrypt encrypted packets

Preferences – Protocols – IEEE 80.11 Decryption Keys





Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- If two stations check the channel at the same time, both get as a result, that the channel is free and send. A collision occurs.
- Collision detection is not possible during radio transmission because the performance of the received signal is negligible compared to the transmitted signal.
- The CSMA/CA method tries to avoid collisions by not accessing an occupied channel immediately as soon as it becomes free.
- Each station waits for a random time before re-checking, which means that the probability of collisions is reduced.
- The attenuation of the radio signals in the medium causes two other media access problems called the hidden station and exposed station problems.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

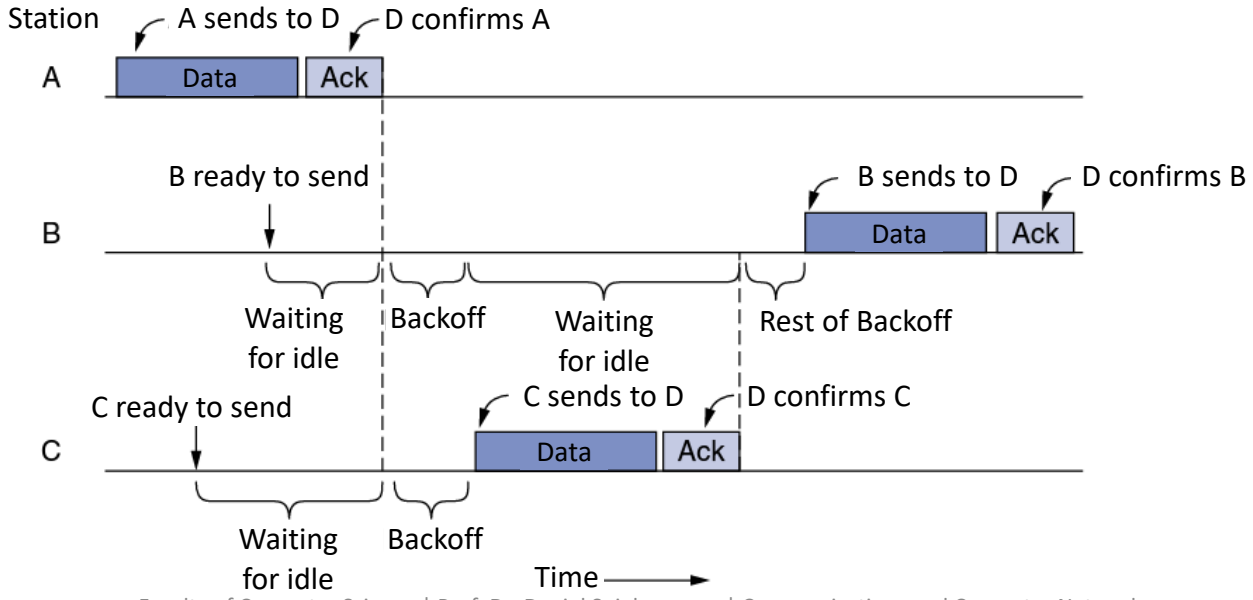
The method of Medium Access Control sublayer called CSMA/CA is:

- When a frame is ready to be transmitted, the transmitting station **checks** whether the **channel** is idle or busy.
- If the channel is **busy**, the station **waits** until the channel becomes idle.
- If the channel is **idle**, the station **waits** for an **Inter-frame spacing** (**IFS**) amount of time and then sends the frame.
- After sending the frame, it sets a timer, then waits for acknowledgement from the receiver.
- If it receives the **acknowledgement** before expiry of timer, it marks a successful transmission.
- Otherwise, it waits for a time period, employing simple exponential **back-off** algorithm to avoid collisions, and restarts the algorithm.

