Wireless Medium Access Technologies

Wireless LAN

Mobile Communication, WS 2014/2015, Kap.3.1

Prof. Dr. Nils Aschenbruck

Mobile Communication Technology according to IEEE (examples)

JS

WiFi

Local wireless networks
WLAN 802.11

- 802.11a → 802.11h
- 802.11i/e/…/n/…/z/aq
- 802.11b → 802.11g

ZigBee

Personal wireless nw
WPAN 802.15

- 802.15.4 → 802.15.4a/b/c/d/e/f/g
- 802.15.5, .6 (WBAN)
- 802.15.3 → 802.15.3b/c
- 802.15.2
- 802.15.1

Bluetooth

Wireless distribution networks
WMAN 802.16 (Broadband Wireless Access)

WiMAX

+ Mobility

[hist.: 802.20 (Mobile Broadband Wireless Access)]
802.16e (addition to .16 for mobile devices)

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary
- …

This strategy of Ethernet and IEEE 802.3 LANs allows **immediate medium access** if no other station uses the **shared bus**.

Collisions are detected and resolved:

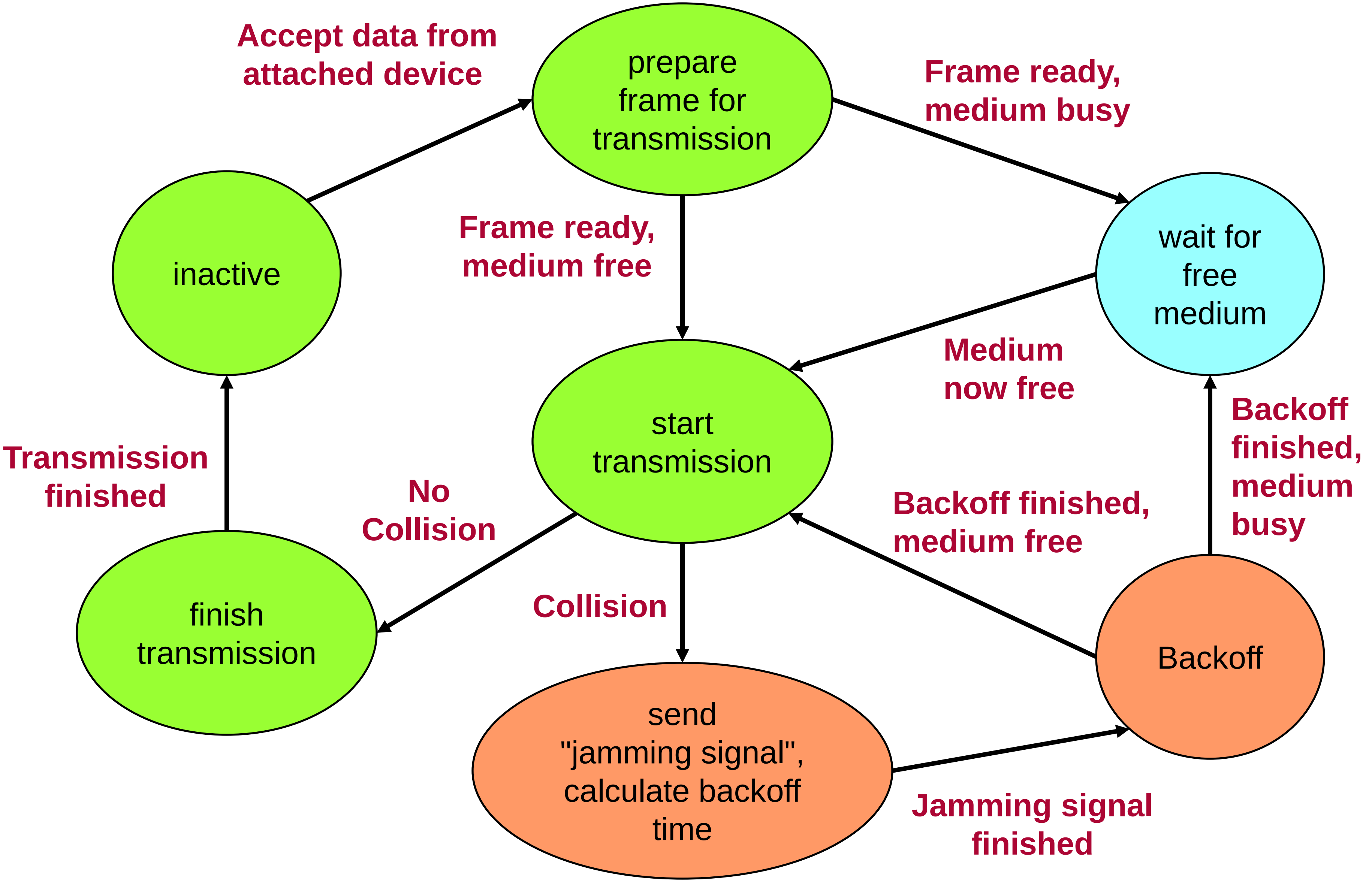
C	**Carrier**
S	**Sense**
M	**Multiple**
A	**Access with**
C	**Collision**
D	**Detection**

Same as:
"Listen-Before-Talk" in conversations.

CSMA/CD is based on a protocol called **"Aloha"** which was developed in Hawaii for satellite communication.

Aloha:
- Send whenever you want
- Collisions are detected by message loss (missing ACK)
- Lost data are re-transmitted

In LANs, the signal propagation time is small. For this reason, **collisions may be detected while transmitting**.


Accept data from attached device
prepare frame for transmission
Frame ready, medium busy
inactive
Frame ready, medium free
wait for free medium
Medium now free
start transmission
Backoff finished, medium busy
Transmission finished
No Collision
Backoff finished, medium free
Collision
finish transmission
Backoff
send "jamming signal", calculate backoff time
Jamming signal finished

In case of light load

stations almost always have **immediate access** to the shared medium.

With higher load

the collision probability increases:
It becomes more and more likely that several stations start a transmission (almost) simultaneously.

Obviously, a **mechanism for load reduction / traffic shaping** is required:

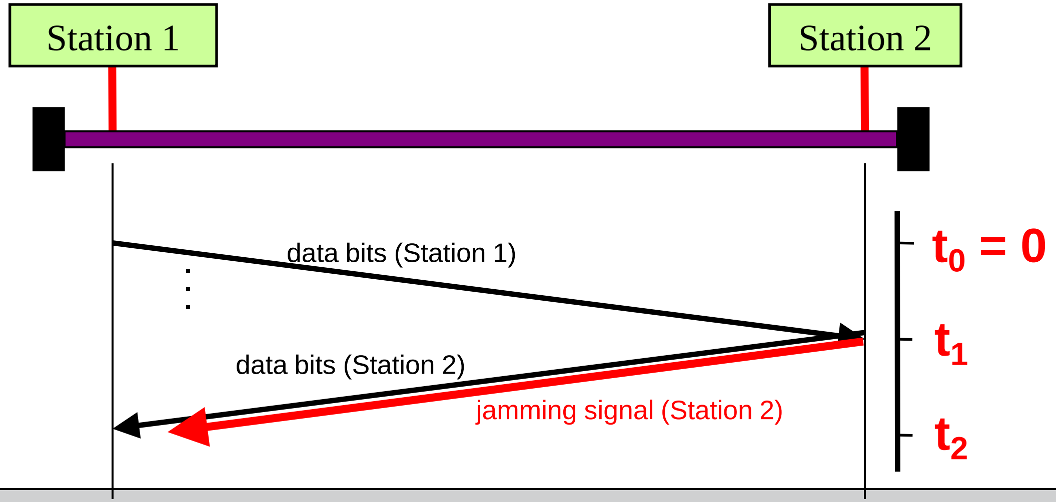
Light load:	choose a **small backoff time**
Heavy load:	choose a **large backoff time**

In real life, the so-called **"Truncated Binary Exponential Backoff"*** is used. With this mechanism, the current load is estimated from the number of collisions the current message was already involved in.

Many collisions already:	**large backoff time**
Small # of collisions so far:	**small backoff time**

***A similar mechanism is used in 802.11 WLAN**

"Truncated Binary Exponential Backoff" (2)



Let t_0 be the time when station 1 starts transmitting

t_1 be the time when station 2 starts transmitting (sensing free medium), shortly after that its transmission collides with the transmission of station 1, station 2 starts to send a jamming signal

t_2 be the time when station 1 detects the collision

Then: $t_1 \leq$ **end-end-delay**; $t_2 \leq \underbrace{2 \bullet \text{end-end-delay}}_{\text{(so-called "Slot Time")}}$

k^{th} re-transmission ($k \leq 10$): Randomly choose a backoff time as r * slot time with $0 \leq r < 2^k$ (r integer, Ethernet slot time: 51.2 µs)

k^{th} re-transmission ($10 < k \leq 16$): same as above, but $0 \leq r < 2^{10}$

If the transmission still fails: no further attempts.

Wireless LAN (WLAN) is also called “Wireless Ethernet”.

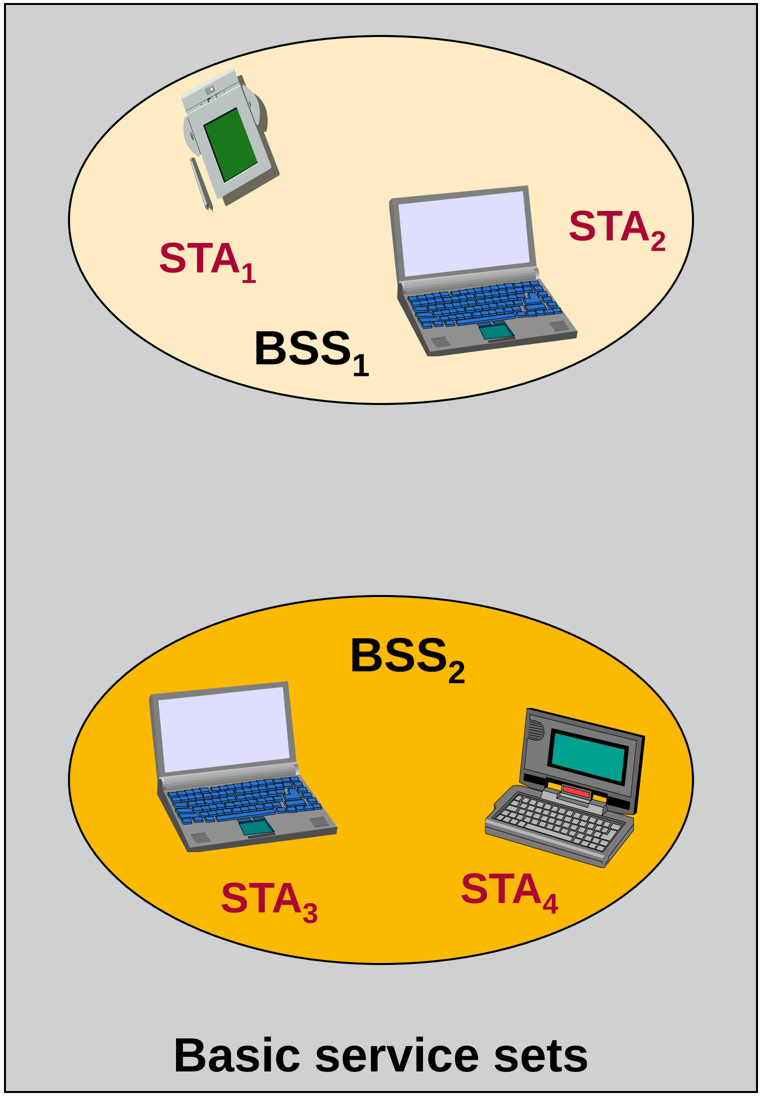
In fact, Ethernet and WLAN have several characteristics in common:

- **Shared medium:** The wireless medium is shared by all stations in the area.
- **Risk of collisions:** Collisions may happen.

However, there are important differences:

- **Collision Detection:** In WLAN, collisions are hard to detect
  (The transmitted signal is much stronger than the received signal)
- **Network Formation:** Who belongs to the network?
  (In Ethernet, you can check the cables. In WLAN, you need identifiers)

The **basic building block** of an IEEE 802.11 LAN is called **basic service set (BSS)**.



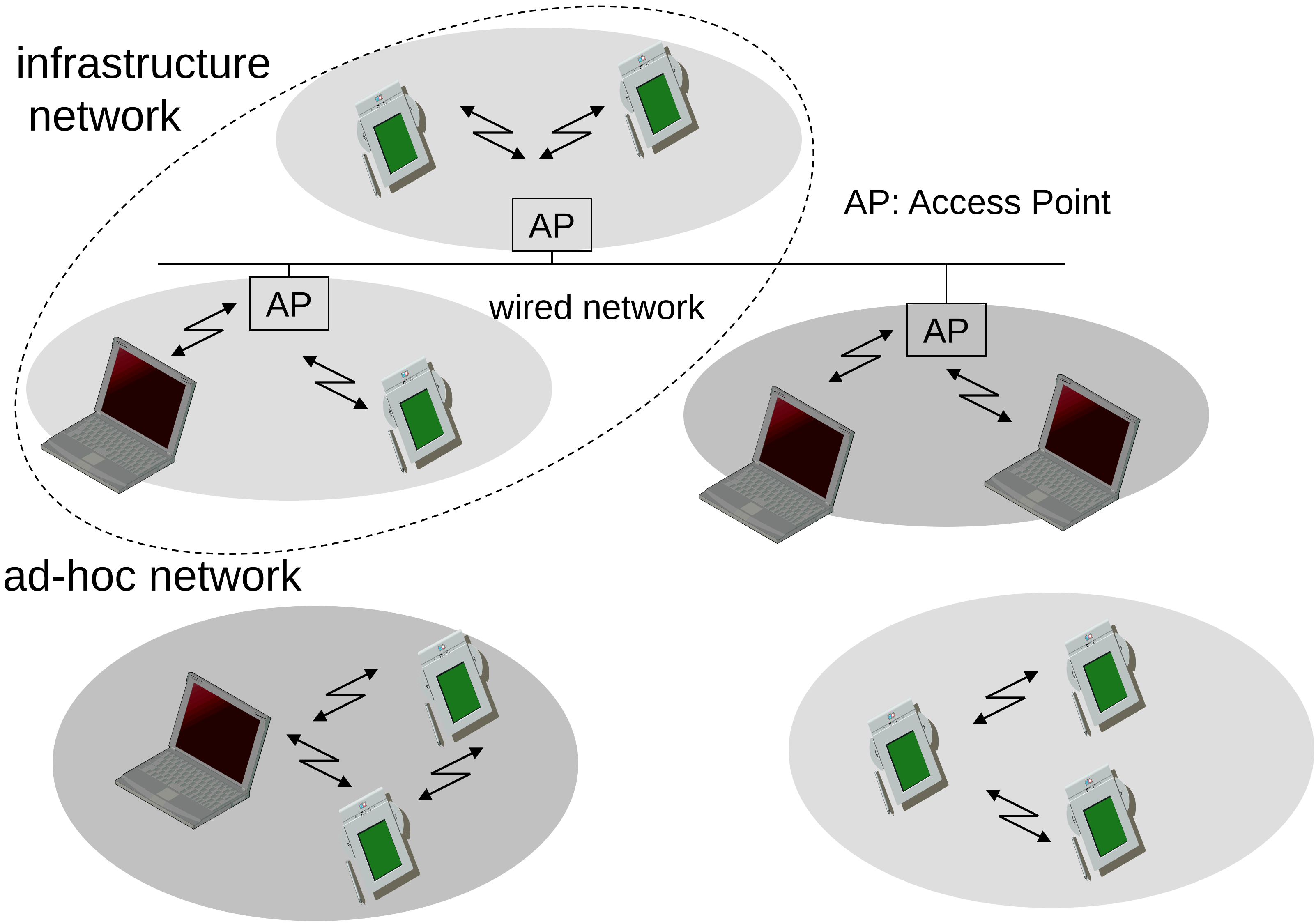
Station (STA):

- **Any device** that contains an **IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY)** interface to the wireless medium (WM).

Basic service set:

- It is useful to think of the ovals used to depict a BSS as the **coverage area within which the member stations of the BSS may remain in communication.**
- The **concept of area**, while not precise, is **often good enough**.
- If a station **moves out** of its BSS, it can **no longer directly communicate with other members of the BSS.**

Comparison: infrastructure vs. ad-hoc networks



Ad-hoc networks in (quite) recent news

http://www.fortschrittskolleg.de/ - rekonq

http://www.fortschrittskolleg.de/

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Censorship-resistant Collaboration with a Hybrid DTN/P2P Network

Masterarbeit

von

Philipp Hagemeister

aus

Braunschweig

vorgelegt am

Lehrstuhl für Rechnernetze und Kommunikationssysteme
Prof. Dr. Martin Mauve
Heinrich-Heine-Universität Düsseldorf

März 2012

MENU

drhein-
n und
ft und
n. Ziel des
ng von
ch genutzt
2014
er
UNI
leitenden Fragestellung arbeiten.
ck

Demonstranten in Hongkong kommunizieren über Mesh-Netzwerk | heise online - rek...

