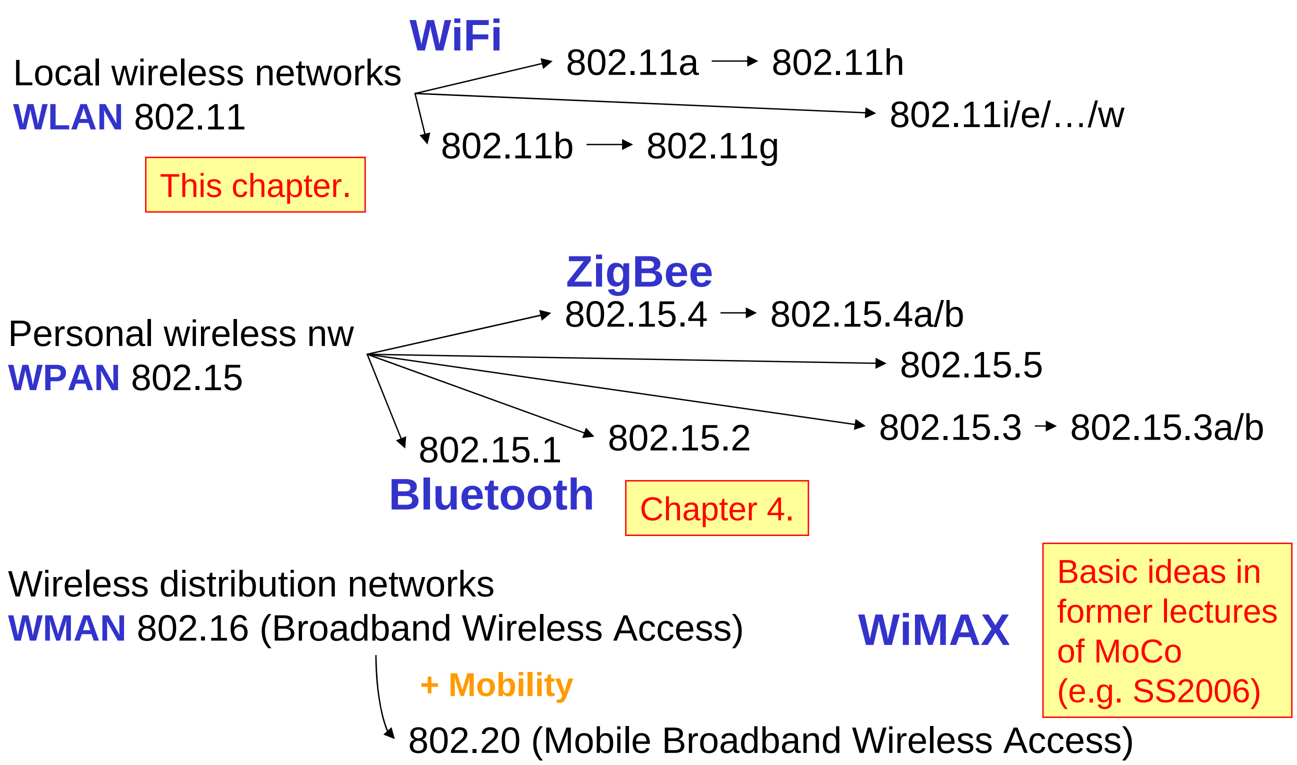
5. Wireless LAN (WLAN)

Wireless Local Area Networks (WLANs) provide **wireless connectivity for fixed, portable, and moving stations within a local area.**

In this section, we discuss the **most famous family of WLANs: IEEE 802.11.**

5.1. Mobile Communication Technology in IEEE 802

JS



IEEE 802.11 Standards Family

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 Task Group (**Work in progress**)

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

Current Standards Activities at 802.11 (PHY)

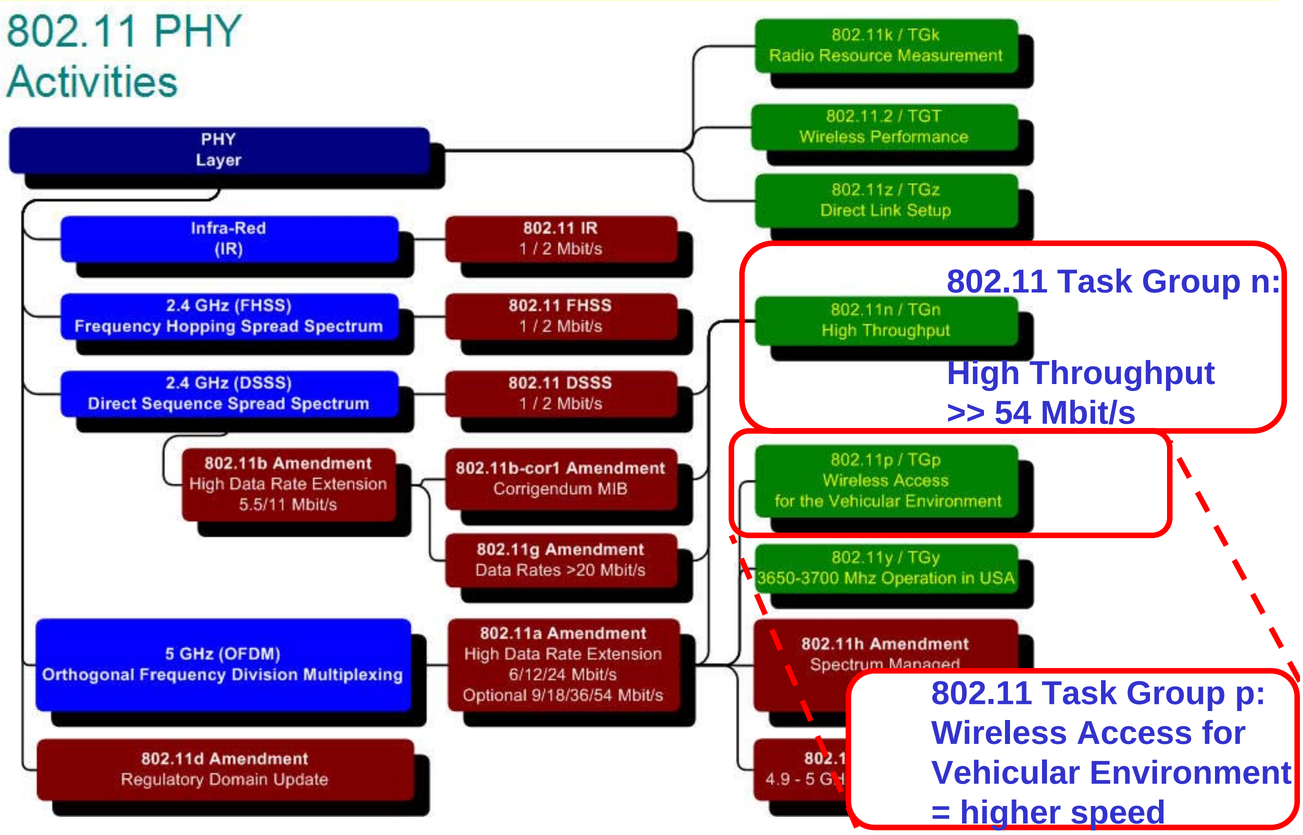


Fig. source and further info see http://www.ieee802.org/11/ (WG-Info / Activities Graphic)
(as of 16.05.2008)

Current Standards Activities at 802.11 (MAC & Others)