Simple CSMA/CA

Assumption:

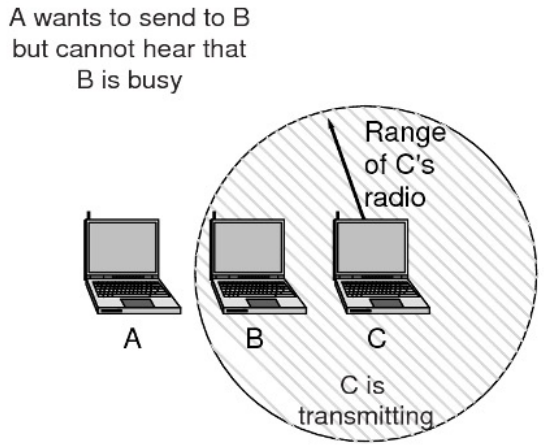
- Stations A, B, C and D can reach each other



Problems accessing the radio channel

Scenario: The two radio subscribers A and C are spatially so far apart that they cannot receive their radio signals from each other. Between them is station B.

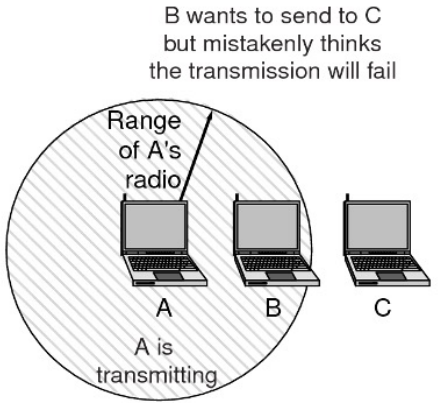
Hidden station problem (hidden end device): Station C sends to B, at the same time A wants to send to B and checks the medium. A cannot see that the medium is occupied at B because A is transmitting out of range.
A sends and there is a collision at B.
C is a hidden terminal for A and vice versa.



Problems accessing the radio channel

Scenario: The two radio subscribers A and C are spatially so far apart that they cannot receive their radio signals from each other. Between them is station B.

Exposed station problem (exposed terminal): Station A sends to any other station that is out of range of B and C. At the same time, B wants to send to C. B detects the signals from A and waits until the transmission of A is finished.
Since the radio waves of A cannot reach C at all,
it would not be necessary to wait at all,
since C would not collide at all. Nevertheless,
station A has an exposed position and
prevents communication between station B and C.



Advanced CSMA/CA with RTS/CTS or PCF

There are advanced coordination functions to further reduce the possibility of collisions, even in the scenarios of hidden and exposed stations.

- Distributed Coordination Function (DCF):
  There is **no central authority** that regulates access (possible in infrastructure and ad hoc mode).
  - Simple CSMA/CA (without RTS/CTS) (exponential backoff time)
  - **CSMA/CA with RTS/CTS** (Sender sends RTS into the network as a BC, all stations receive this, intended receiver sends CTS)
- Point Coordination Function (PCF):
  The **access point** regulates access to the medium (only possible in infrastructure mode).

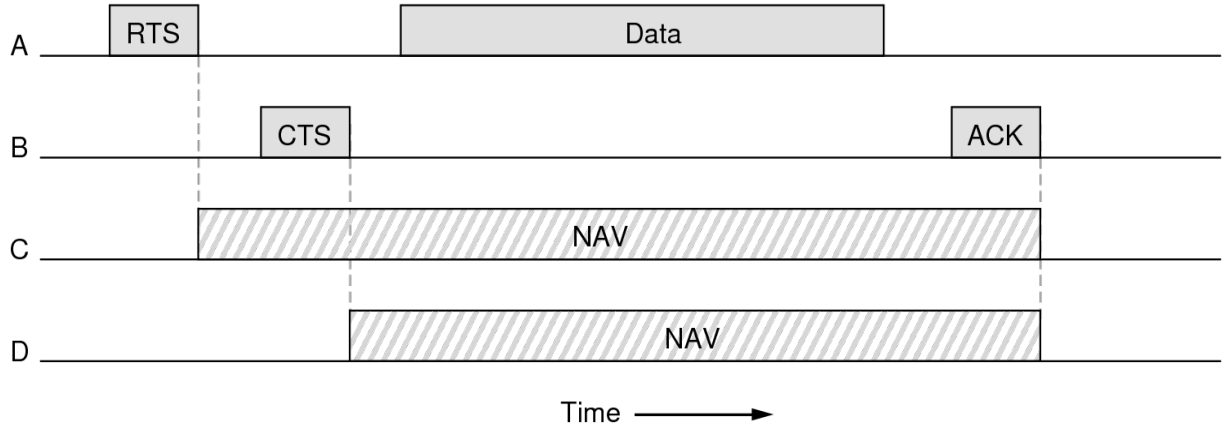
RTS – request to send
CTS – clear to send