Demonstranten in Hongkong kom...

http://www.heise.de/newsticker/meldung/Demonstranten-in-Ho

heise online > News > 2014 > KW 41 > Demonstranten in Hongkong kommunizieren über Mes

06.10.2014 08:36

Technology Review « Vorige | Nächste »

Demonstranten in Hongkong kommunizieren über Mesh-Netzwerk

vorlesen / MP3-Download

Auch wenn die Behörden zwischenzeitlich die Mobilfunknetze abdrehten, blieben die Protestierenden in der chinesischen Sonderverwaltungszone untereinander in Verbindung. Apps wie FireChat machten es möglich.

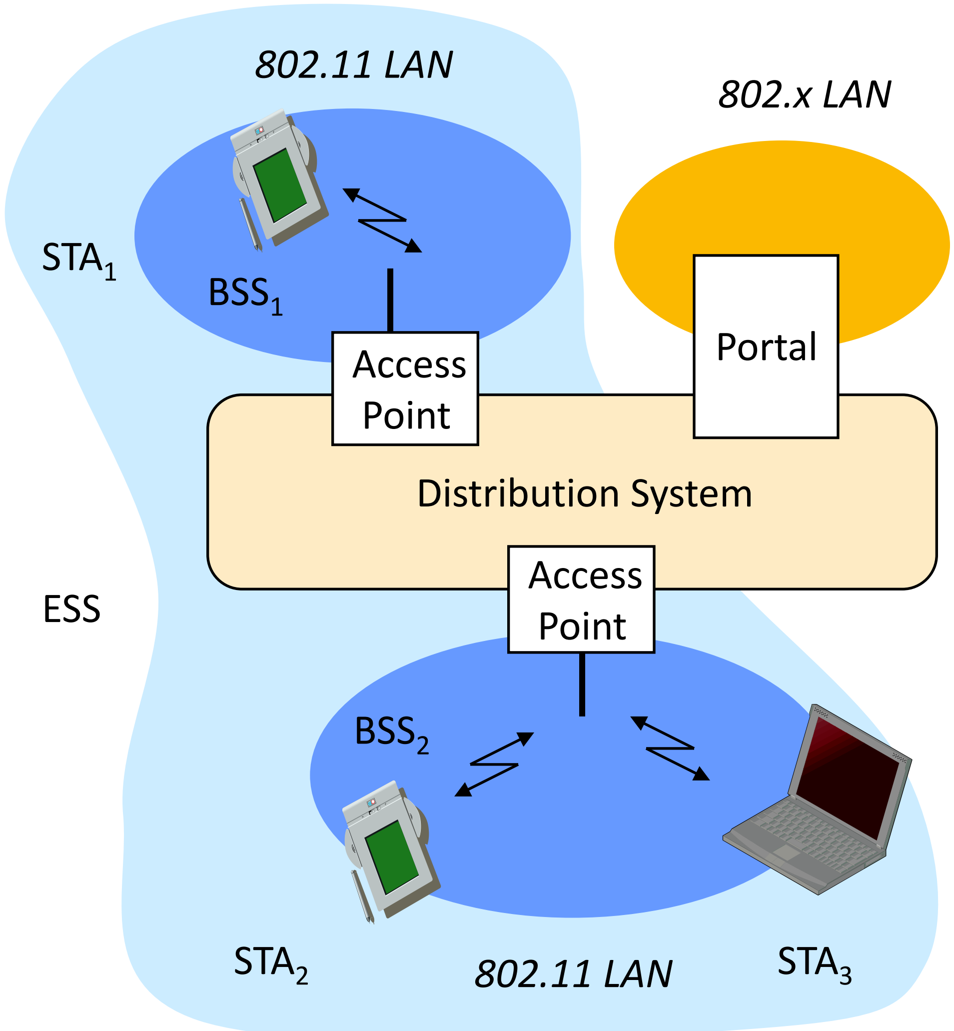
Die Demonstranten, die in Hongkong für mehr Demokratie demonstrieren, setzen stark auf neue Vernetzungstechniken wie die Mesh-Messaging-App FireChat, berichtet *Technology Review* in seiner Online-Ausgabe. Die App verbreitete sich erst seit dem vorvergangenen Samstag schnell. Ein Teenager habe in verschiedenen Social-Media-Postings andere Nutzer dazu aufgefordert, die App herunterzuladen, berichtet Christophe Daligault, Vizepräsident von Open Garden aus San Francisco, der jungen Firma hinter der App.

Von jenem Samstag bis zum Montag voriger Woche war die Anwendung die beliebteste App Hongkongs sowohl in Apples App Store für das iPhone als auch Googles Play Store für Android. Twitter, Facebook oder WhatsApp wurden dabei locker überrundet. In diesem Zeitraum luden mehr als 200.000 Menschen in der Sonderverwaltungszone die App aus einem der beiden Stores herunter. Nutzer in der Stadt sendeten rund zwei Millionen Nachrichten in diesen Tagen, bis zu 33.000 User kamen gleichzeitig zusammen, wie Daligault sagt.

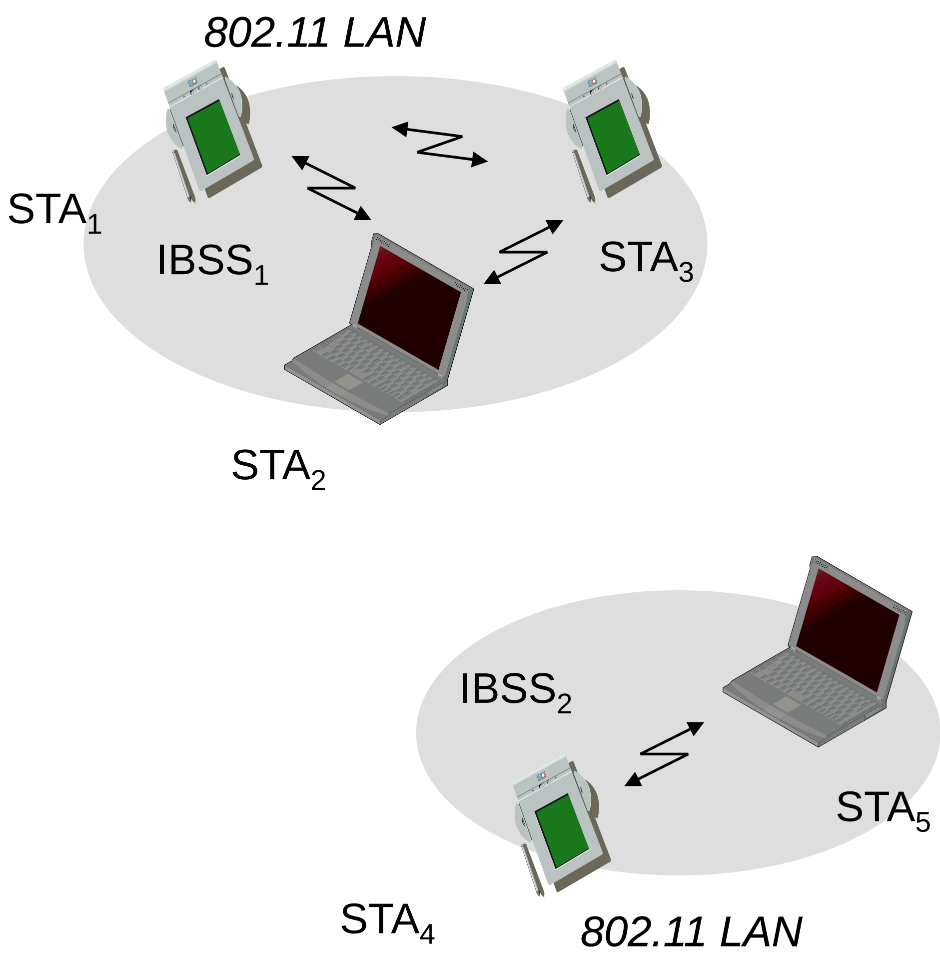
Mit Anwendung kann direkt von Telefon zu Telefon kommuniziert werden. Dabei wird entweder der Kurzstreckenfunk Bluetooth oder die WLAN-Variante WiFi Direct verwendet. Mit einer Mobilfunk- oder WLAN-Basisstation muss niemand verbunden sein. Wer FireChat öffnet, kann Text-Chat-Räume mit Menschen betreten, die sich in einem Umkreis von bis zu 60 Metern befinden. Das Netz kann aber auch deutlich größere Ausdehnungen haben, denn jeder Nutzer ist gleichzeitig ein weiterer Knoten.

FireChat wird vor allem für einfache Formen der Organisation genutzt, die App ist derzeit nicht verschlüsselt. "Man konnte Leute sehen, die 'Räume' für einen bestimmten Ort eröffnet haben, beispielsweise eine Straßenkreuzung oder ein bekanntes Gebäude", sagt Daligault. Die fragten da dann untereinander, wie viele Schutzmasken man brauche, wo man Wasser herbekomme und welche Angriffe der Polizei zu erwarten seien.

802.11 - Architecture of an infrastructure network

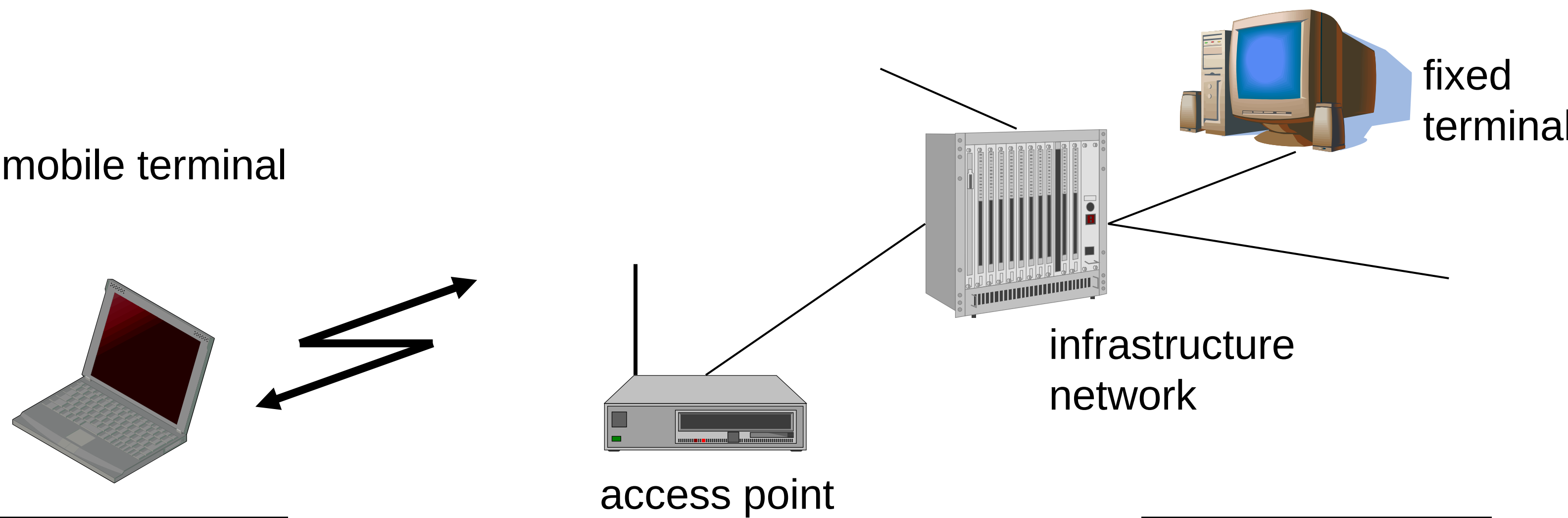


- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS



- Direct communication within a limited range
  - Station (STA):
    terminal with access mechanisms to the wireless medium
  - Independent Basic Service Set (IBSS):
    group of stations using the same radio frequency

IEEE standard 802.11



mobile terminal
application
TCP
IP
LLC
802.11 MAC
802.11 PHY

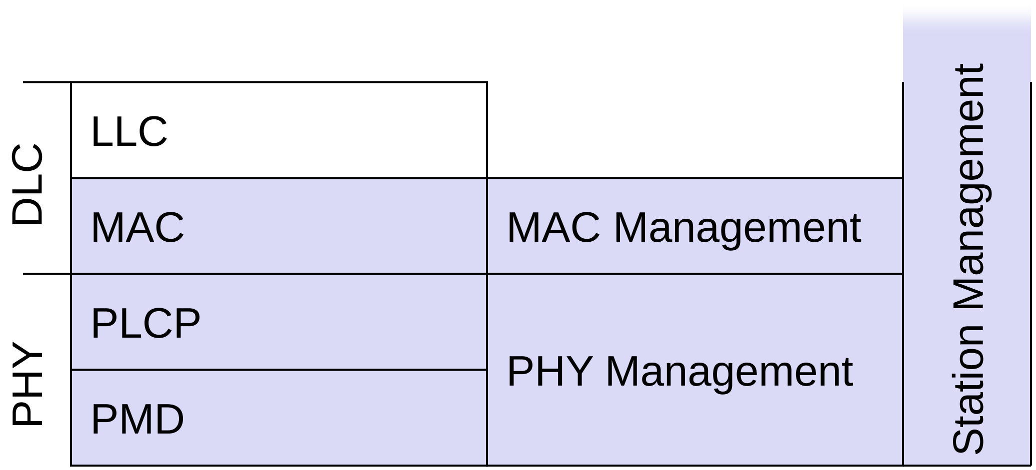
access point	
LLC	
802.11 MAC	802.3 MAC
802.11 PHY	802.3 PHY

fixed terminal
application
TCP
IP
LLC
802.3 MAC
802.3 PHY

802.11 - Layers and functions

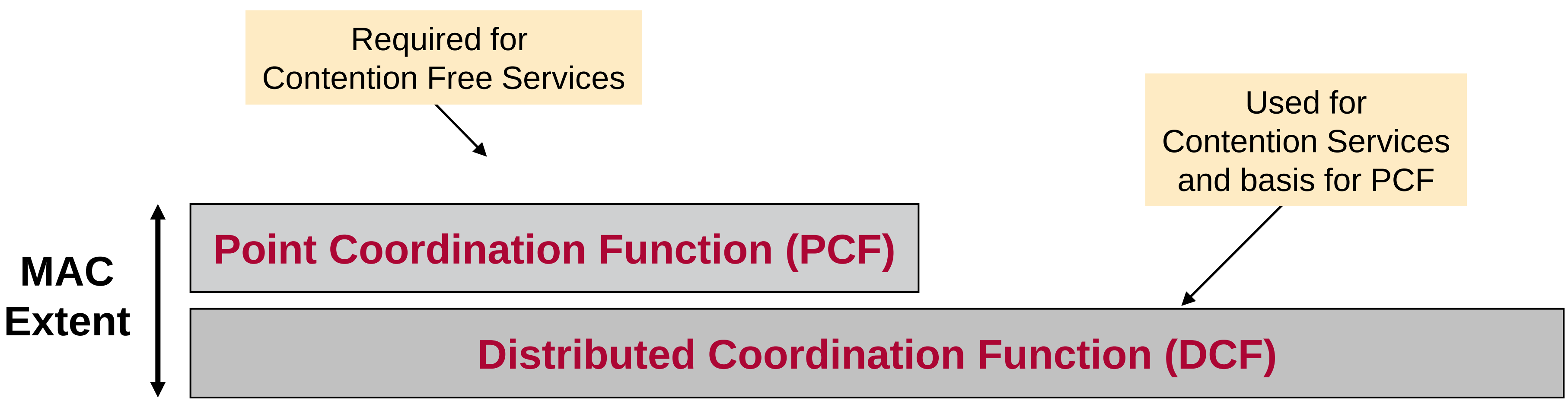
JS

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



Fundamental access method:
- **"Distributed Coordination Function" (DCF),**
- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).**
- shall be implemented **in all STAs** (both IBSS and infrastructure network configurations)

Optional access method:
- **"Point Coordination Function" (PCF),**
- polling with the BSS **access point** as **polling master**
- for **infrastructure network** configurations only