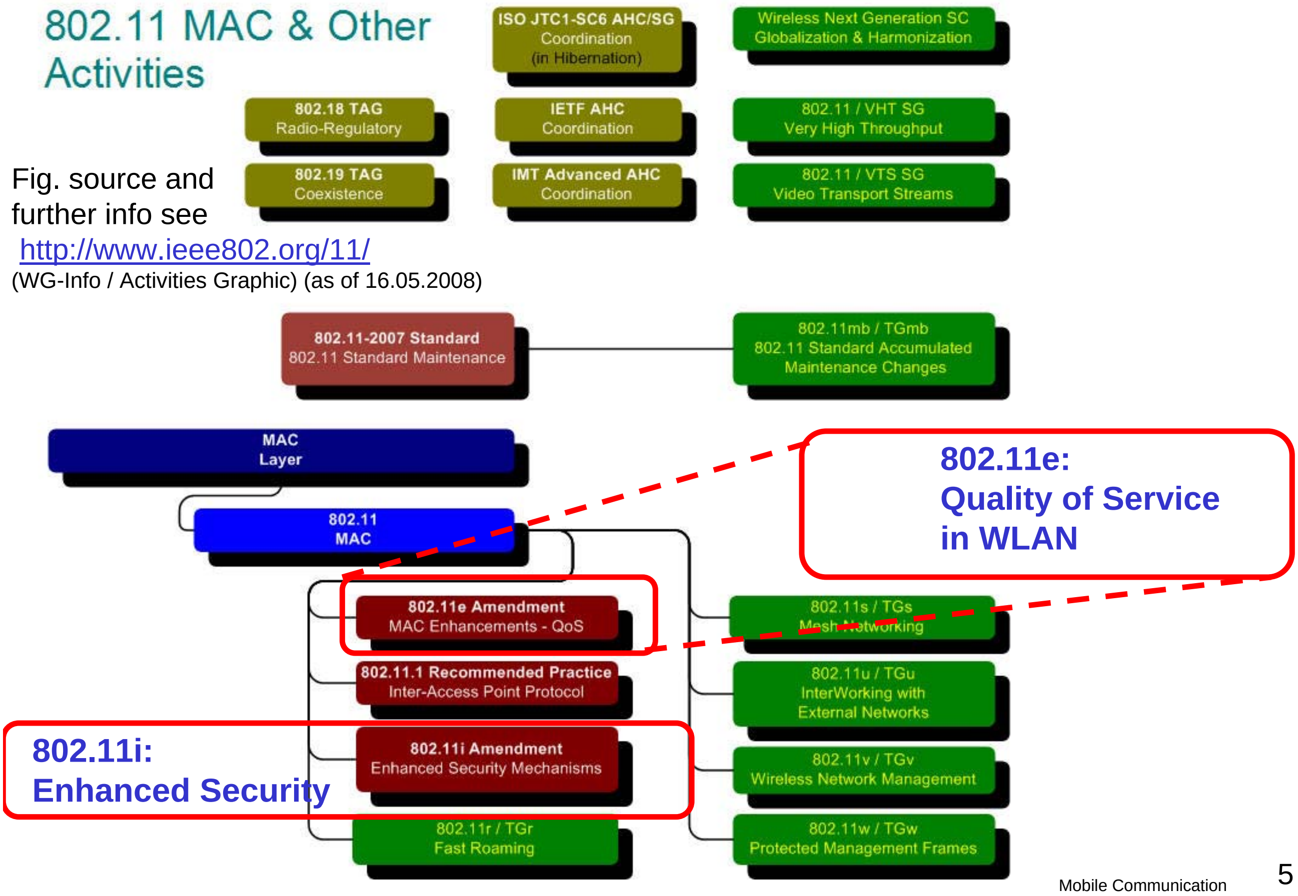


Fig. source and further info see
http://www.ieee802.org/11/
(WG-Info / Activities Graphic) (as of 16.05.2008)

Scope and purpose of IEEE 802.11

Scope
The scope of this standard is to develop a medium access control (MAC) and physical layer (PHY) specification for **wireless connectivity for fixed, portable, and moving stations within a local area.**

Purpose
The purpose of this standard is to provide **wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment**, which may be **portable or hand-held, or which may be mounted on moving vehicles within a local area.** This standard also offers regulatory bodies a means of standardizing access to one or more frequency bands for the purpose of local area communication.

Specifically, this standard

- Describes the functions and services required by an IEEE 802.11 compliant device to operate within **ad hoc and infrastructure networks as well as the aspects of station mobility (transition) within those networks.**
- Defines the MAC procedures to support the **asynchronous MAC service** data unit (MSDU) delivery services.
- Defines **several PHY signaling techniques and interface functions** that are controlled by the IEEE 802.11 MAC.
- Permits the operation of an IEEE 802.11 conformant device within a wireless local area network (LAN) that may **coexist with multiple overlapping IEEE 802.11 wireless LANs**.
- Describes the requirements and procedures to provide **privacy** of user information being transferred over the wireless medium (WM) and **authentication** of IEEE 802.11 conformant devices.

Source: IEEE Std. 802.11 - 1997, p. 1

Abbreviations and acronyms

4. Abbreviations and acronyms

ACK	acknowledgment
AID	association identifier
AP	access point
ATIM	announcement traffic indication message
BSA	basic service area
BSS	basic service set
BSSID	basic service set identification
CCA	clear channel assessment
CF	contention free
CFP	contention-free period
CID	connection identifier
CP	contention period
CRC	cyclic redundancy code
CS	carrier sense
CTS	clear to send
CW	contention window
DA	destination address
DBPSK	differential binary phase shift keying
DCE	data communication equipment
DCF	distributed coordination function
DCLA	direct current level adjustment
DIFS	distributed (coordination function) interframe space
DLL	data link layer
Dp	desensitization
DQPSK	differential quadrature phase shift keying
DS	distribution system
DSAP	destination service access point
DSM	distribution system medium
DSS	distribution system service
DSSS	direct sequence spread spectrum
DTIM	delivery traffic indication message
ED	energy detection
EIFS	extended interframe space
EIRP	equivalent isotropically radiated power
ERS	extended rate set
ESA	extended service area
ESS	extended service set
FC	frame control
FCS	frame check sequence
FER	frame error ratio
FH	frequency hopping
FHSS	frequency-hopping spread spectrum
FIFO	first in first out
GFSK	Gaussian frequency shift keying
IBSS	independent basic service set
ICV	integrity check value
IDU	interface data unit
IFS	interframe space
IMp	intermodulation protection
IR	infrared
ISM	industrial, scientific, and medical
IV	initialization vector
LAN	local area network
LLC	logical link control
LME	layer management entity
LRC	long retry count
lsb	least significant bit
MAC	medium access control
MDF	management-defined field
MIB	management information base
MLME	MAC sublayer management entity
MMPDU	MAC management protocol data unit
MPDU	MAC protocol data unit
msb	most significant bit
MSDU	MAC service data unit
N/A	not applicable
NAV	network allocation vector
PC	point coordinator
PCF	point coordination function
PDU	protocol data unit
PHY	physical (layer)
PHY-SAP	physical layer service access point
PIFS	point (coordination function) interframe space
PLCP	physical layer convergence protocol
PLME	physical layer management entity
PMD	physical medium dependent
PMD-SAP	physical medium dependent service access point
PN	pseudo-noise (code sequence)
PPDU	PLCP protocol data unit
ppm	parts per million
PPM	pulse position modulation
PRNG	pseudo-random number generator