CSMA/CA with DCF and RTS/CTS

Assumptions:

- Station A can reach Stations B and C
- Station D can reach Station B, but is out of range of Station A

→ Destination: Station A wants to send data to Station B



NAV - Network Allocation Vector

NAV - Network Allocation Vector

- The **NAV** is a virtual carrier-sensing mechanism
- The virtual carrier-sensing is a logical abstraction which limits the need for physical carrier-sensing at the air interface **in order to save power**.
- **Duration field** in MAC Layer specifies a time required for transmission of a frame
- In this time, the medium will be busy.
- Stations listening on the wireless medium read the duration field and set their NAV
- Wireless stations are often battery-powered, so to conserve power the stations may enter a **power-saving mode**. A station decrements its NAV counter until it becomes zero, at which time it is awakened to sense the medium again.

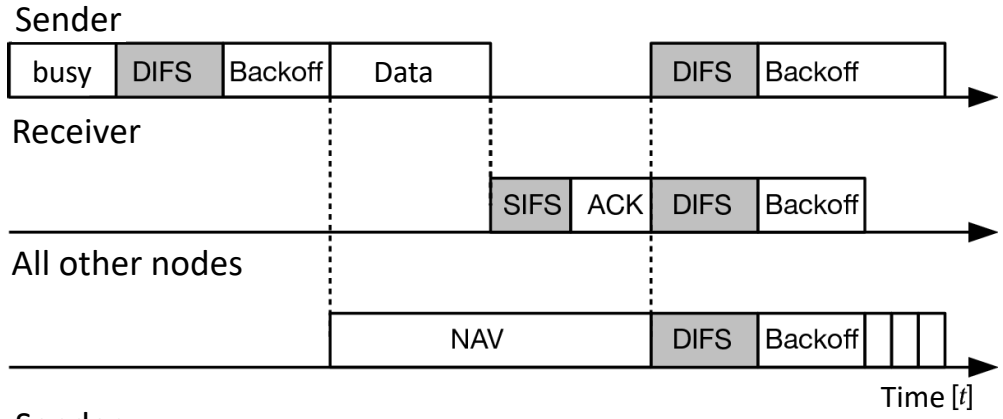
Fachhochschule Dortmund
University of Applied Sciences and Arts