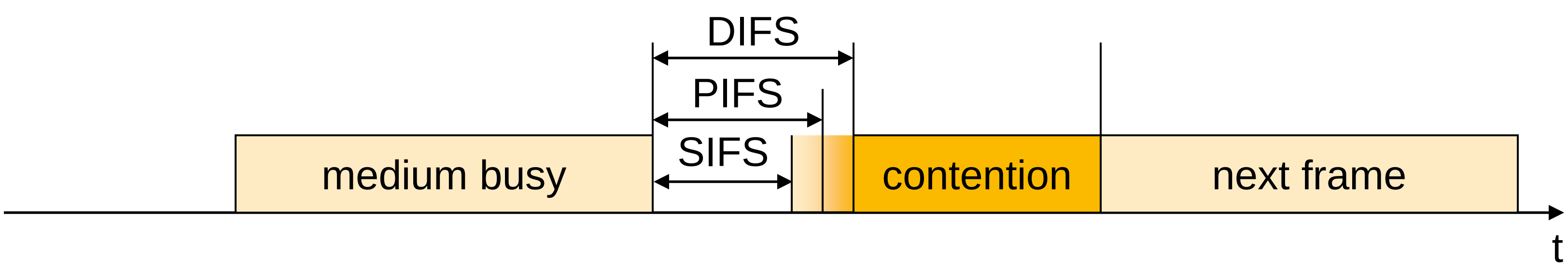
The DCF allows for automatic medium sharing through the use of

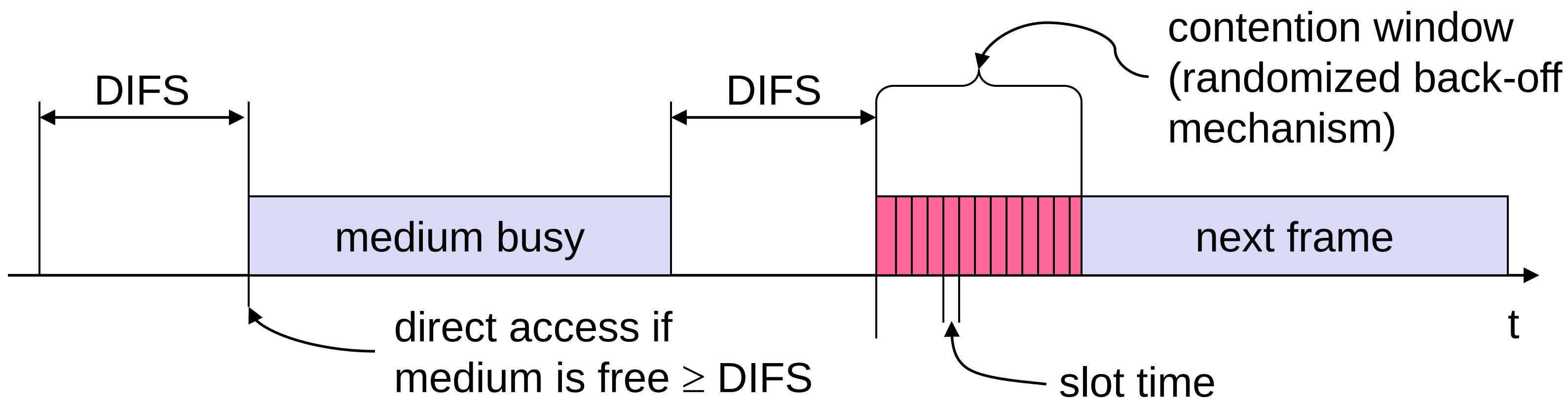
- **CSMA/CA** with a **random backoff time following a busy medium condition**.

All directed traffic uses immediate **positive acknowledgment** (ACK frame) where retransmission is scheduled by the sender if no ACK is received.

IEEE 802.11 defines **access priorities through different inter frame spaces:**

- **SIFS** (Short Inter Frame Spacing)
  - **highest priority**, for ACK, CTS, polling response
- **PIFS** (PCF IFS)
  - **medium priority**, for time-bounded service using PCF
- **DIFS** (DCF, Distributed Coordination Function IFS)
  - **lowest priority**, for asynchronous data service

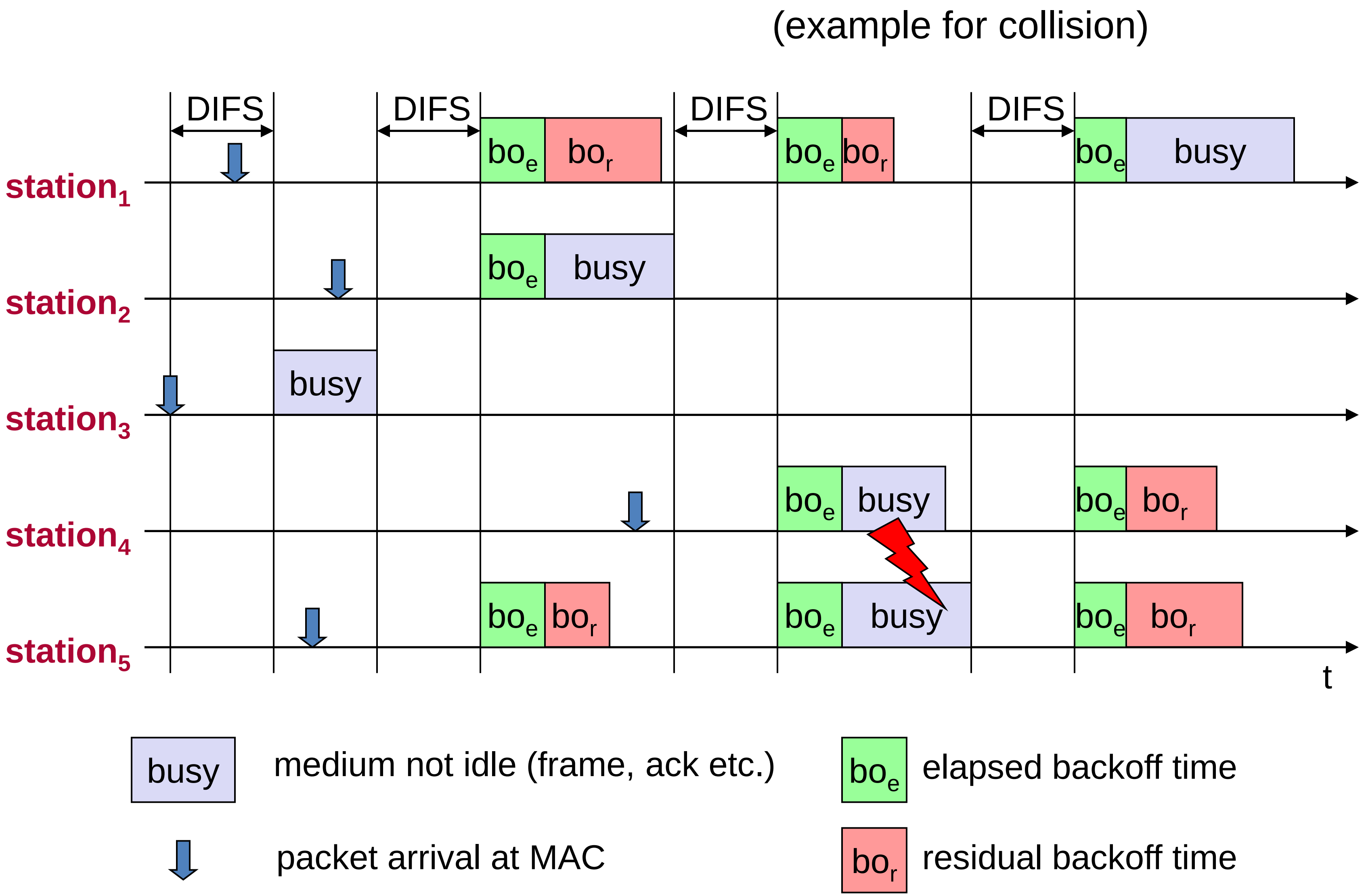




- when ready: start **sensing the medium**
- **if the medium is free** for the duration of an Inter-Frame Space (IFS), the station can **start sending** (IFS depends on service type)
- **if the medium is busy**,
  - the station has to **wait for a free IFS**,
  - then the station must **additionally wait a random back-off time** (collision avoidance, multiple of slot-time)
- **if another station occupies the medium during the back-off time** of the station, the **back-off timer stops** (fairness)
- IEEE 802.11 uses **exponential backoff**: The **contention window doubles** with each collision.

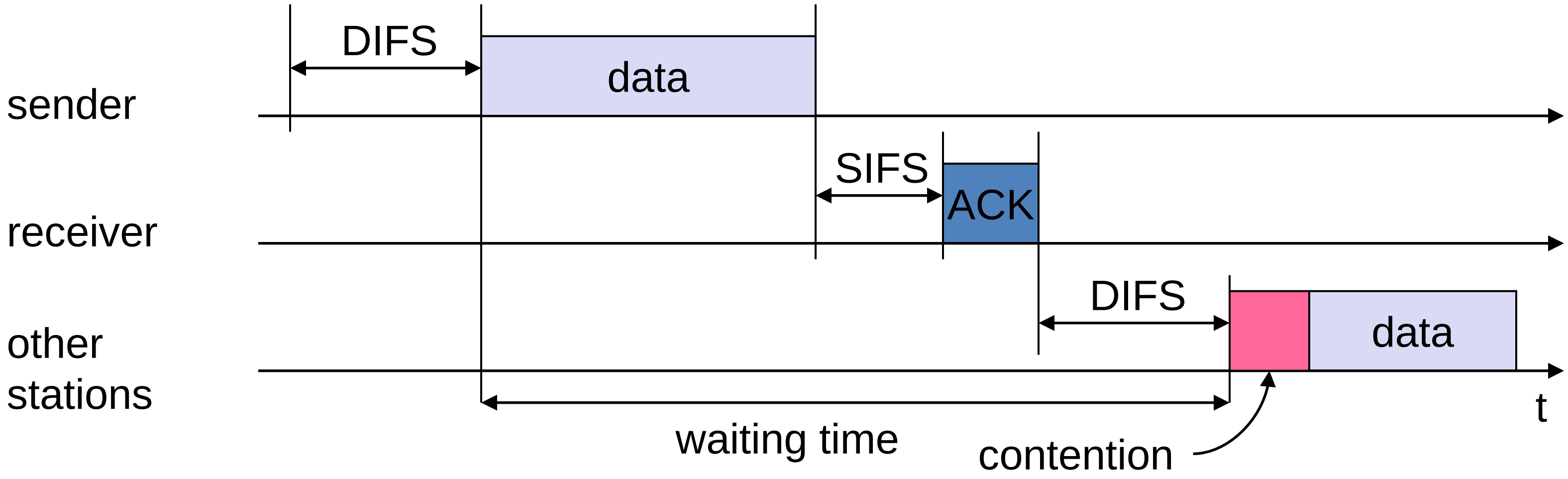
Basic idea: 5 stations competing for access

JS



Instead of Collision Detection, **IEEE 802.11 uses ACKs**:

- station has to **wait for DIFS** before sending data
- **receivers acknowledge at once** (after waiting for SIFS) if the packet was received correctly (CRC)
- **automatic retransmission** of data packets in case of transmission errors



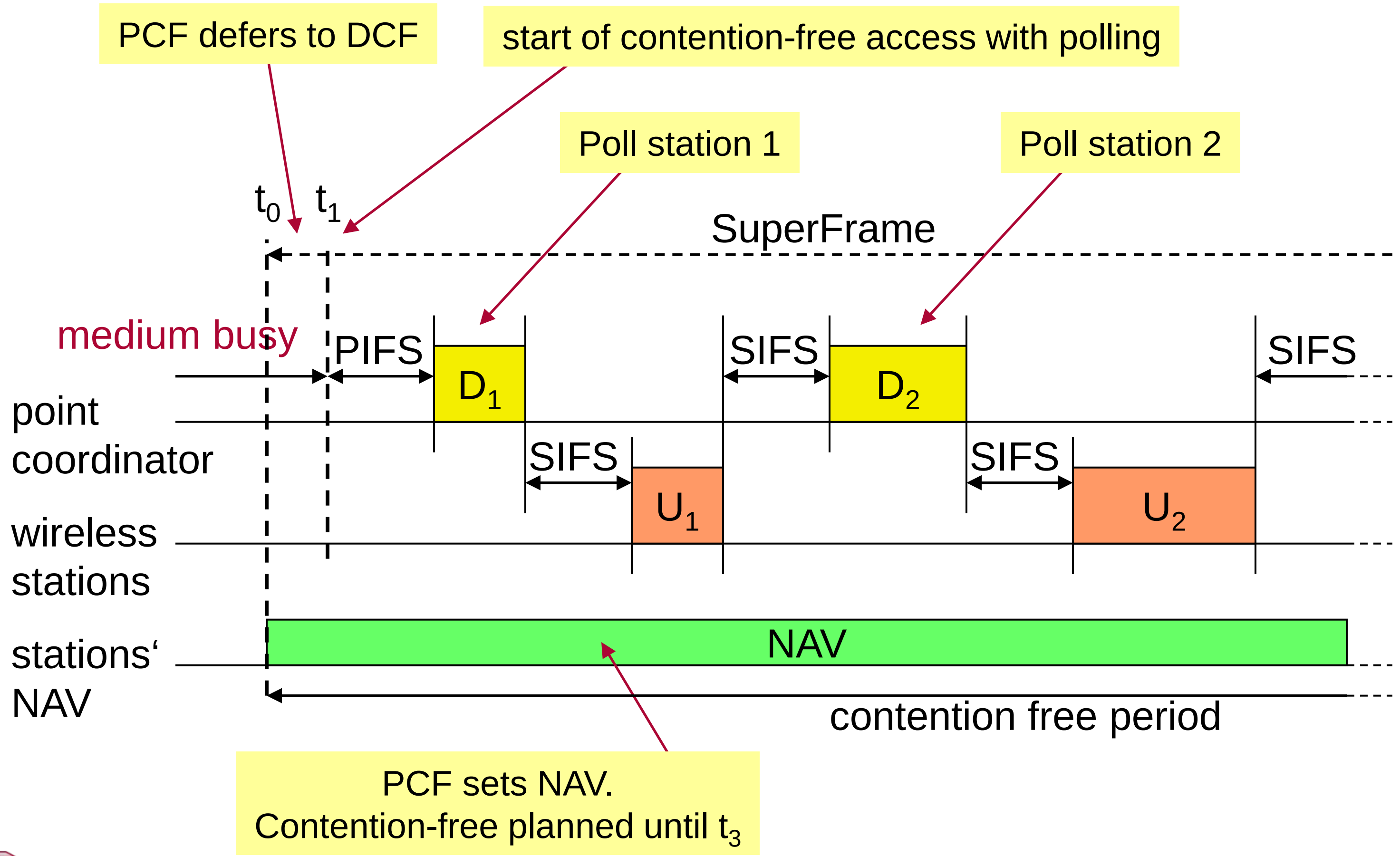
Duplicate frames (lost ACK) shall be filtered out within the destination MAC.

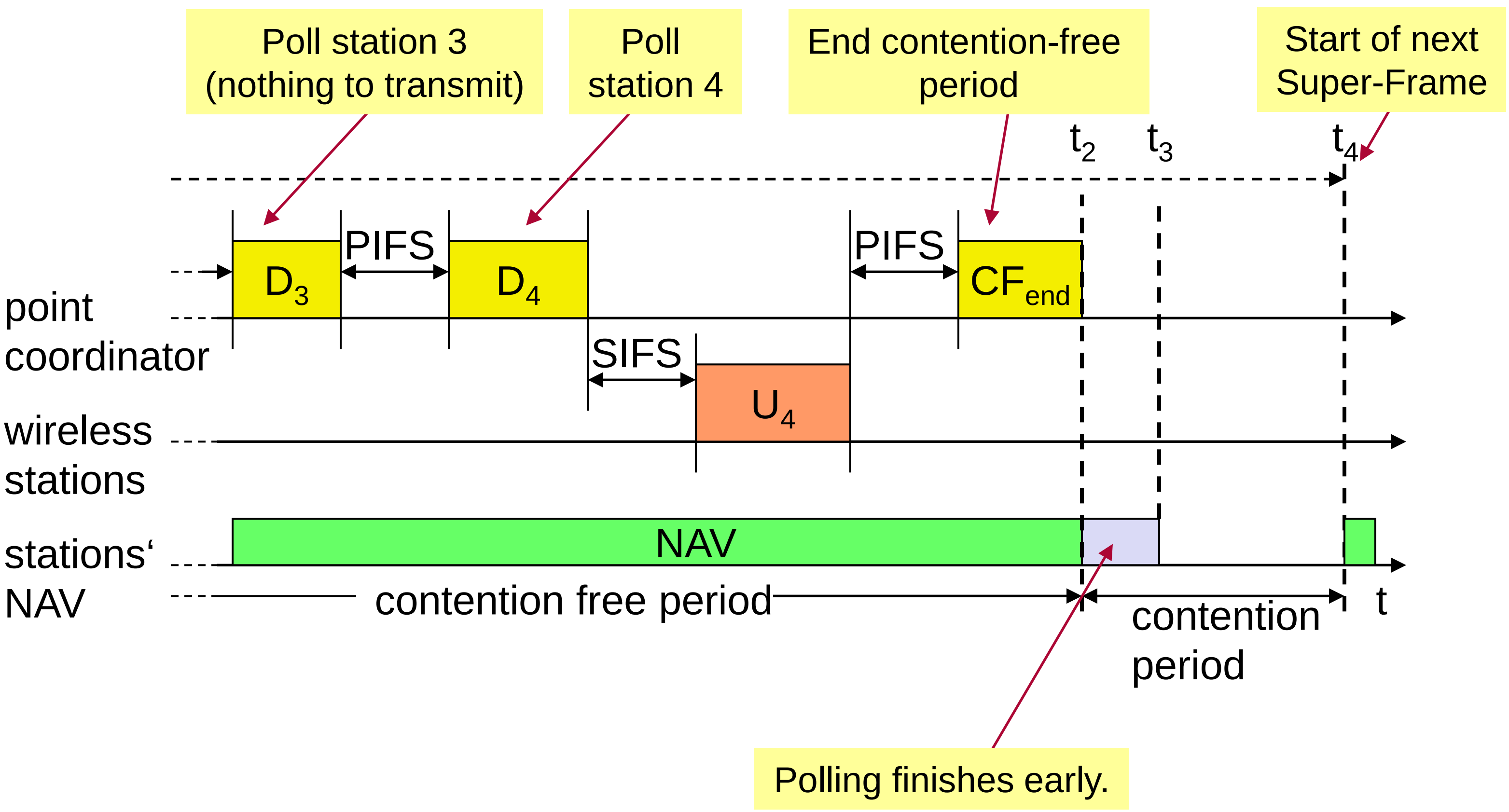
This is facilitated through a **Sequence Control field** (sequence number + fragment number) within data and management frames.