Source: IEEE Std. 802.11 - 1999

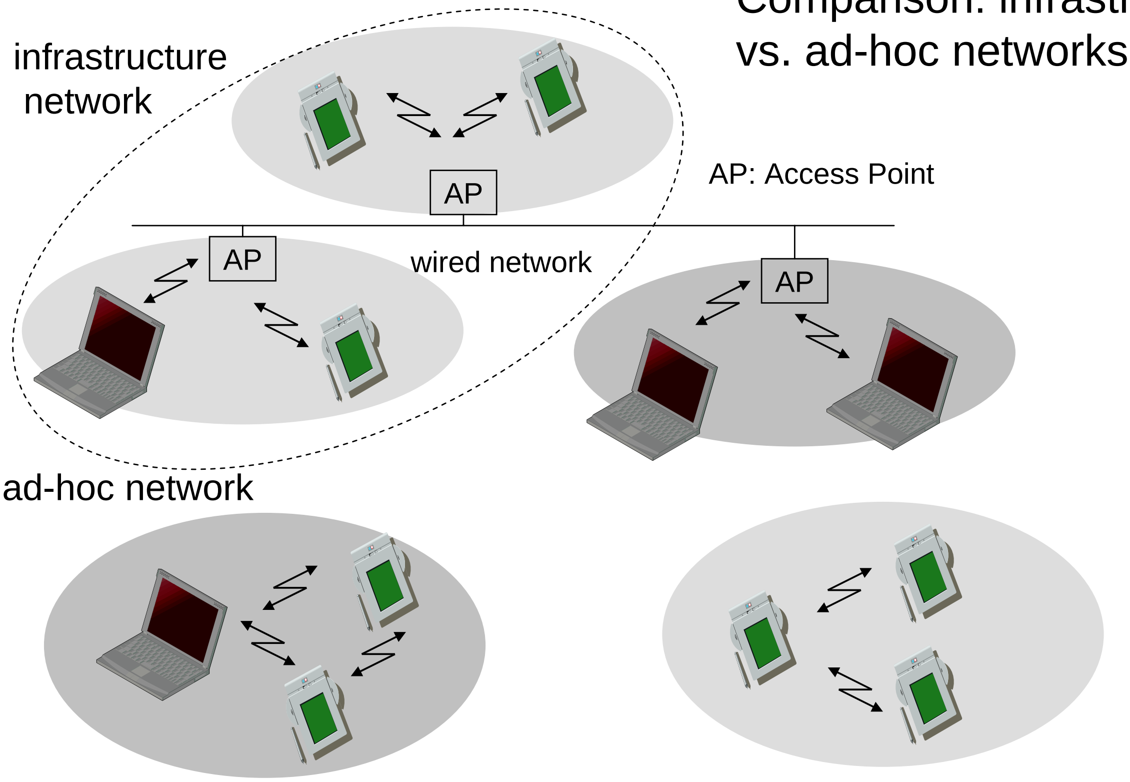
Abbreviations and acronyms (2)

PS	power save (mode)
PSDU	PLCP SDU
RA	receiver address
RF	radio frequency
RSSI	received signal strength indication
RTS	request to send
RX	receive or receiver
SA	source address
SAP	service access point
SDU	service data unit
SFD	start frame delimiter
SIFS	short interframe space
SLRC	station long retry count
SME	station management entity
SMT	station management
SQ	signal quality (PN code correlation strength)
SRC	short retry count
SS	station service
SSAP	source service access point
SSID	service set identifier
SSRC	station short retry count
STA	station
TA	transmitter address
TBTT	target beacon transmission time
TIM	traffic indication map
TSF	timing synchronization function
TU	time unit
TX	transmit or transmitter
TXE	transmit enable
UCT	unconditional transition
WAN	wide area network
WDM	wireless distribution media
WDS	wireless distribution system
WEP	wired equivalent privacy
WM	wireless medium

5.2. Components of the IEEE 802.11 architecture

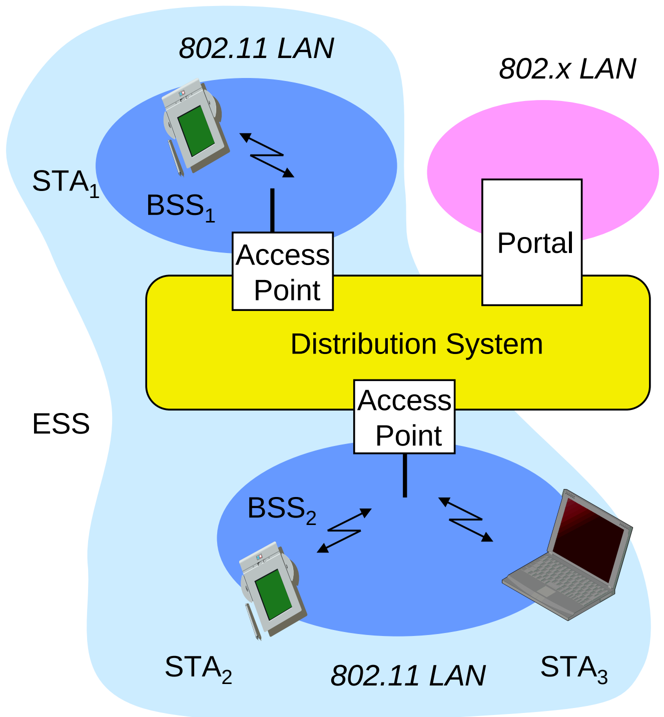
JS

Comparison: infrastructure vs. ad-hoc networks



802.11 - Architecture of an infrastructure network

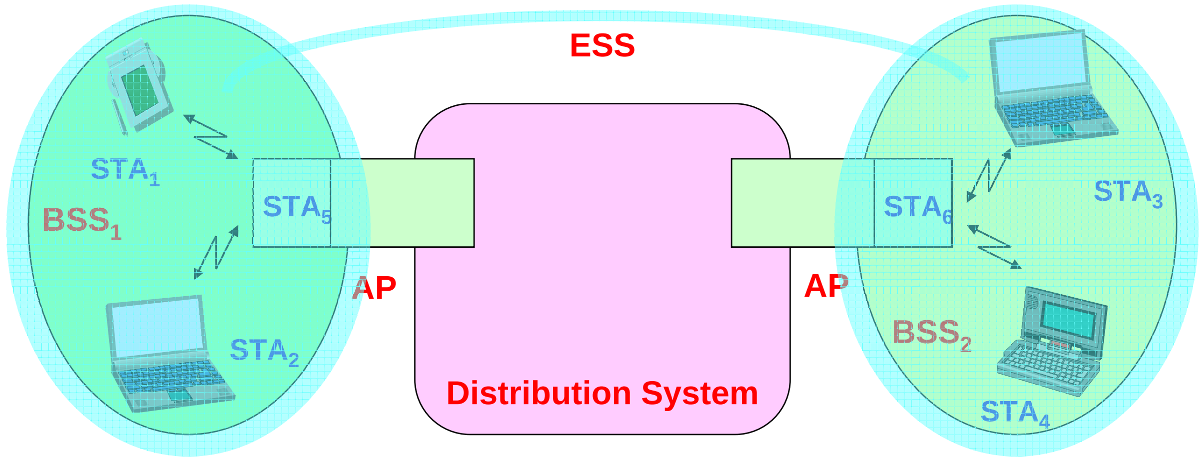
JS



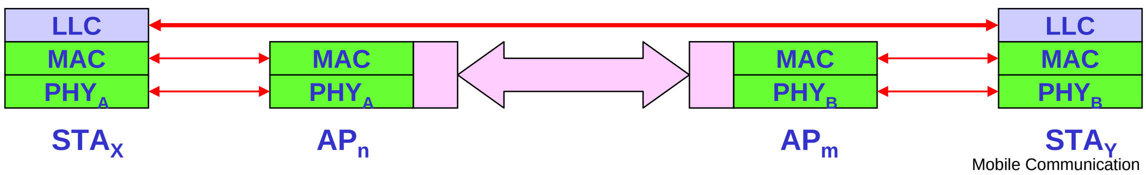
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to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

Extended service set

DS and BSSs allow IEEE 802.11 to create a **wireless network of arbitrary size and complexity**: An **extended service set (ESS)** network.