Comparison of simple CSMA/CA with CSMA/CA and RTS/CTS

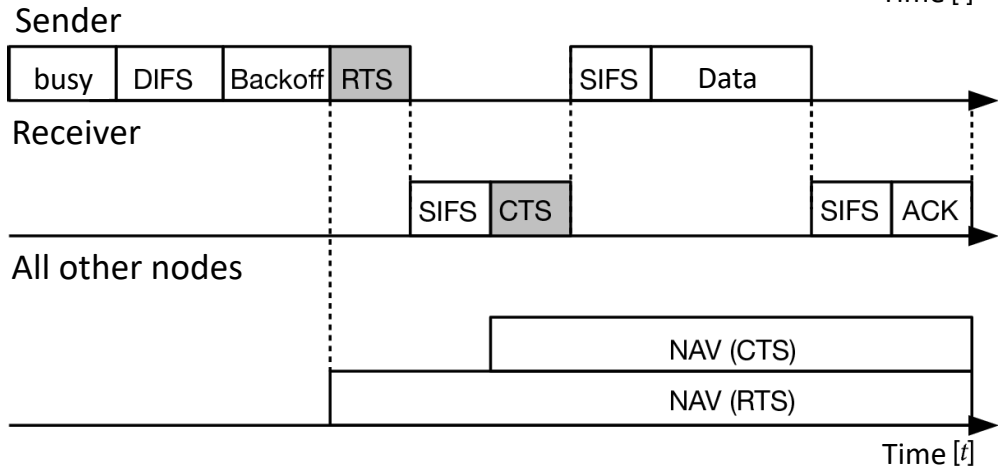
DIFS:
DCF Inter-Frame Spacing
50 μs

SIFS:
Short Inter Frame Spacing
10 μs

Simple CSMA/CA



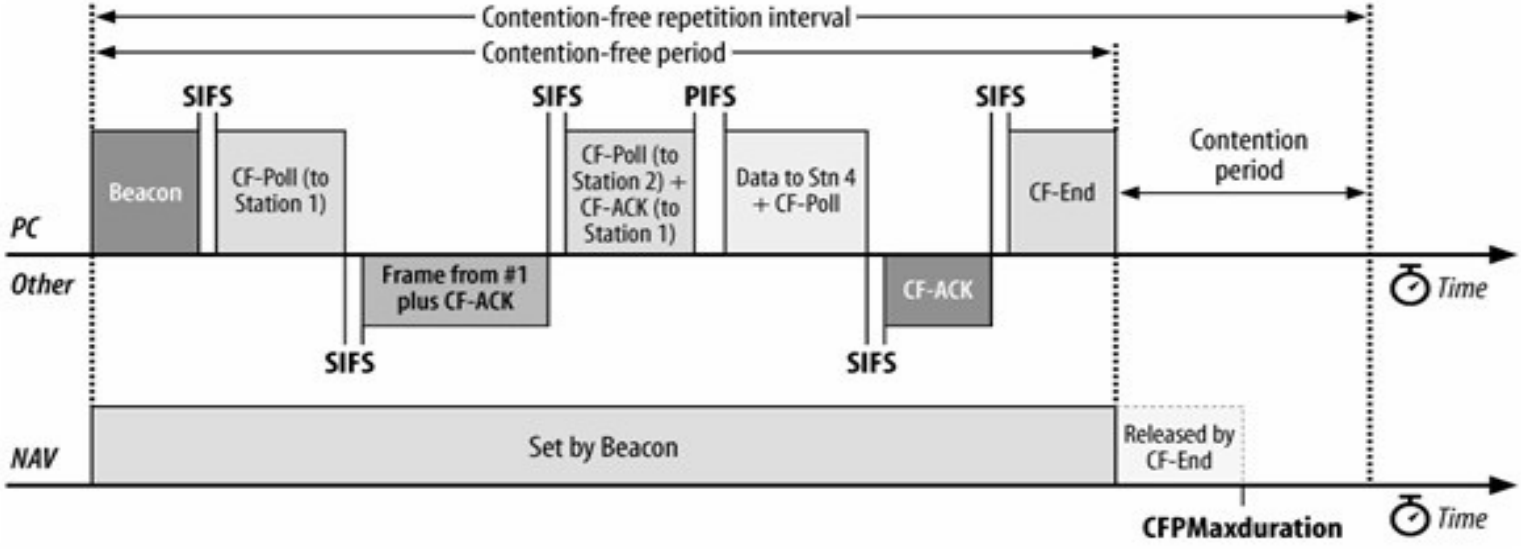
CSMA/CA with RTS/CTS



CSMA/CA with PCF

- Central access control by the Point Coordinator (PC) (usually AccessPoint).
- One after the other, all stations are granted the right to broadcast by the PC with a **CF-poll** frame (CF = **contention-free**).
- **Optimization** of the assignment of the frequency channel:
  - A station can send an ACK together with a data frame.(Data + **CF-Ack** Frame SubType)
  - With a CF poll, a PC can send an ACK to the previous broadcast of a station. (Data + **CF-Ack + CF-Poll** Frame SubType)
  - A PC can also send data to the station with a CF poll frame. (**Data + CF-Poll** Frame SubType)
  - A station does not necessarily have to send a data frame to the PC. However, ACK of the other station may only take place when the received station has the right to send.

PCF: Contention Free Period and Contention Period



Inter-Frame Spacing (IFS), Short IFS (SIFS), Point Coordination IFS (PIFS, 30 μs)

Fachhochschule
Dortmund
University of Applied Sciences and Arts

Additional Slides

Prof. Dr. Daniel Spiekermann
Faculty of Computer Science