The sequence number is generated by the transmitting STA as an **incrementing sequence of integers.**

Maximum access delays and **minimum bandwidth** can only be **guaranteed** when using the **PCF** on top of the DCF.

At access points with PCF, **the point coordinator splits** the access **time** into "**super frame periods**".





Poll station 3 (nothing to transmit)
Poll station 4
End contention-free period
Start of next Super-Frame
t2
t3
t4
D3
PIFS
D4
PIFS
CFend
point coordinator
SIFS
U4
wireless stations
NAV
stations' NAV
contention free period
contention period
t
Polling finishes early.

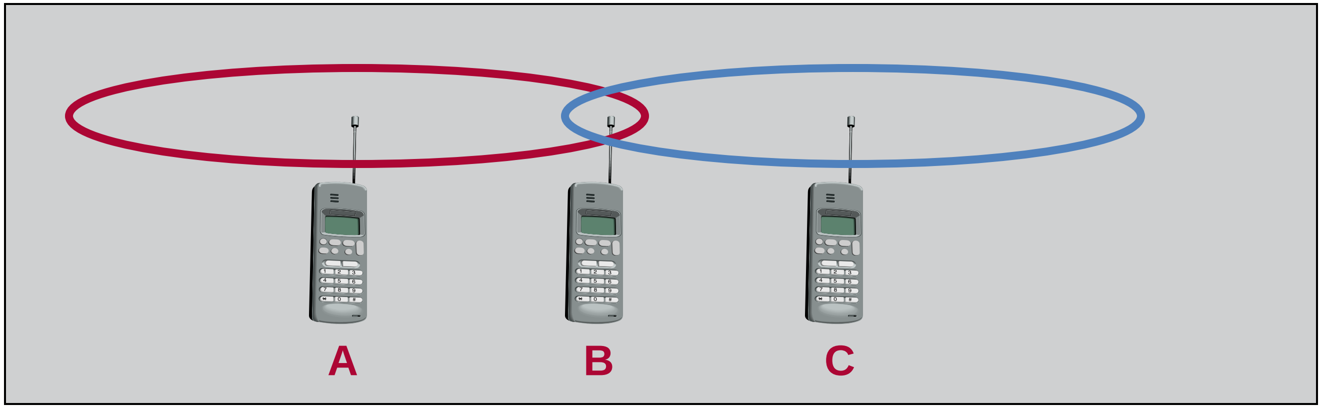
Summary: Point coordination function (PCF)

- The IEEE 802.11 MAC may also incorporate an **optional** access method called a PCF, which is **only usable on infrastructure network configurations**.
- This access method uses a **point coordinator** (PC), which shall operate **at the access point of the BSS**, to determine which STA currently has the right to transmit.
- The operation is essentially that of polling, with the **PC performing the role of the polling master.** The operation of the PCF may require additional coordination, not specified in this standard, to permit efficient operation in cases where multiple point-coordinated BSSs are operating on the same channel, in overlapping physical space.
- The PCF uses a **virtual carrier-sense mechanism** aided by an access priority mechanism. The PCF shall **distribute information within Beacon management frames to gain control of the medium by setting the network allocation vector (NAV) in STAs**.
- In addition, all frame transmissions under the PCF may use an **interframe space (IFS) that is smaller than the IFS for frames transmitted via the DCF**.
- The use of a smaller IFS implies that **point-coordinated traffic shall have priority access** to the medium over STAs in overlapping BSSs operating under the DCF access method.
- The access priority provided by a PCF may be utilized to create a **contention-free (CF) access method**. The PC controls the frame transmissions of the STAs so as to eliminate contention for a limited period of time.

IEEE 802.11-1999, pp. 70, 71

Hidden terminals

- A sends to B, C cannot receive A
- C wants to send to B, C senses a "free" medium (**CS fails**)
- collision at B, A cannot receive the collision (**CD fails**)
- **A is "hidden" for C**



=> cf. section 2. Wireless Communication Basics

RTS/CTS, optional

The **exchange of RTS and CTS frames** is one means of distribution of **medium reservation** information. RTS and CTS frames contain a **Duration/ID field** that defines the period of time that the medium is to be **reserved to transmit the actual data frame and the returning ACK frame**.

All STAs within the reception range of either the originating STA (which transmits the RTS) or the destination STA (which transmits the CTS) shall learn of the medium reservation. Thus a **STA can be unable to receive from the originating STA, yet still know about the impending use of the medium to transmit a data frame**.

The RTS/CTS exchange also performs both a type of **fast collision inference and a transmission path check**. If the return CTS is not detected by the STA originating the RTS, the originating STA may repeat the process (after observing the other medium-use rules) more quickly than if the long data frame had been transmitted + a return ACK frame had not been detected.

IEEE 802.11-1999, p. 71

RTS = request to send
CTS = clear to send
(class 1 frames, cf. slide 21)

RTS/CTS, optional (2)

The RTS/CTS mechanism **cannot be used for** MPDUs **with broadcast and multicast** immediate address because there are multiple destinations for the RTS, and thus potentially multiple concurrent senders of the CTS in response. The RTS/CTS mechanism need not be used for every data frame transmission. Because the additional RTS and CTS frames add overhead inefficiency, the **mechanism is not always justified**, especially for short data frames.

The use of the RTS/CTS mechanism is under control of the **dot11RTSThreshold attribute**. This attribute may be set on a **per-STA basis**. This mechanism allows STAs to be configured to use **RTS/CTS either always, never, or only on frames longer than a specified length**.

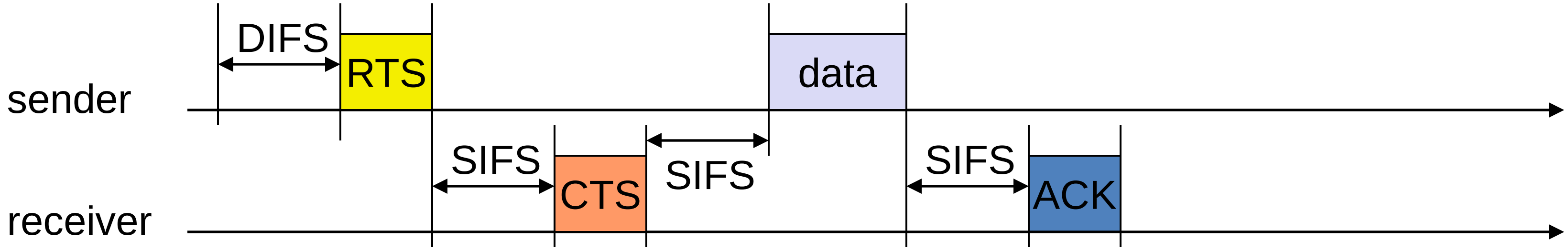
A STA configured not to initiate the RTS/CTS mechanism shall still update its virtual carrier-sense mechanism with the duration information contained in a received RTS or CTS frame, and shall always respond to an RTS addressed to it with a CTS.

The medium access protocol allows for STAs to support different sets of data rates. All **STAs shall receive all the data rates in aBasicRateSet** and **transmit at one or more** of the aBasicRateSet data rates. To support the proper operation of the RTS/CTS and the virtual carrier-sense mechanism, all STAs shall be able to detect the RTS and CTS frames. For this reason the **RTS and CTS frames shall be transmitted at one of the aBasicRateSet rates**.

IEEE 802.11-1999, pp. 71, 72

RTS = request to send
CTS = clear to send
(class 1 frames, cf. slide 21)

- station can **send RTS** with reservation parameter **after waiting for DIFS** (reservation determines amount of time the data packet needs the medium)
- **acknowledgement via CTS after SIFS** by receiver (if ready to receive)
- sender can now **send data at once, acknowledgement via ACK**
- **other stations store medium reservations** distributed via RTS and CTS



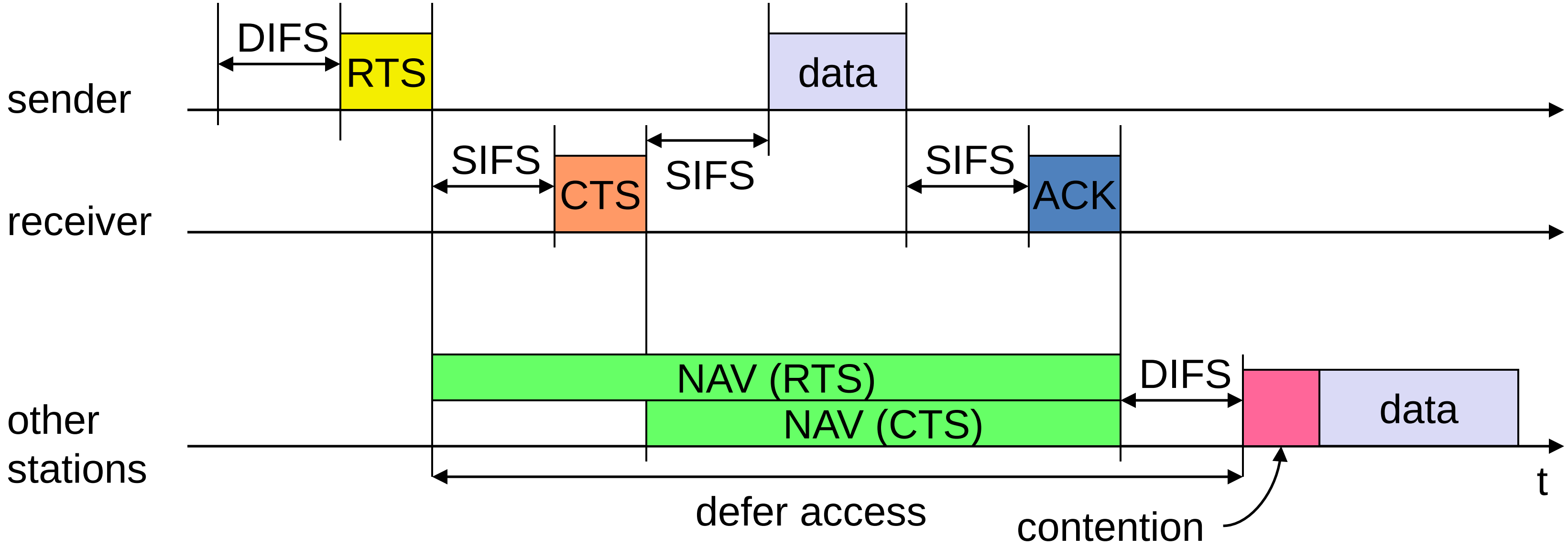
RTS = request to send
CTS = clear to send
(class 1 frames, cf. slide 21)

Example: NAV with RTS/CTS

Virtual carrier sensing: Network allocation vector (NAV)

The NAV maintains a **prediction of future traffic** on the medium based on duration information that is announced in RTS/CTS frames prior to the actual exchange of data.

- station can **send RTS** with reservation parameter **after waiting for DIFS** (reservation determines amount of time the data packet needs the medium)
- **acknowledgement via CTS after SIFS** by receiver (if ready to receive)
- sender can now **send data at once, acknowledgement via ACK**
- **other stations store medium reservations** distributed via RTS and CTS



How about the hidden terminal problem and RTS/CTS with NAV?

RTS/CTS – How about performance?

The use of **802.11 RTS/CTS** can increase the reliability of 802.11 data frame transmissions in the presence of hidden nodes, which improves the throughput of the network. Similar to analyzing the need for fragmentation, a way to gauge whether RTS/CTS will help throughput is to monitor the WLAN for retransmissions. **If the retransmission rate is low** (under 5 percent), **do not implement RTS/CTS**. The additional frame transmissions need to implement RTS/CTS will likely **dramatically increase the overhead on the network**, which will actually reduce throughput. [..]

In most cases, **initiating RTS/CTS in the access point is fruitless** because the hidden station problem does not exist from the perspective of the access point. All stations having valid associations are within range and not hidden from the access point. Forcing the access point to implement the RTS/CTS handshake will significantly increase the overhead and reduce throughput. **Focus on using RTS/CTS in the client radios to improve performance**.

Source: Jim Geier "WLAN Design: Range, Performance, and Roaming Considerations" in "Designing and Deploying 802.11n Wireless Networks", Cisco Press, 2010.

WLAN general frame format

- **Types**
  - control frames, management frames, data frames
- **Sequence numbers**
  - important against duplicated frames due to lost ACKs
- **Addresses**
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- **Miscellaneous**
  - sending time, checksum, frame control, data

Important message:
Four (!) address fields

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order
bits	2	2	4	1	1	1	1	1	1	1	1

scenario	to DS	from DS	address 1	address 2	address 3	address 4
Ad-hoc network	0	0	DA	SA	BSSID	-
Infrastructure network, from AP	0	1	DA	BSSID	SA	-
Infrastructure network, to AP	1	0	BSSID	SA	DA	-
Infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS and CTS

Acknowledgement (ACK):

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

Request To Send (RTS):

bytes	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	CRC

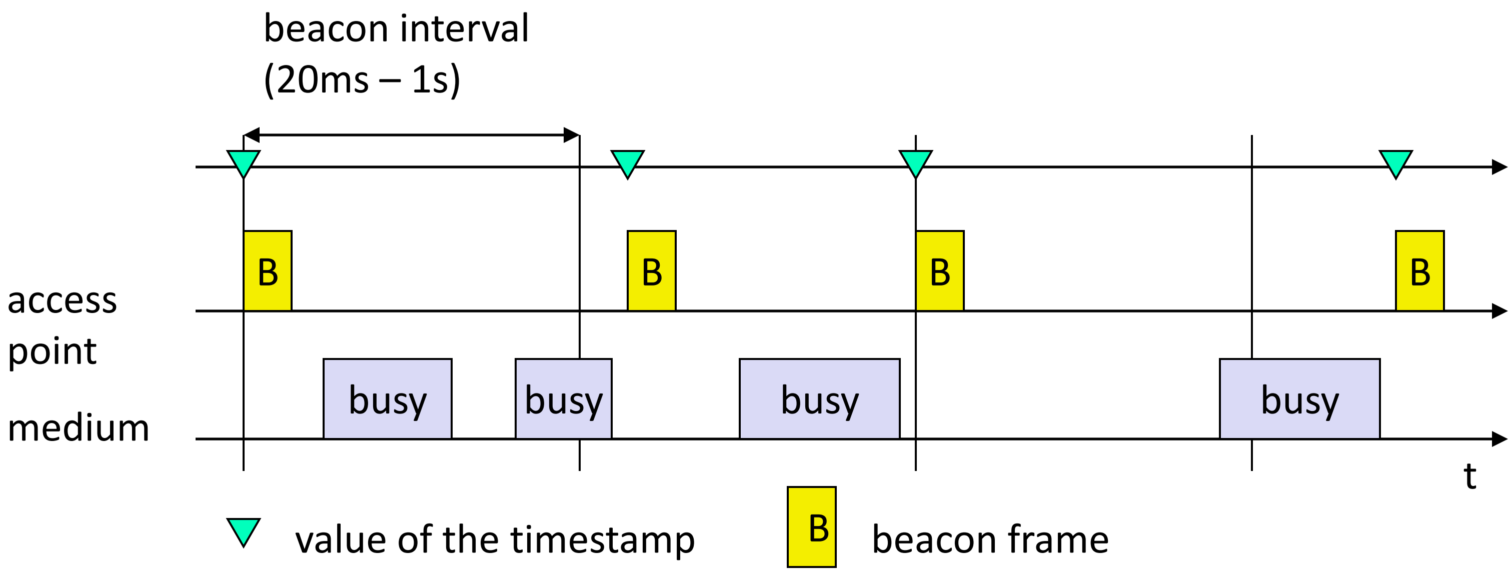
Clear To Send (CTS):