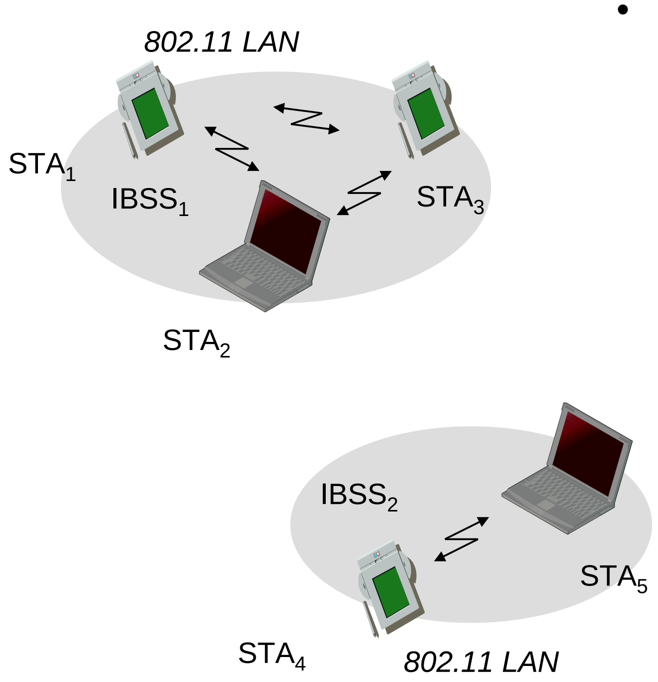


The key concept is that **the ESS network appears the same to an LLC layer as an IBSS network**. Stations within an ESS may communicate and mobile stations may move from one BSS to another (within the same ESS) **transparently to LLC.**



802.11 - Architecture of an ad-hoc network

JS



- 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

5.3. The services specified in IEEE 802.11

There are nine services specified by IEEE 802.11:

- **six services** to support **MSDU delivery between STAs**.
- **three services** to control IEEE 802.11 LAN **access and confidentiality**.

Each of the services is supported by **one or more MAC frame types**.

Some of the services are supported by MAC management messages and some by MAC data messages. All of the messages gain access to the wireless medium via the IEEE 802.11 MAC sublayer medium access method.

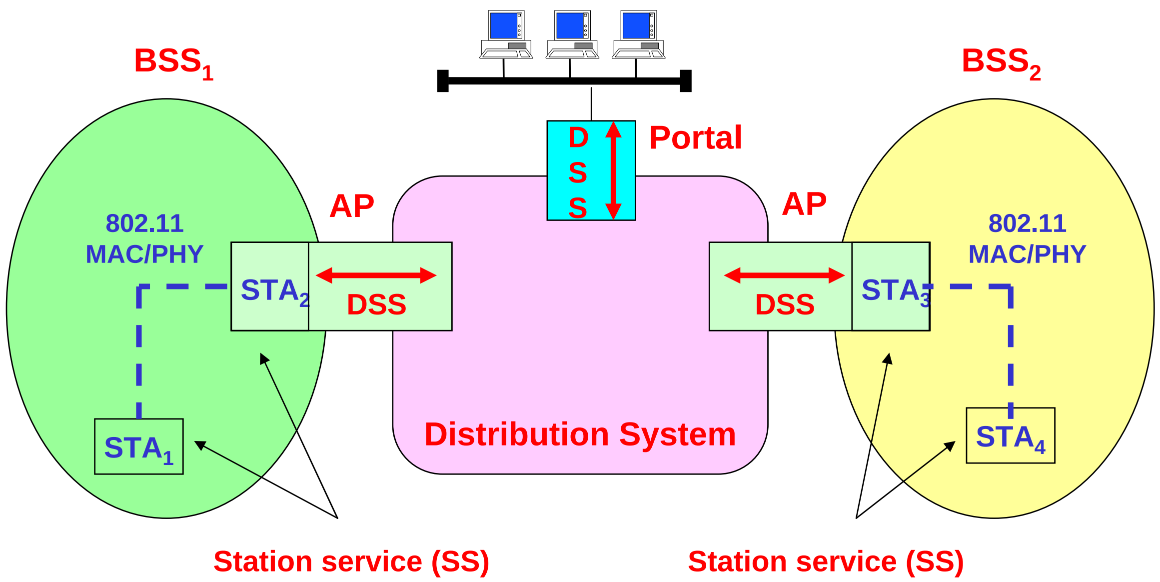
Example first
(Some) **details** afterwards (short)

5.3.1. Categories of service

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) and distribution system service (DSS)

Station service (SS)

The SSs are as follows:
a) **Authentication**
b) **Deauthentication**
c) **Privacy**
d) **MSDU delivery**

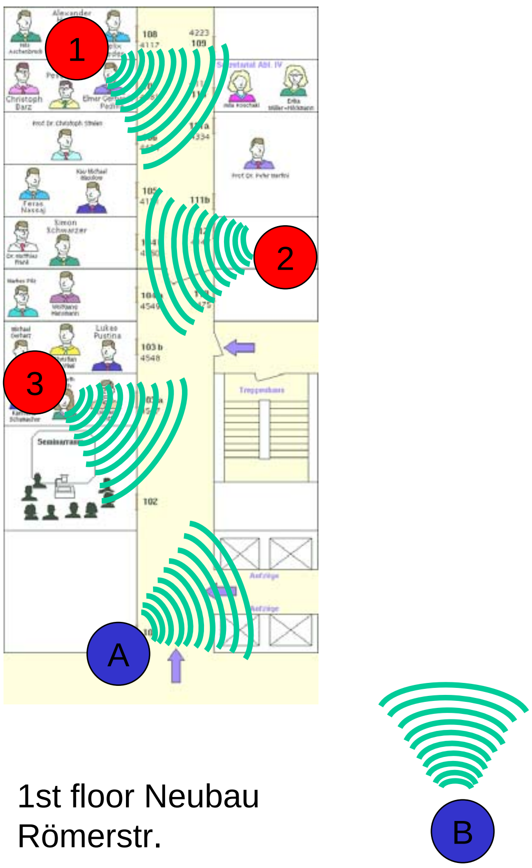
- The SS is **present in every IEEE 802.11 station** (including APs, as APs include station functionality).
- All conformant stations provide SS.

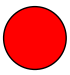
Distribution system service (DSS)

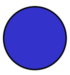
The DSSs are as follows:
a) **Association**
b) **Disassociation**
c) **Distribution**
d) **Integration**
e) **Reassociation**

- 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.

5.3.2. Example of SS/DSS services – with moving device



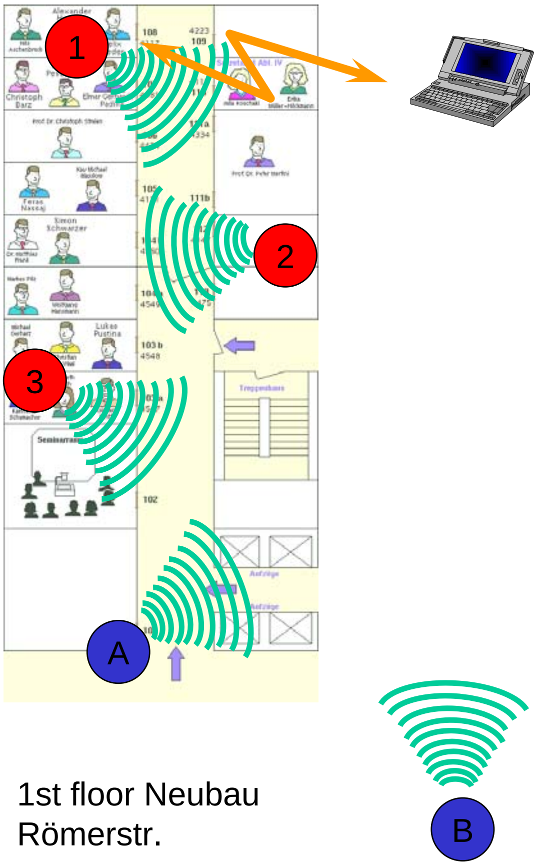

„private“ WLAN of research group Martini


public WLAN of Uni Bonn SSID „bonnet“

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

1st floor Neubau Römerstr.

Example of SS/DSS services – with moving device



Station service:

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

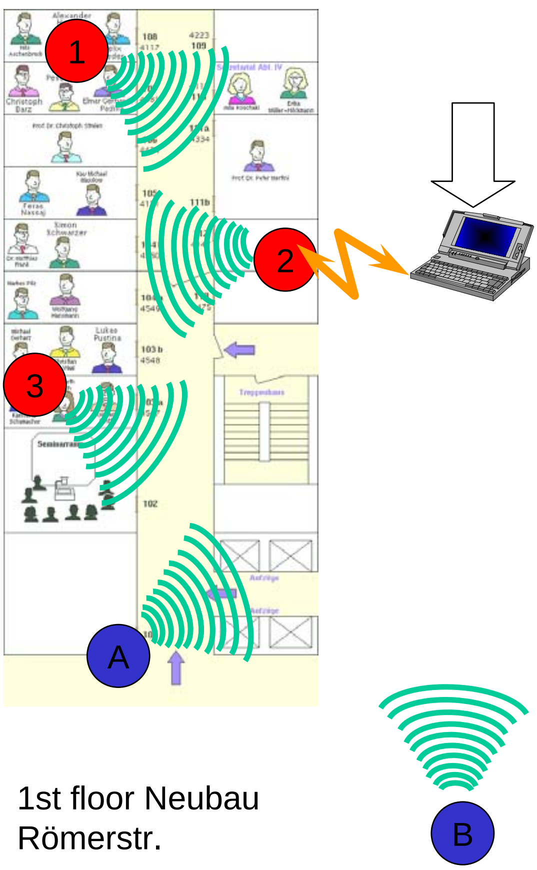
Distribution system service:

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



Movement within ESS = BSS-transition

Station service:

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

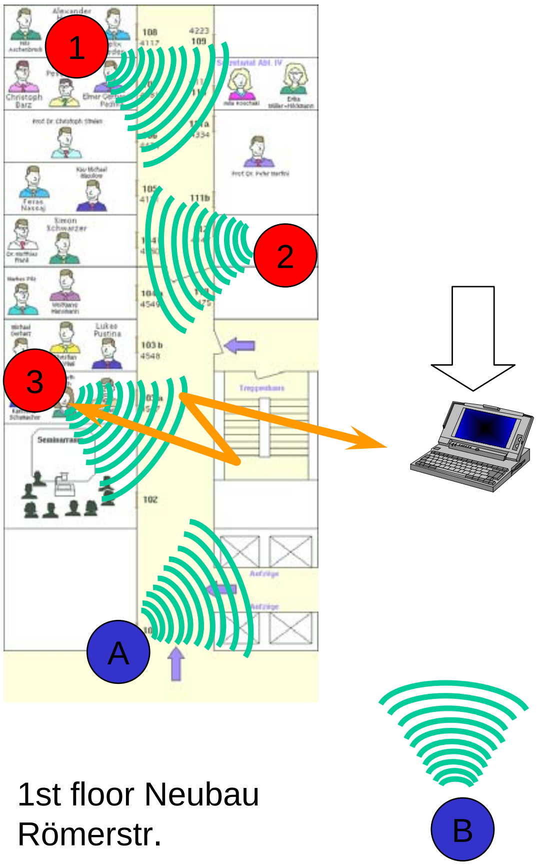
Distribution system service:

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!

1st floor Neubau Römerstr.

Example of SS/DSS services – with moving device



Movement within ESS = BSS-transition

Station service:

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

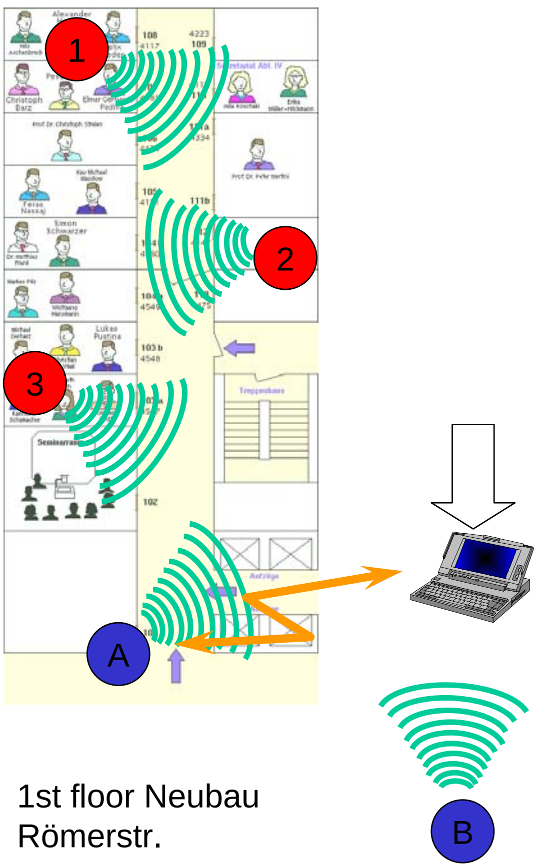
Distribution system service:

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

1st floor Neubau Römerstr.

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



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:

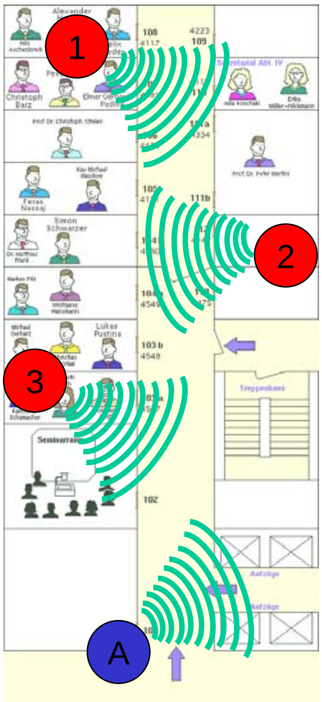
1. (possibly) disassocation – with AP 3 before leaving
2. association – with AP A
3. distribution – with devices within ESS

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

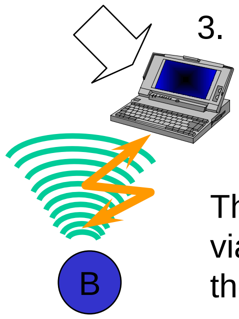
1st floor Neubau Römerstr.

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)

Example of SS/DSS services – with moving device



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:

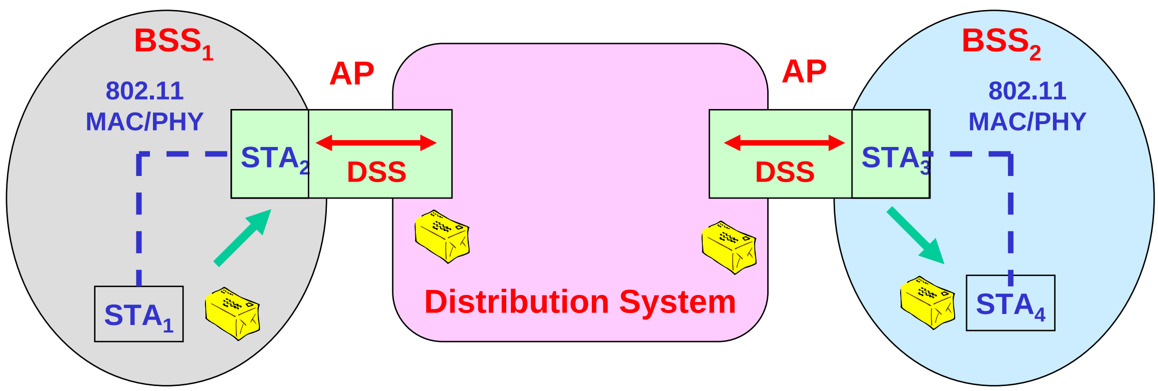
1. re-association – with AP B
2. distribution – with devices within ESS
3. integration via portal/gateway
   VPN connection still active