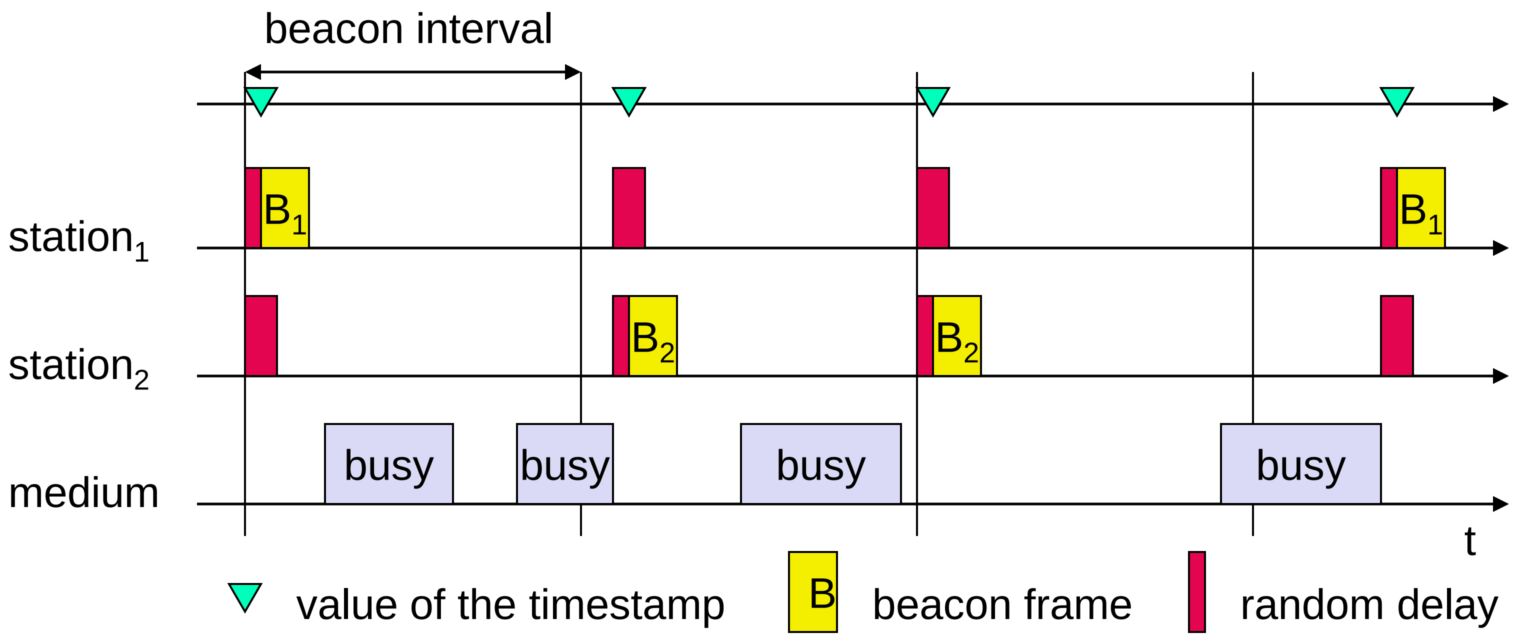
bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

802.11 - MAC management

- Synchronization
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

Synchronization using a Beacon (infrastructure)

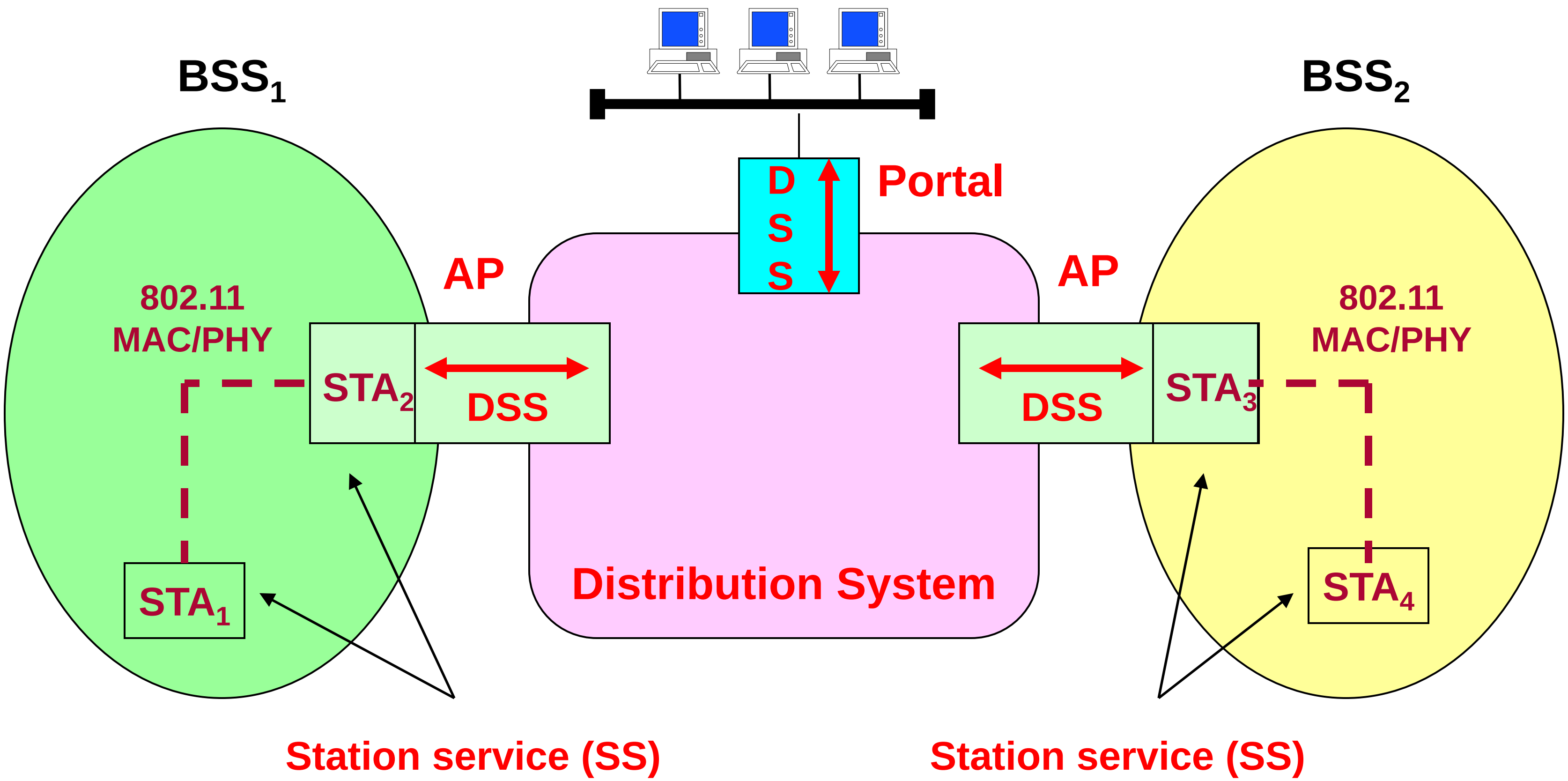



beacon interval
station1
station2
medium
B1
B2
B2
B1
busy
busy
busy
busy
t
value of the timestamp
B
beacon frame
random delay

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources
- Fast roaming – 802.11r
  - e.g. for vehicle-to-roadside networks

IEEE 802.11 specifies **two categories of service** provided **to the IEEE 802.11 MAC**:
- the **station service (SS)** and
- the **distribution system service (DSS).**

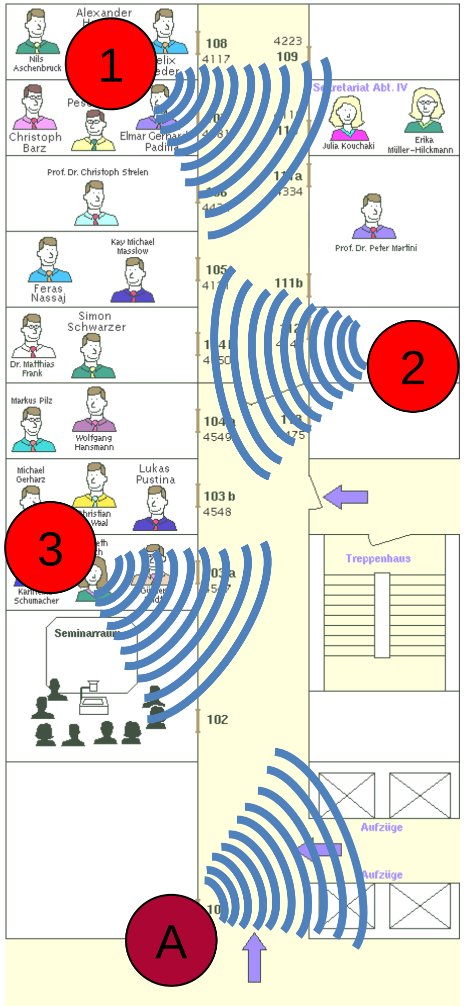
The standard does not constrain the DS to be either data link or network layer based, either centralized or distributed on nature.



Station service (SS)	Distribution system service (DSS)
The SSs are as follows: a) **Authentication** b) **Deauthentication** c) **Privacy** d) **MSDU delivery**	The DSSs are as follows: a) **Association** b) **Disassociation** c) **Distribution** d) **Integration** e) **Reassociation**

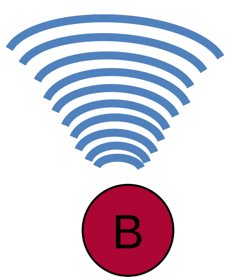
• The SS is **present in every IEEE 802.11 station** (including APs, as APs include station functionality).
• All conformant stations provide SS.
	• The DSS is
	  • **represented** in the IEEE 802.11 architecture **by arrows within the APs**,
	  • used to **cross media and address space logical boundaries**.
	• The **physical embodiment** of various services **may or may not be within a physical AP**.
	• The DSSs are **provided by the DS**. They are **accessed via a STA** that also provides DSSs. A STA that is providing access to DSS is an AP.

Example of SS/DSS services – with moving device



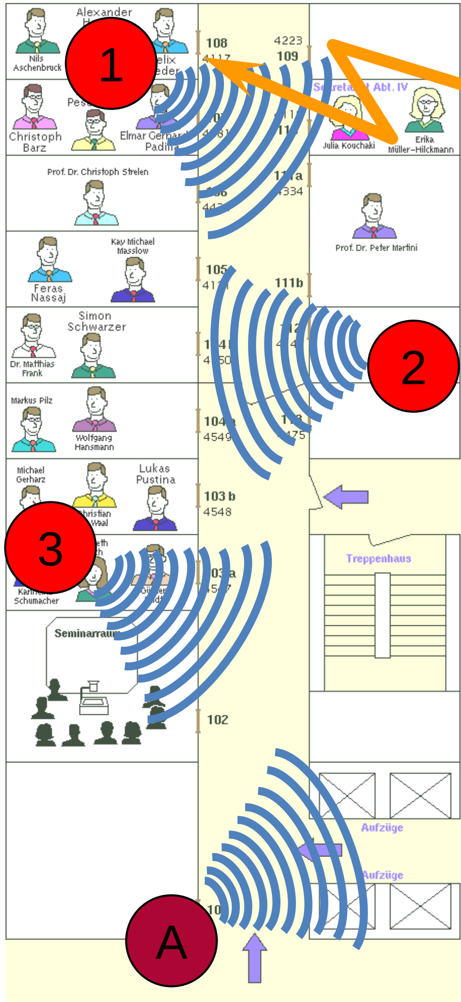
„private“ WLAN of
research group Martini

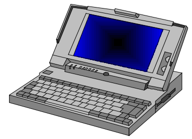
public WLAN of
Uni Bonn
SSID „bonnet“



The access points form
a cellular system and
neighbouring APs
use different channels.

1st floor Neubau
Römerstr.
(history: was up to 05/2009)



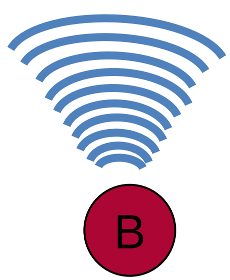


Station service:

1. authentication – only devices with registered MAC addresses may contact AP
2. privacy – encryption is activated

Distribution system service:

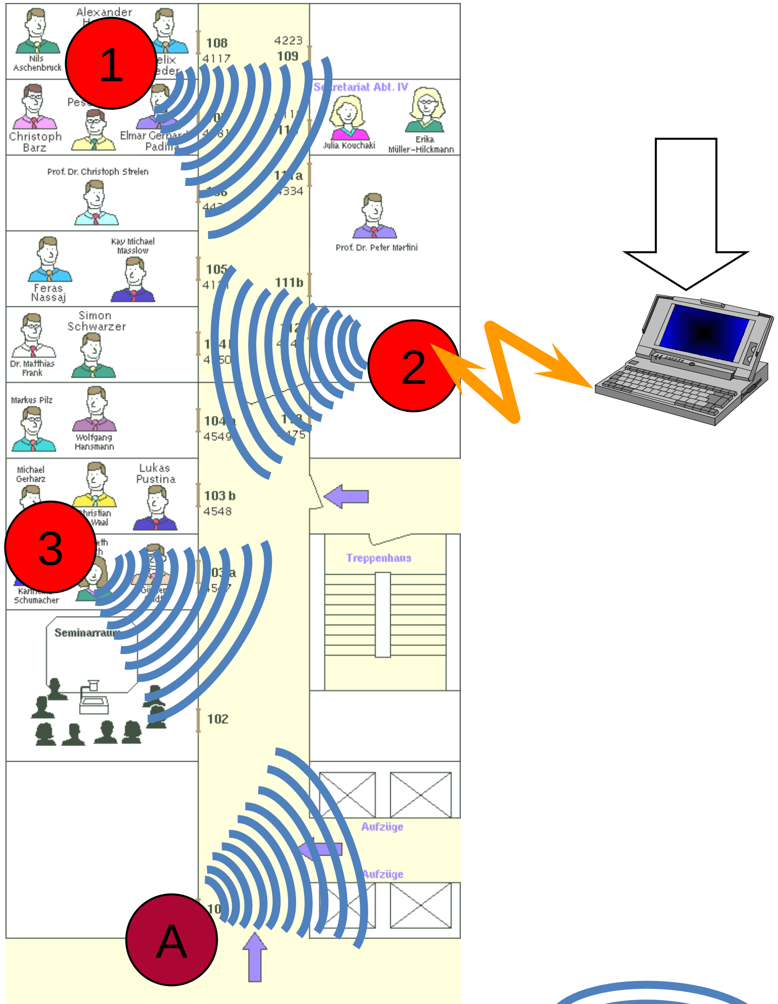
1. association – with AP 1
2. distribution – with devices within ESS
3. integration – with hosts in LAN or Internet

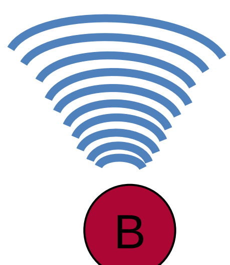


The mobile device receives an IP address via DHCP, e.g. 131.220.6.48

1st floor Neubau Römerstr.

Example of SS/DSS services – with moving device





1st floor Neubau Römerstr.