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)

5.3.3. Distribution (a DSS)

The distribution service

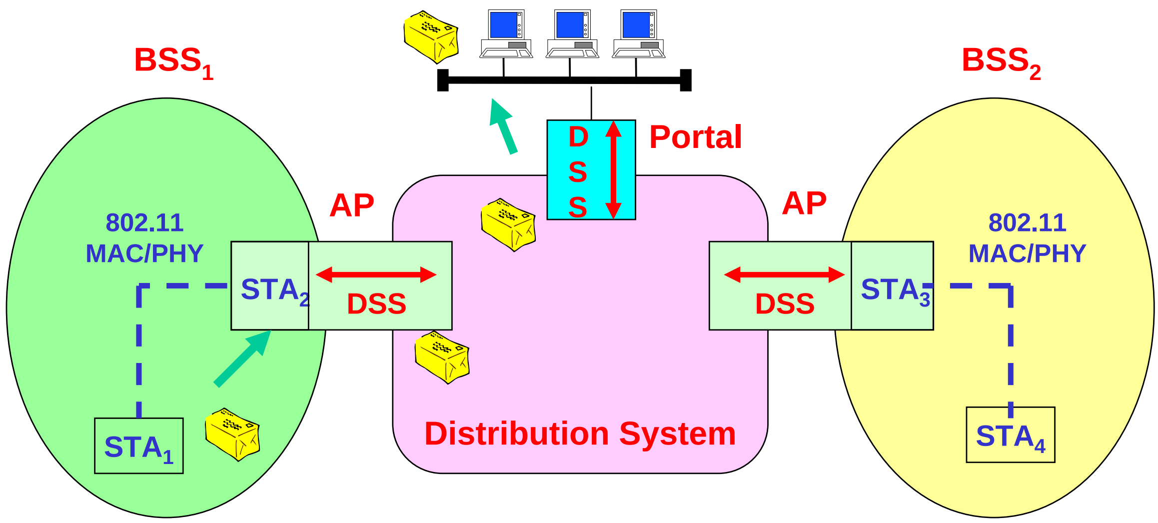
- is conceptually **invoked by every data message** to or from an IEEE 802.11 STA operating in an ESS (when the frame is sent via the DS),
- **delivers the message within the DS** in such a way that it **arrives at the appropriate DS destination** for the intended recipient
- is **based on** information provided to the DS by **the three association related services** (association, reassociation, and disassociation).



How the message is distributed within the DS is not specified by IEEE 802.11 !

5.3.4. Integration (a DSS)

If the distribution service DS determines that the **"output" point of the DS is a portal** instead of an AP, the **DS invokes the Integration function**.
The Integration function does whatever is needed to **deliver a message** from the DS medium **to the integrated LAN** medium (eg. media or address space translations).

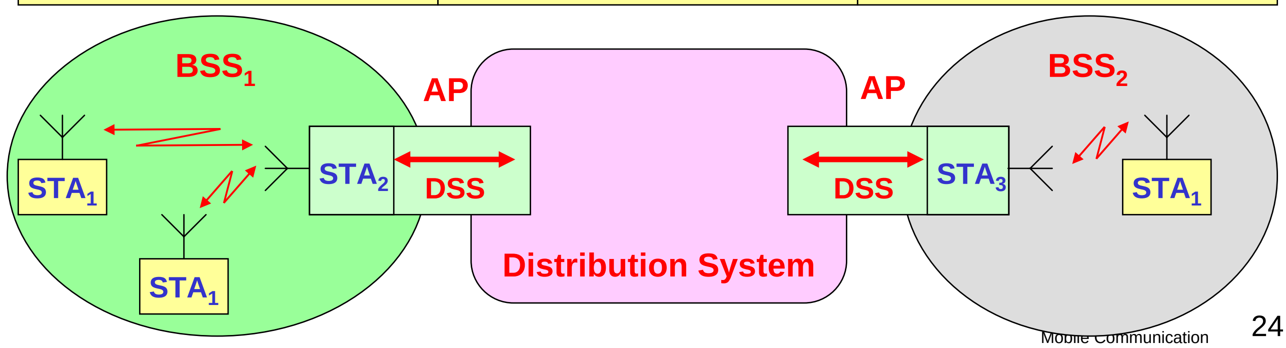


Messages received from an integrated LAN (via a portal) by the DS for an IEEE 802.11 STA will **invoke the Integration function** before the message is distributed by the distribution service.

5.3.5. Services supporting the distribution service

Before a data message can be handled by the distribution service, a STA shall be "**associated**". Different association services support different categories of mobility.

Mobility types:		
No-transition:	**BSS-transition**:	**ESS-transition**:
• **Static – no motion** • **Local movement** movement within the PHY range of the communicating STAs [i.e., movement within a basic service area (BSA)].	station movement • **from one BSS** in one ESS • **to another BSS within the same ESS**.	station movement • **from one BSS** in one ESS • **to a BSS in a different ESS**. This case is supported only in the sense that the STA may move. Maintenance of upper-layer connections cannot be guaranteed by IEEE 802.11; in fact, disruption of service is likely to occur.



Association (a DSS)

A **STA**

- first **learns about** what **APs** are present (scanning),
- then **requests to establish an association** (by invoking the association service),
- then is **allowed to send data messages via this AP,**
- **may be associated with no more than one AP** at a given instant,
  This ensures that the DS may determine a unique answer to the question, “which AP is serving STA X?”
- may be **one of many STAs associated with the same AP.**

How the information provided by the association service is **stored and managed** within the DS is **not specified** by IEEE 802.11.

Association is **always initiated by the mobile STA**, not the AP.

Reassociation (a DSS) and disassociation (a DSS)

Reassociation:
The reassociation service is **invoked to “move” a current association from one AP to another.** This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP. **Reassociation is always initiated by the mobile STA.**

Disassociation
The disassociation service is invoked whenever an existing association is to be terminated. In an ESS, this tells the DS to void existing association information. Attempts to send messages via the DS to a disassociated STA will be unsuccessful. The disassociation service may be invoked by either party to an association (non-AP STA or AP). **Disassociation is a notification, not a request.**

APs may need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons. STAs shall attempt to disassociate whenever they leave a network. However, the MAC protocol does not depend on STAs invoking the disassociation service. (MAC management is designed to accommodate loss of an associated STA.)

Access and confidentiality control services

Wired LAN design assumes the physically closed and controlled nature of wired media. The physically open medium nature of an IEEE 802.11 LAN violates those assumptions. Two services are provided to bring the IEEE 802.11 functionality in line with wired LAN assumptions; authentication and privacy.

Authentication (an SS)
IEEE 802.11 provides the ability to control LAN access via the authentication service. This service is used by all stations to establish their identity to stations with which they will communicate. IEEE 802.11 supports **several authentication processes**. **IEEE 802.11 requires mutually acceptable, successful, authentication.** A STA may be authenticated with many other STAs at any given instant.

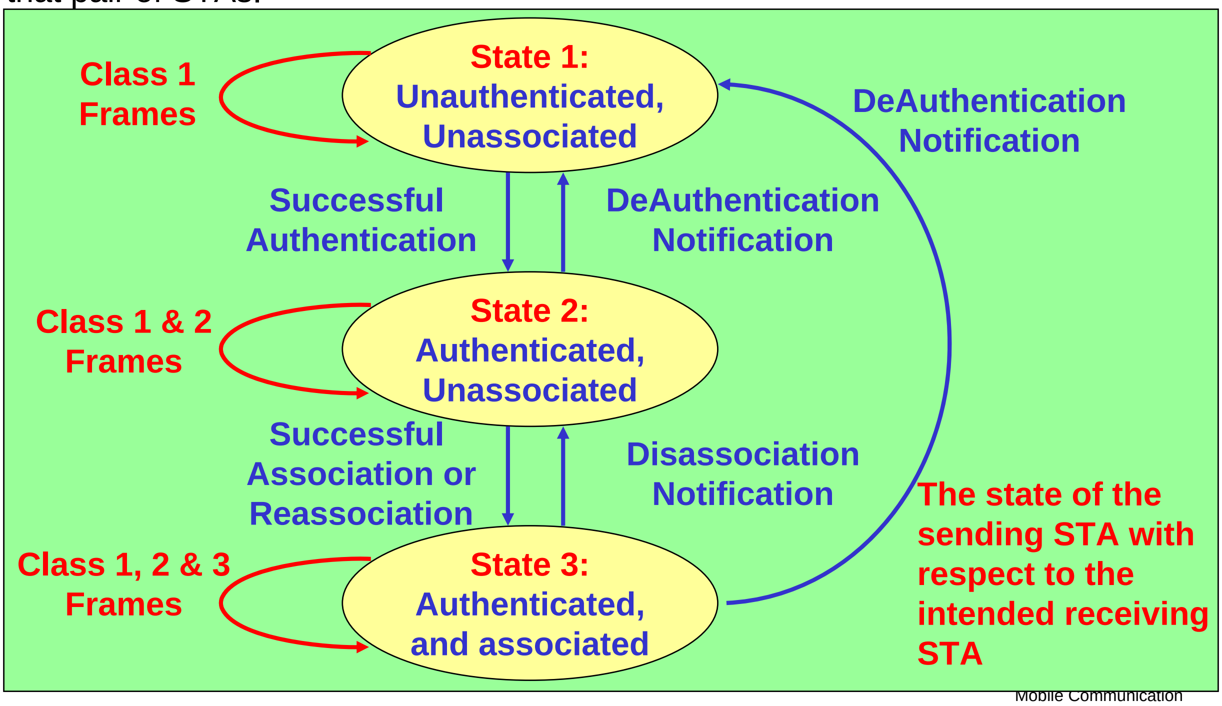
Deauthentication (an SS)
The deauthentication service is invoked whenever an **existing authentication is to be terminated.** In an ESS, since authentication is a prerequisite for association, the act of deauthentication shall cause the station to be disassociated. The deauthentication service may be invoked by either authenticated party (non-AP STA or AP). **Deauthentication is not a request, it is a notification**.

Privacy (an SS)
Any IEEE 802.11-compliant STA may hear all like-PHY IEEE 802.11 traffic that is within range. To bring the functionality of the wireless LAN up to the level implicit in wired LAN design, IEEE 802.11 provides the ability to **encrypt the contents of messages.**

5.3.6. Relationships between services

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

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

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

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

1) Management frames:

- 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

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**

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.

5.4. MAC sublayer functional description

5.4.1. Motivation

JS

Why not simply use protocols from the wired world ?

How about CSMA/CD ?

- **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
- send as soon as the medium is free, listen into the medium whether a collision occurs (original method in IEEE 802.3)

Problems in wireless networks

- **signal strength decreases** proportional to the square of the distance
- the **sender would apply CS and CD**, but the **collisions happen at the receiver**
- it **might be** the case that a sender cannot "hear" the collision, i.e., **CD does not work**
- furthermore, **CS might not work** if, e.g., a terminal is "hidden"

=> cf. subsection 3. Wireless Communication Basics

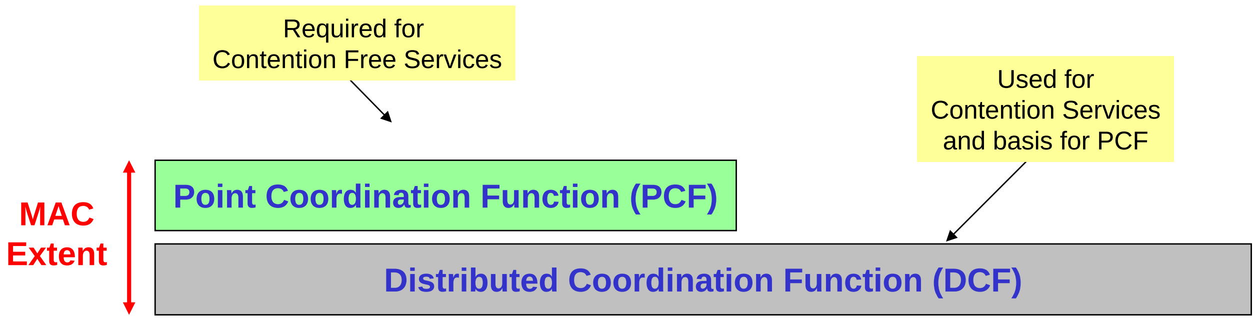
5.4.2. IEEE 802.11 MAC Architecture

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



Services and access methods

JS

Traffic services

- **Asynchronous Data Service (mandatory)**
  - exchange of data packets based on "best-effort"
  - support of broadcast and multicast
- **Time-Bounded Service (optional)**
  - implemented using PCF (Point Coordination Function)

Access methods

- **DCF CSMA/CA (mandatory)**
  - collision avoidance via randomized „back-off" mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- **DCF w/ RTS/CTS (optional)**
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- **MAC- PCF (optional)**
  - access point polls terminals according to a list

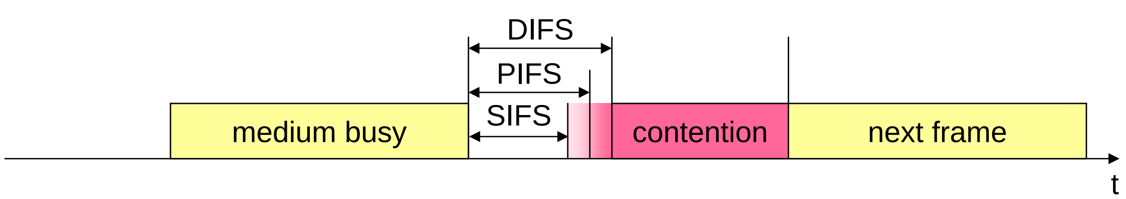
5.4.3. The distributed coordination function (DCF)

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.

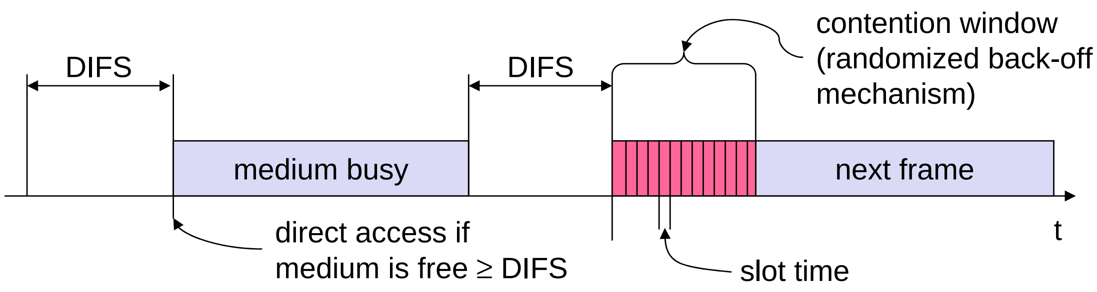
IEEE 802.11 defines **access priorities through different inter frame spaces:**