Movement within ESS = BSS-transition

Station service:

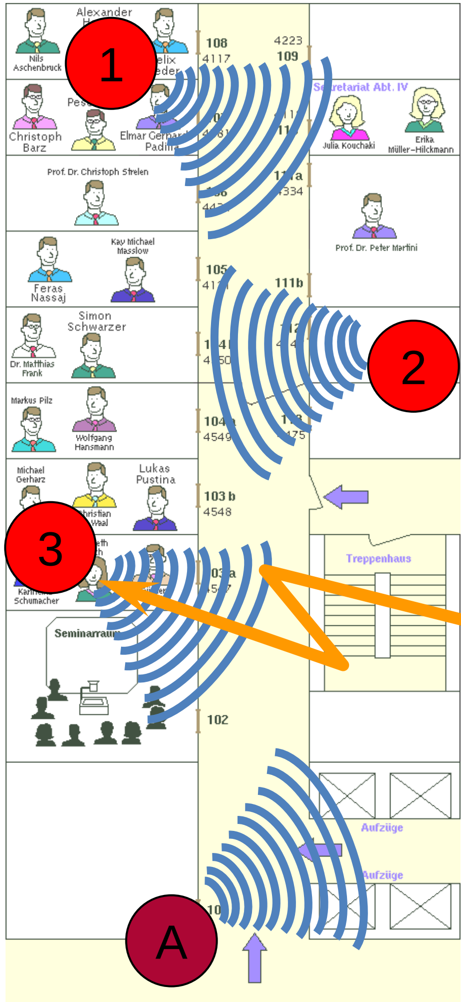
1. authentication – only devices with registered MAC addresses may contact AP
2. privacy – encryption is activated

Distribution system service:

1. re-association – with AP 2
2. distribution – with devices within ESS
3. integration – with hosts in LAN or Internet

The mobile device keeps the IP address e.g. 131.220.6.48
in particular: higher layers will not notice about movement!

Example of SS/DSS services – with moving device

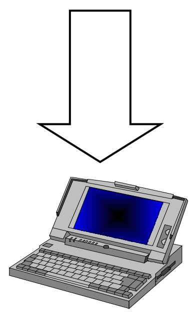


1st floor Neubau Römerstr.

Movement within ESS = BSS-transition

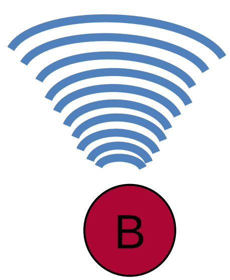
Station service:

1. authentication – only devices with registered MAC addresses may contact AP
2. privacy – encryption is activated

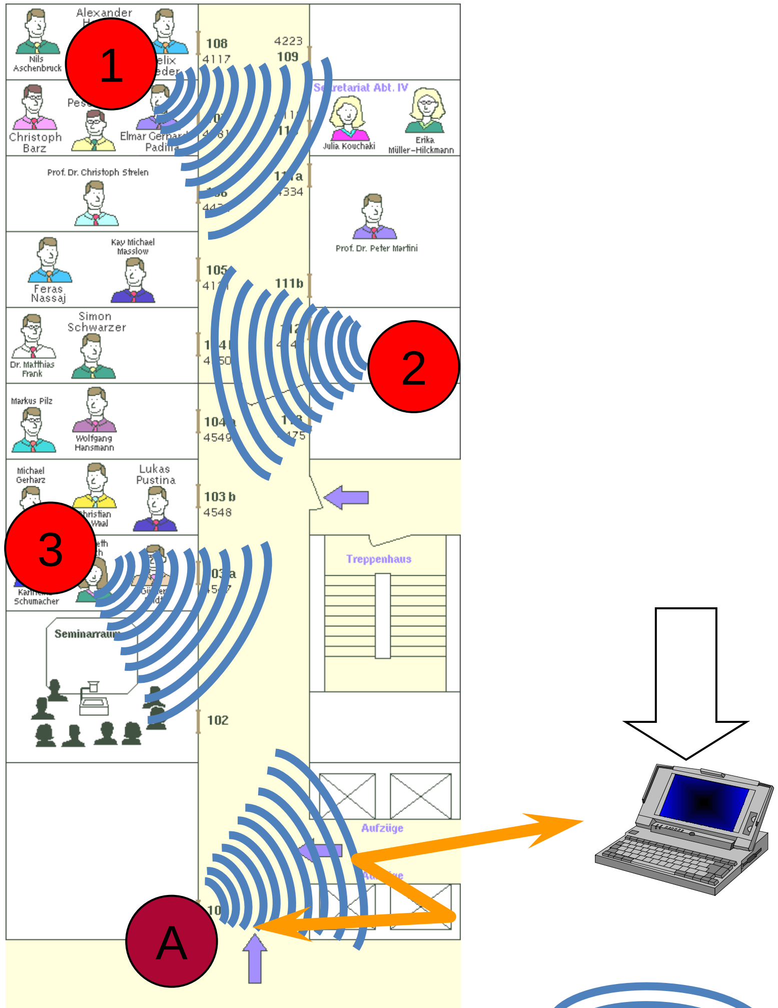


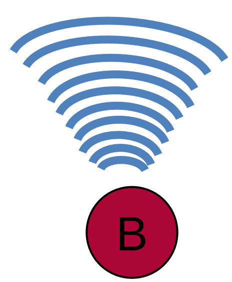
Distribution system service:

1. re-association – with AP 3
2. distribution – with devices within ESS
3. integration – with hosts in LAN or Internet



The mobile device keeps the IP address
e.g. 131.220.6.48
in particular: higher layers will not notice about movement!





1st floor Neubau
Römerstr.

Movement to different ESS = ESS-transition

Station service with new AP:

1. no authentication !
2. no privacy – encryption is not activated!

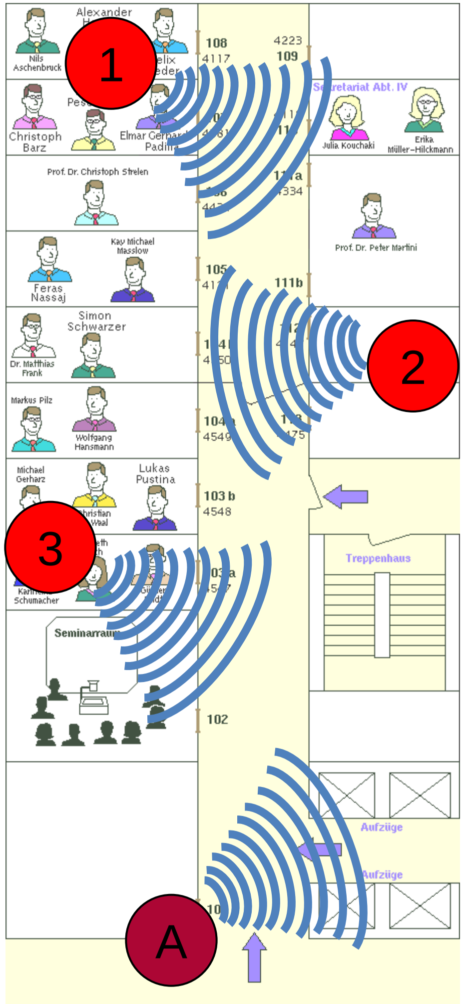
(Security features in „bonnet“ via VPN!)

Distribution system service:

1. (possibly) disassocation – with AP 3 before leaving
2. association – with AP A
3. distribution – with devices within ESS

Integration via portal/gateway only possible after VPN connection has been set up!

The mobile device receives a new IP address via DHCP, e.g. 10.243.1.80 (private)
the VPN-client receives 131.220.243.99 (public)



1st floor Neubau
Römerstr.

Movement within ESS = BSS-transition

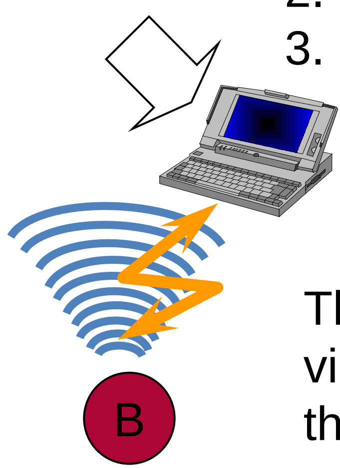
Station service with new AP:

1. no authentication !
2. no privacy – encryption is not activated!

(Security features in „bonnet“ via VPN!)

Distribution system service:

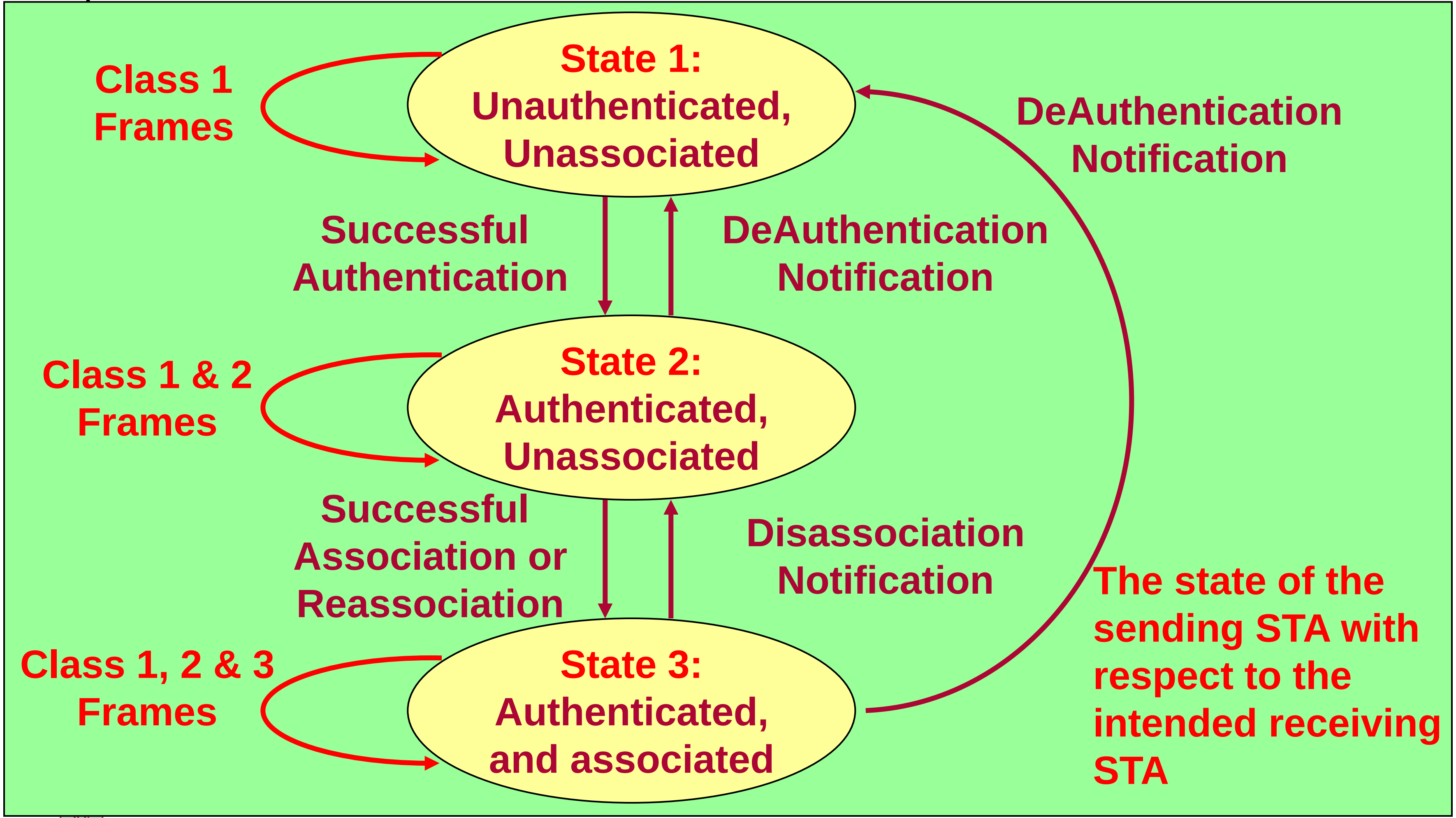
1. re-association – with AP B
2. distribution – with devices within ESS
3. integration via portal/gateway
   VPN connection still active



The mobile device keeps the IP addresses
via DHCP, e.g. 10.243.1.80 (private)
the VPN-client keeps 131.220.243.99 (public)

A STA keeps two state variables (Authentication State and Association State) resulting in **three local states for each remote STA**:

The current **state** existing between the source and destination station **determines the IEEE 802.11 frame types that may be exchanged** between that pair of STAs.



Class 1 frames (permitted from within States 1, 2, and 3):

1) Control frames

i. Request to send (RTS)
ii. Clear to send (CTS)
iii. Acknowledgment (ACK)
iv. Contention-Free (CF)-End+ACK
v. CF-End

Frames for ad hoc mode
or
to achieve authentication

2) Management frames

i. Probe request/response
ii. Beacon
iii. Authentication:
Successful authentication enables a station to exchange Class 2 frames. Unsuccessful authentication leaves the STA in State 1.
iv. Deauthentication:
Deauthentication notification when in State 2 or State 3 changes the STA's state to State 1. The STA shall become authenticated again prior to sending Class 2 frames.
v. Announcement traffic indication message (ATIM)

3) Data frames

i. Data:
Data frames with frame control (FC) control bits “To DS” and “From DS” both false.

Class 2 frames (if and only if authenticated; allowed from within State 2 and State 3 only):

1) Management frames:

Frames
to achieve association

i. **Association request/response**
   - Successful association enables Class 3 frames.
   - Unsuccessful association leaves STA in State 2.

ii. **Reassociation request/response**
   - Successful reassociation enables Class 3 frames.
   - Unsuccessful reassociation leaves the STA in State 2 (with respect to the STA that was sent the reassociation message). Reassociation frames shall only be sent if the sending STA is already associated in the same ESS.

iii. **Disassociation**
   - Disassociation notification when in State 3 changes a Station's state to State 2. This station shall become associated again if it wishes to utilize the DS.

If STA A receives a Class 2 frame with a unicast address in the address 1 field from STA B that is not authenticated with STA A, STA A shall send a deauthentication frame to STA B.

Class 3 frames (if and only if associated; allowed only from within State 3):

1) Data frames

- **Data subtypes:** Data frames allowed. That is, either the "To DS" or "From DS" FC control bits may be set to true to utilize DSSs.

2) Management frames

- **Deauthentication:** Deauthentication notification when in State 3 implies disassociation as well, changing the STA's state from 3 to 1. The station shall become authenticated again prior to another association.

3) Control frames

- **PS-Poll**

Frames for infrastructure mode i.e. communication with AP and via DS

If STA A receives a Class 3 frame with a unicast address in the address 1 field from STA B that is authenticated but not associated with STA A, STA A shall send a disassociation frame to STA B.

If STA A receives a Class 3 frame with a unicast address in the address 1 field from STA B that is not authenticated with STA A, STA A shall send a deauthentication frame to STA B.

Evolution of WLAN bandwidth in 802.11 standards

IEEE 802.11 (1999 Edition) – Basis of WLAN

- ISM (Industrial Scientific Medical) Band 2.4 GHz
- Data rates **1 and 2 Mbit/s**, FHSS + DSSS

IEEE 802.11b-1999 - Supplement to 802.11

- Data rates **5.5 and 11 Mbit/s** (only DSSS) at 2.4 GHz

IEEE 802.11a-1999

- Data rates **up to 54 Mbit/s at 5 GHz**

IEEE 802.11g-2003

- Data rates **up to 54 Mbit/s at 2.4 GHz**

IEEE 802.11n-2009

- Data rates **up to 300 ... 600 Mbit/s at 2.4 GHz/5 GHz (backw. comp. to 11b/g/a)**

- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - DSSS, 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products, many vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

Long PLCP PPDU format

128	16	8	8	16	16	variable	bits
synchronization	SFD	signal	service	length	HEC	payload	

$\underbrace{\text{synchronization} \mid \text{SFD}}_{\text{PLCP preamble}}$ $\underbrace{\text{signal} \mid \text{service} \mid \text{length} \mid \text{HEC}}_{\text{PLCP header}}$

PLCP preamble + PLCP header: 192 µs at 1 Mbit/s DBPSK

payload: 1, 2, 5.5 or 11 Mbit/s

Short PLCP PPDU format (optional)

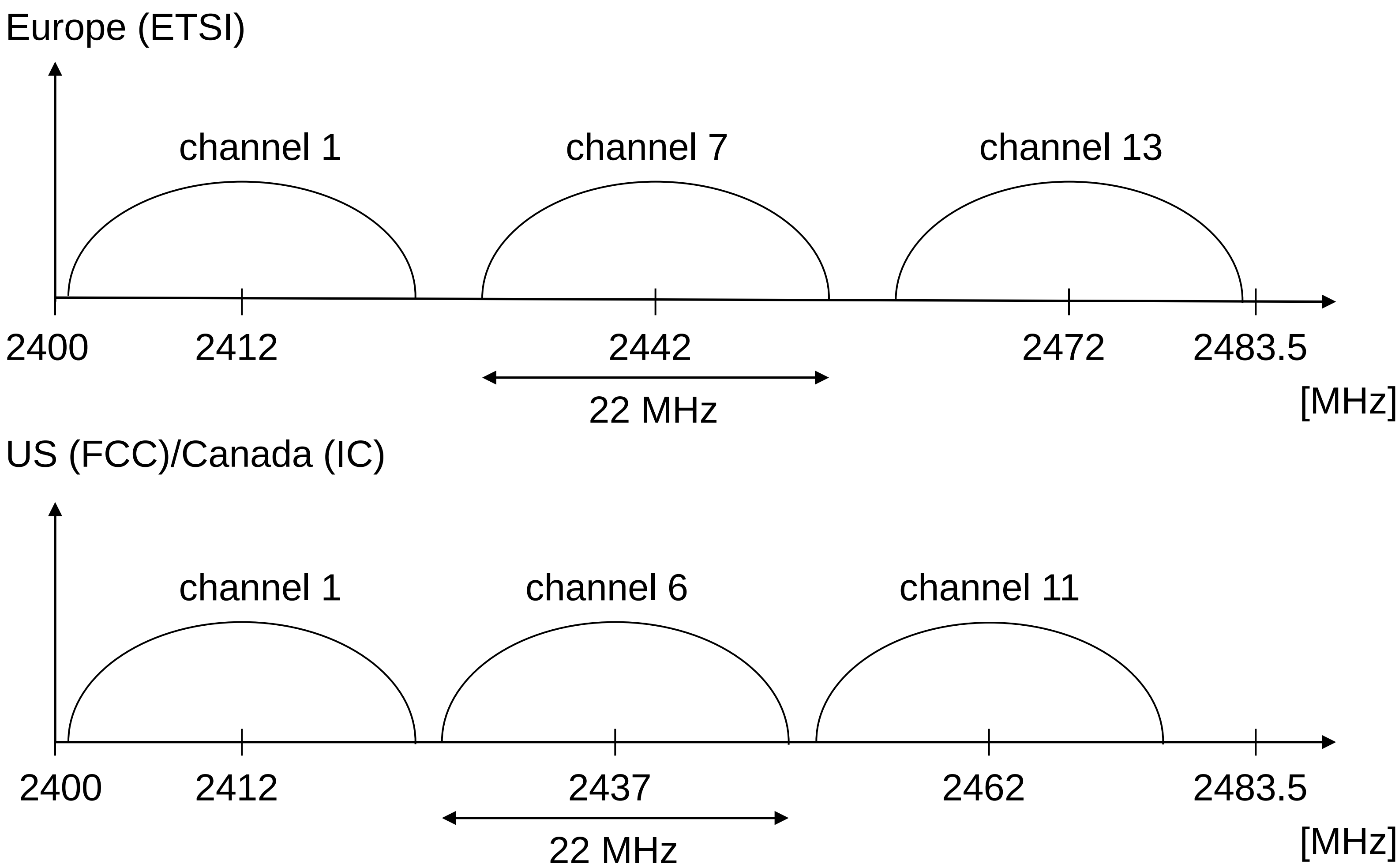
56	16	8	8	16	16	variable	bits
short synch.	SFD	signal	service	length	HEC	payload	

PLCP preamble
(1 Mbit/s, DBPSK)

PLCP header
(2 Mbit/s, DQPSK)

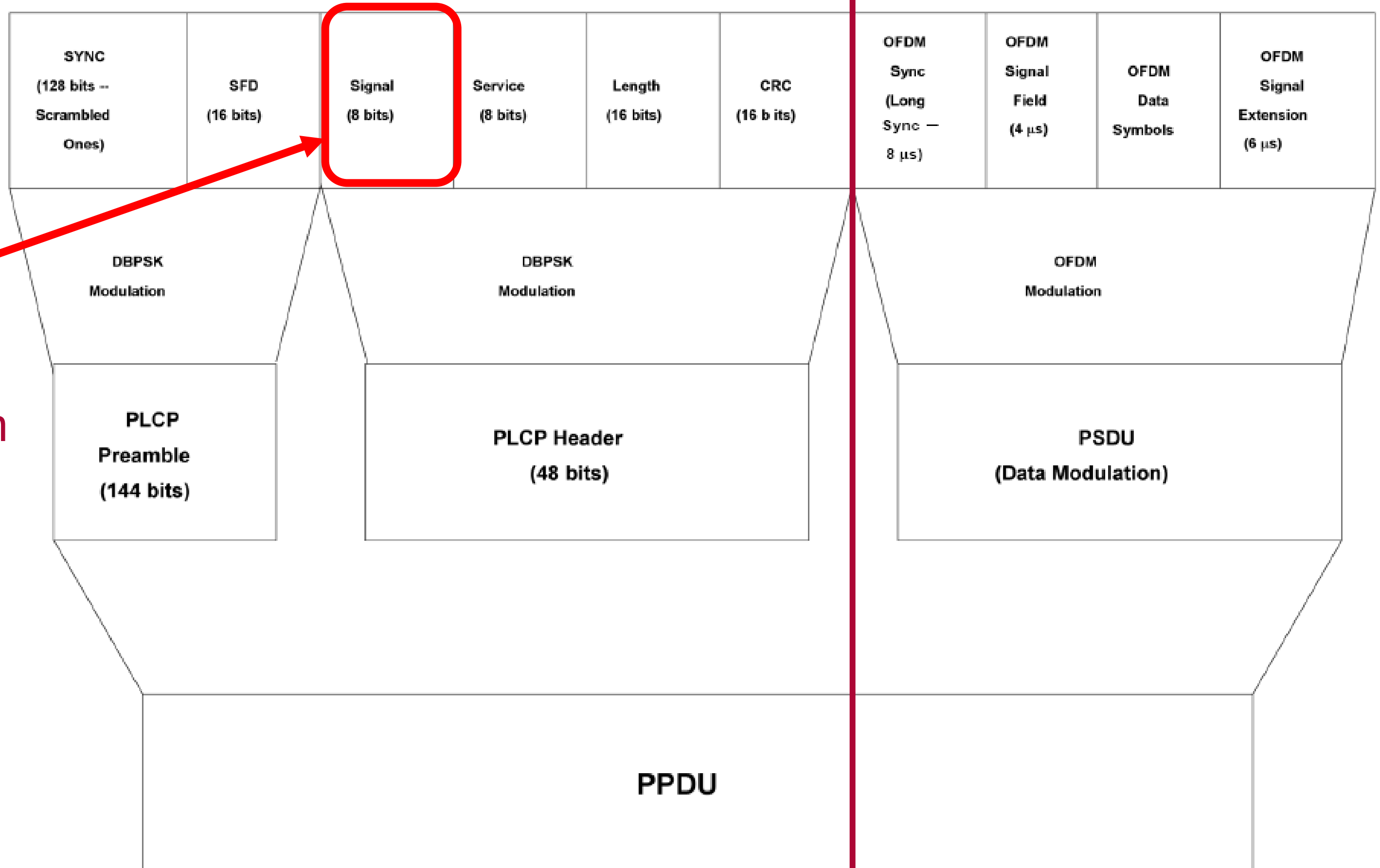
PLCP preamble + PLCP header: 96 µs

payload: 2, 5.5 or 11 Mbit/s



IEEE 802.11g, n **backwards compatible**, using same channels with different modulation.

Long preamble: modulation + data rates 802.11g



Source: Standard IEEE 802.11g-2003

Field <Signal> defines modulation and rate of PSDU

(PLCP PDU)

DBSK modulation = 1 Mbit/s

backwards compatibility

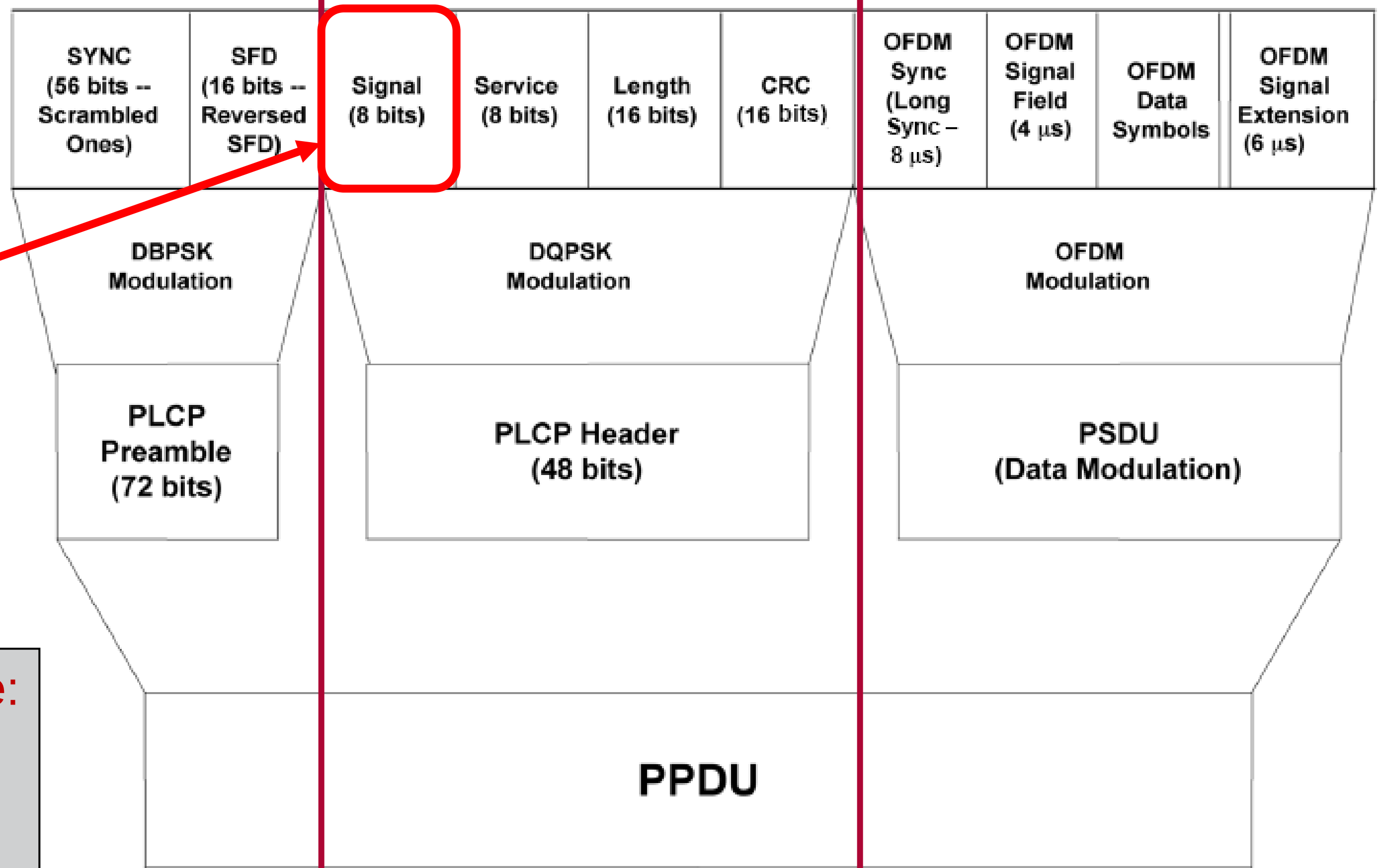
ERP Enhanced rate PHY using DSSS or OFDM

higher rates
5.5, 11, 22, 33 Mbit/s
6, 12, 24 Mbit/s
9, 18, 36, 48, 54 Mbit/s

PLCP =
Physical Layer
Convergence Protocol

(DBSK = Differential Binary Shift Keying)

Short preamble: modulation + data rates 802.11g



Field <Signal> defines modulation and rate of PSDU

Important message: Data rates differ between parts of PPDU

DBSK modulation = 1 Mbit/s

backwards compatibility

DQPSK modulation = 2 Mbit/s

backwards compatibility

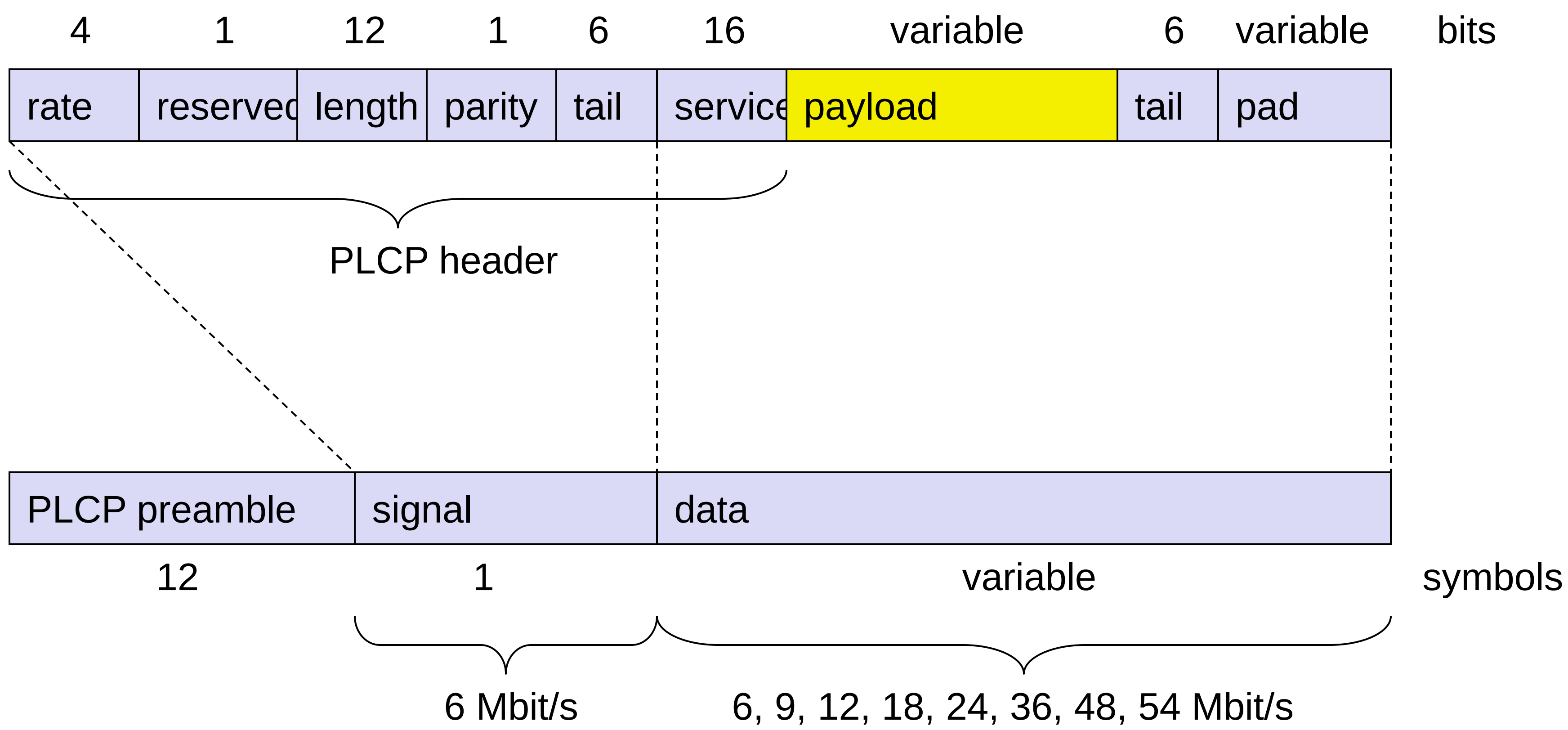
(DQPSK = Differential Quadrature Phase Shift Keying)

ERP Enhanced rate PHY using DSSS or OFDM

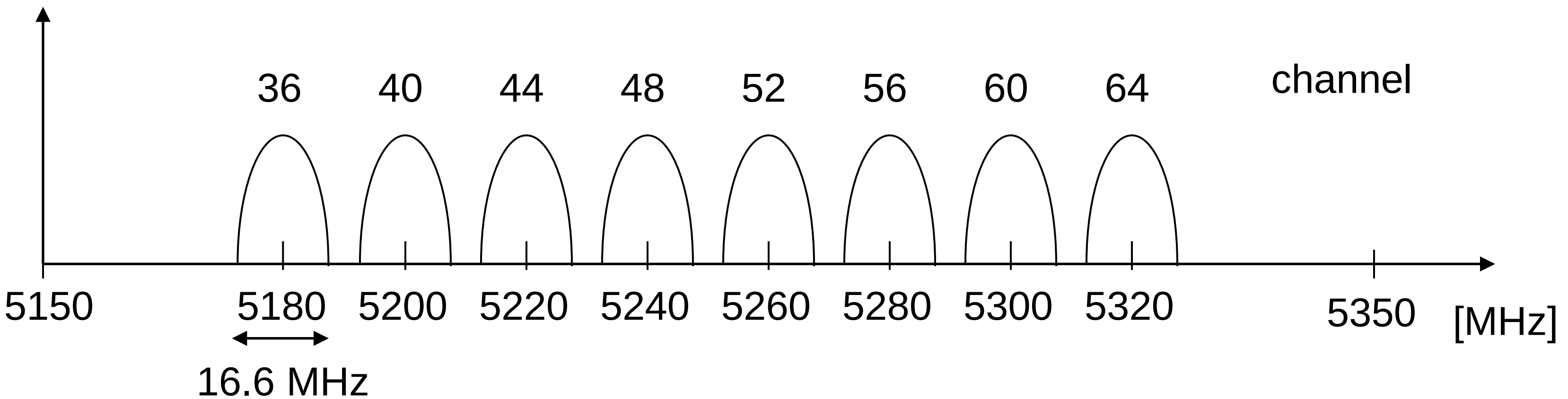
higher rates

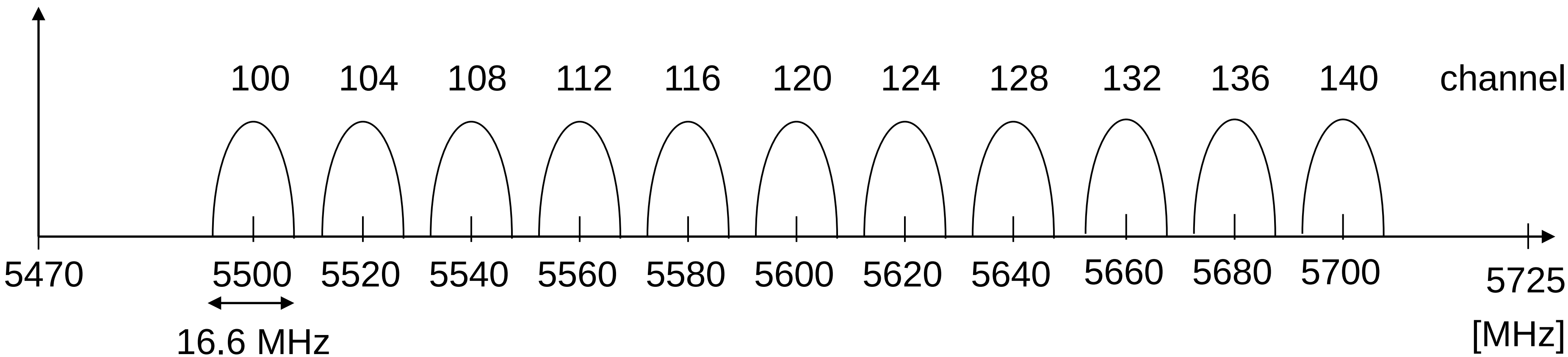
5.5, 11, 22, 33 Mbit/s
6, 12, 24 Mbit/s
9, 18, 36, 48, 54 Mbit/s

- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS


4
1
12
1
6
16
variable
6
variable
bits
rate
reserved
length
parity
tail
service
payload
tail
pad
PLCP header
PLCP preamble
signal
data
12
1
variable
symbols
6 Mbit/s
6, 9, 12, 18, 24, 36, 48, 54 Mbit/s

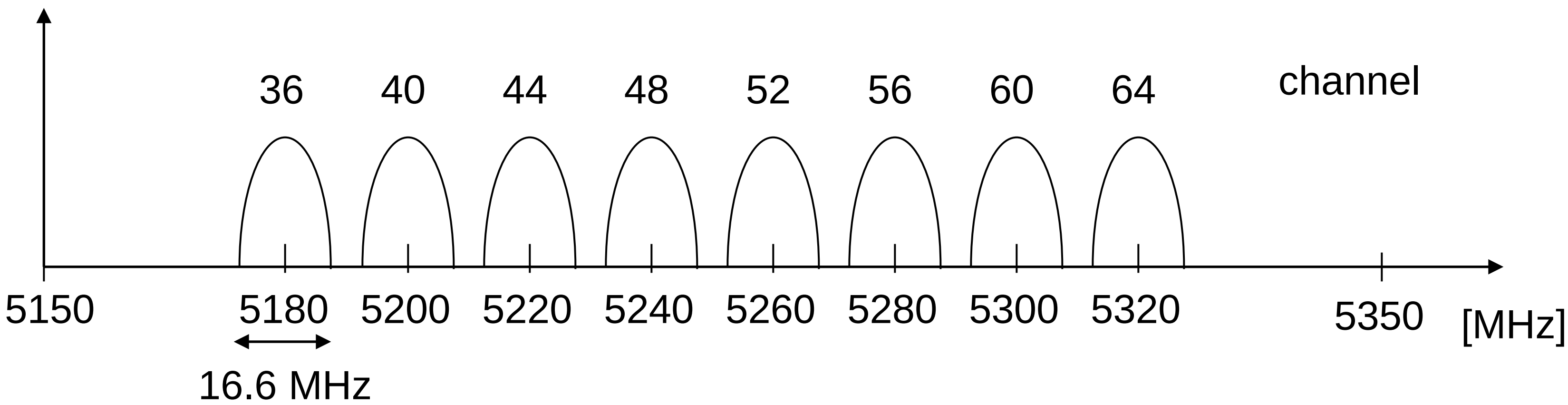
Operating channels of 802.11a in Europe

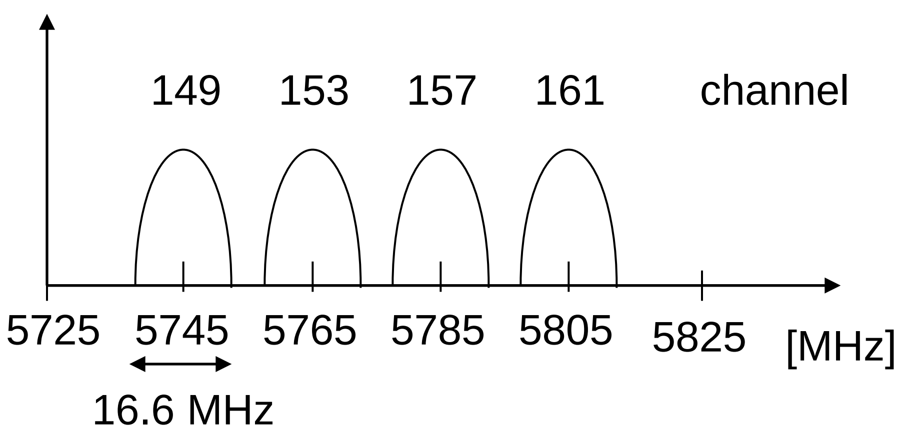




center frequency =
5000 + 5*channel number [MHz]

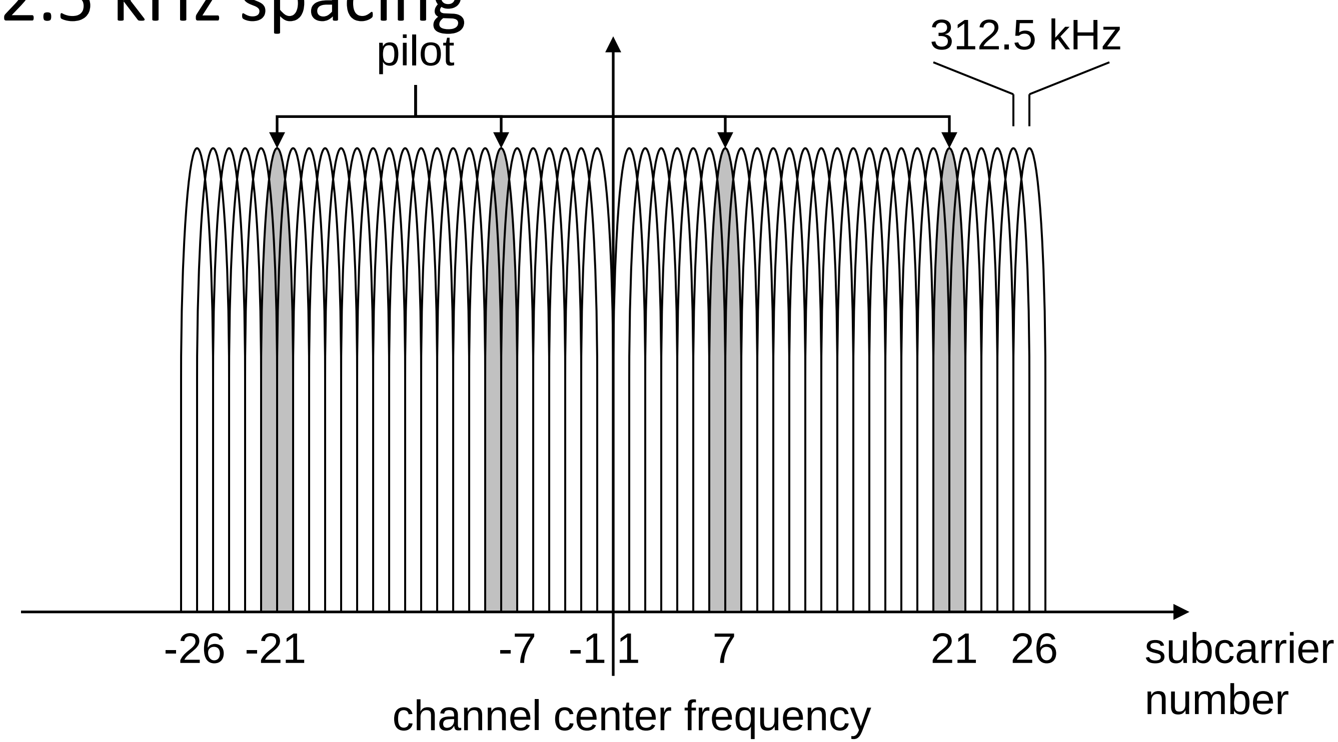
JS





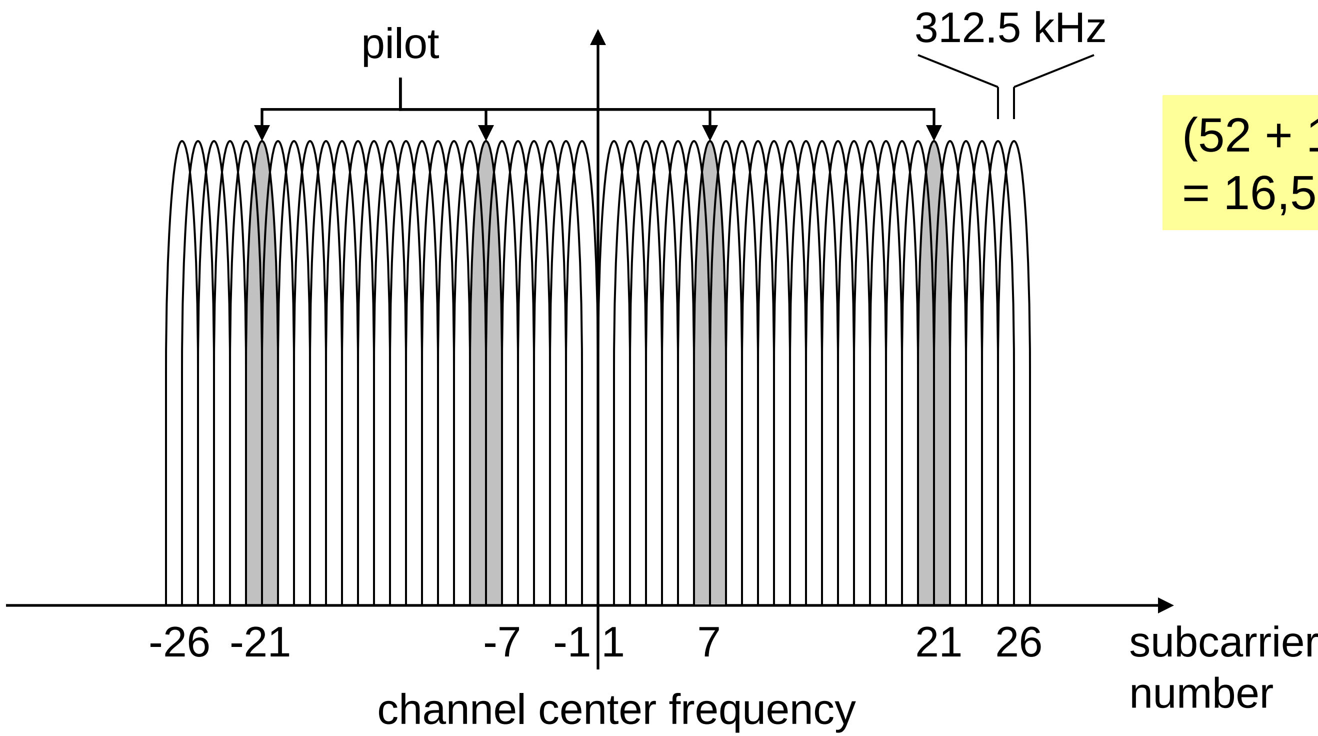
center frequency =
5000 + 5*channel number [MHz]

- OFDM with 52 used subcarriers (64 in total)
  - 48 data + 4 pilot
    - (plus 12 virtual subcarriers)
  - 312.5 kHz spacing



- OFDM with 52 used subcarriers (64 in total)
- 48 data + 4 pilot
- (plus 12 virtual subcarriers)
- 312.5 kHz spacing

64 * 312.5 kHz
= 20 MHz



(52 + 1) * 312.5 kHz
= 16,5625 MHz

- 802.11c: Bridge Support
  - Definition of MAC procedures to support bridges as extension to 802.1D
- 802.11d: Regulatory Domain Update
  - Support of additional regulations related to channel selection, hopping sequences
- **802.11e**: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
  - Definition of a data flow ("connection") with parameters like rate, burst, period… supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
  - Additional energy saving mechanisms and more efficient retransmission
  - EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access
- 802.11F: Inter-Access Point Protocol (withdrawn)
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
- **802.11g**: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
  - Successful successor of 802.11b, performance loss during mixed operation with .11b
- 802.11h: Spectrum Managed 802.11a
  - Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)
- 802.11i: Enhanced Security Mechanisms
  - Enhance the current 802.11 MAC to provide improvements in security.
  - TKIP enhances the insecure WEP, but remains compatible to older WEP systems
  - AES provides a secure encryption method and is based on new hardware

- 802.11j: Extensions for operations in Japan
  - Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- **802.11-2007**: Current “complete” standard
  - Comprises amendments a, b, d, e, g, h, i, j
- 802.11k: Methods for channel measurements
  - Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- 802.11m: Updates of the 802.11-2007 standard
- **802.11n**: Higher data rates above 100Mbit/s
  - Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
  - MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
  - However, still a large overhead due to protocol headers and inefficient mechanisms
- 802.11p: Inter car communications
  - Communication between cars/road side and cars/cars
  - Planned for relative speeds of min. 200km/h and ranges over 1000m
  - Usage of 5.850-5.925GHz band in North America
- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be feasible within 50ms in order to support multimedia applications efficiently

- 802.11s: Mesh Networking
  - Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
  - Support of point-to-point and broadcast communication across several hops
- 802.11T: Performance evaluation of 802.11 networks
  - Standardization of performance measurement schemes
- 802.11u: Interworking with additional external networks
- 802.11v: Network management
  - Extensions of current management functions, channel measurements
  - Definition of a unified interface
- 802.11w: Securing of network control
  - Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.
- 802.11y: Extensions for the 3650-3700 MHz band in the USA
- 802.11z: Extension to direct link setup
- 802.11aa: Robust audio/video stream transport
- **802.11ac**: Very High Throughput <6Ghz
- 802.11ad: Very High Throughput in 60 GHz
- 802.11af: TV white space, ah: sub 1GHz, ai: fast initial link set-up; … aq: pre-association discovery

- Note: Not all “standards” will end in products, many ideas get stuck at working group level
- Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

- quite new: developed from 2011 - 2013 and approved in January 2014,
- several devices available (based on draft versions)
- single link troughput > 500Mbit/s, multi-station > 1 Gbit/s
- Bandwidth up to 160 MHz (80 MHz mandatory), up to 8x MIMO, up to 256 QAM, beamforming, SDMA via MIMO
- Example home configuration:
  - 8-antenna access point, 160 MHz bandwidth, 6.77 Gbit/s
  - 4-antenna digital TV, 3.39 Gbit/s
  - 2-antenna tablet, 1.69 Gbit/s
  - two 1-antenna smartphones, 867 Mbit/s each

Comparison Ethernet - WLAN

	Ethernet	WLAN – “Wireless Ethernet”
CS	sense medium before sending	sense medium before sending
MA	all stations share the medium (cable)	all stations share the medium (radio frequency)
collisions (CD vs. CA)	collision detection (CD): physically detect collision, stop transmission, retry after random backoff	collision avoidance (CA): when medium getting free, wait for DIFS + random contention period collision is detected by ACKnowledgement mechanism
operation without collisions	full-duplex Ethernet	PCF – Point Coordination Function