- **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



CSMA/CA, mandatory

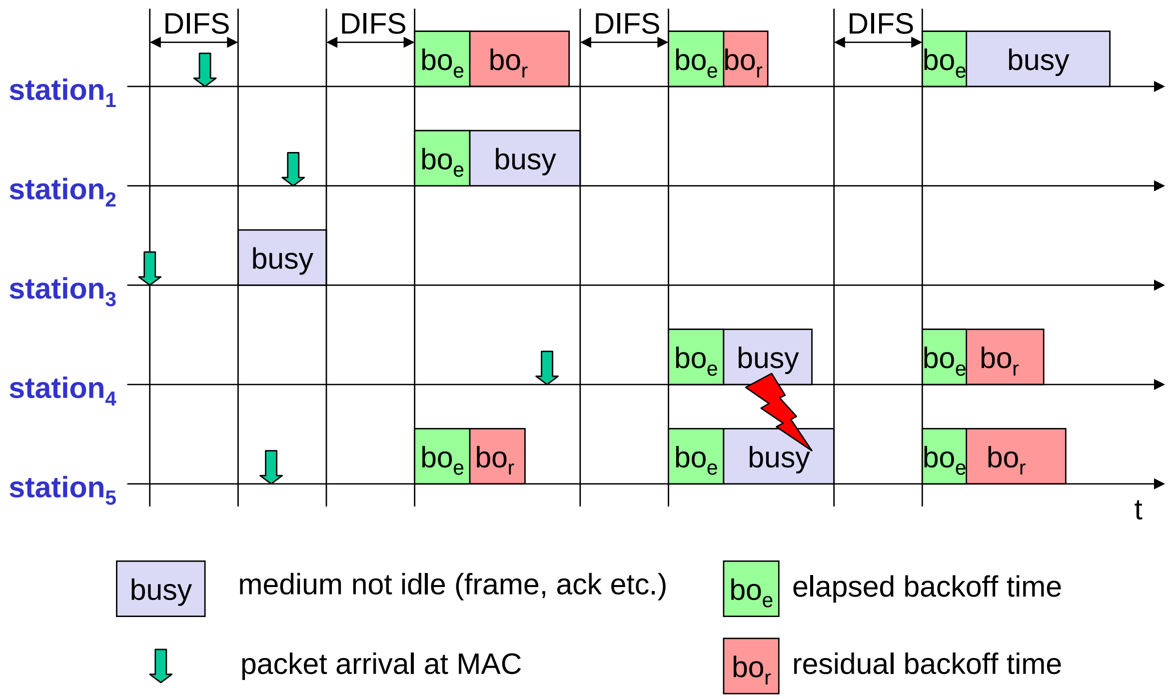
JS



- 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

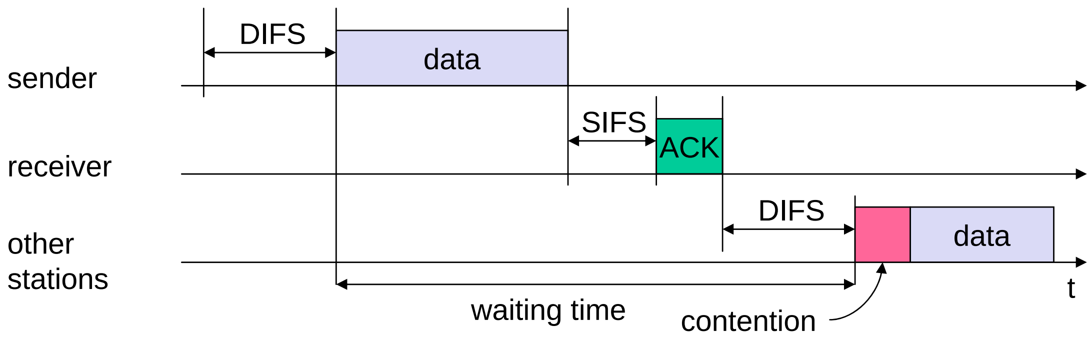
JS



Acknowledgements

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.**

Fragmentation / defragmentation

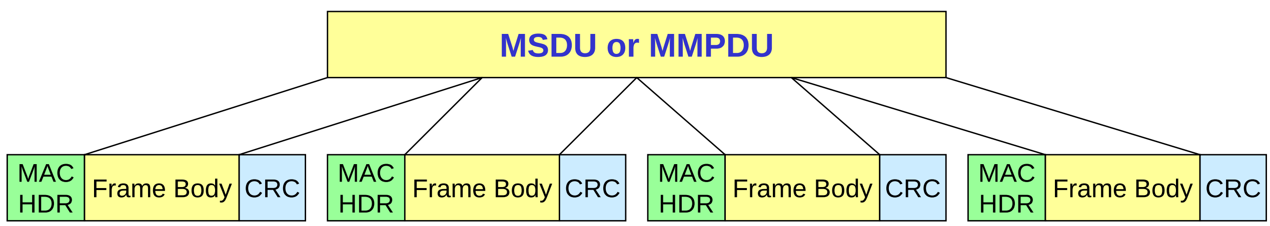
In WLANs, **bit error rates** typically are **much higher** than in conventional LANs.

Fragmentation

- **of MSDUs** (MAC service data units, from/to LLC) or
- **of MMPDUs** (MAC management protocol data units)
- **into smaller MPDUs** (MAC protocol data units),

increases reliability, by increasing the probability of successful transmission in cases **where channel characteristics limit reception reliability for longer frames.**

IEEE 802.11 **fragmentation** is accomplished **at each immediate transmitter**.
Similarly, **defragmentation** is accomplished **at each immediate recipient**.
Only MPDUs with a unicast receiver address shall be fragmented.



Fragmentation / defragmention (2)

The MPDUs resulting from the fragmentation are sent as **independent transmissions**, **each** of which is **separately acknowledged**.

This permits **retransmissions per fragment**, rather than per MSDU or MMPDU.

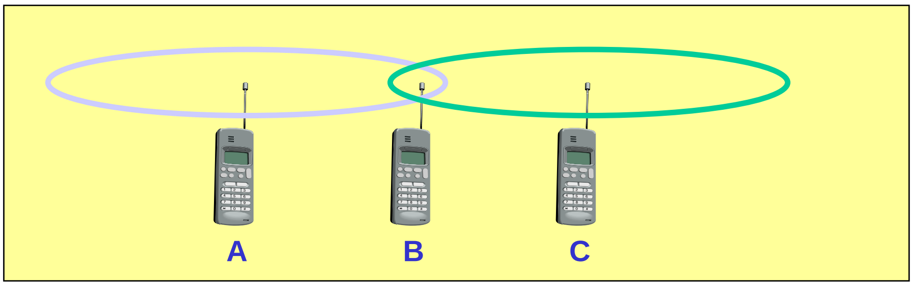
Unless interrupted due to medium occupancy limitations for a given PHY,
- the **fragments of a single MSDU or MMPDU are sent as a burst during the CP**,
- using a **single invocation of the DCF medium access procedure**.

Hidden terminals

JS

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**

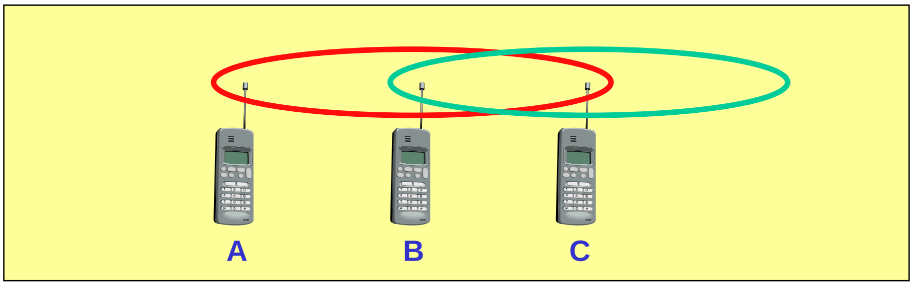


=> cf. subsection 3. Wireless Communication Basics

Exposed terminals

Exposed terminals

- **B** sends to **A**, **C** wants to send to another terminal (not A or B)
- **C** has to wait, CS signals a medium in use, but …
- **A** is outside the radio range of **C**, therefore waiting is not necessary
- **C** is “exposed” to **B**

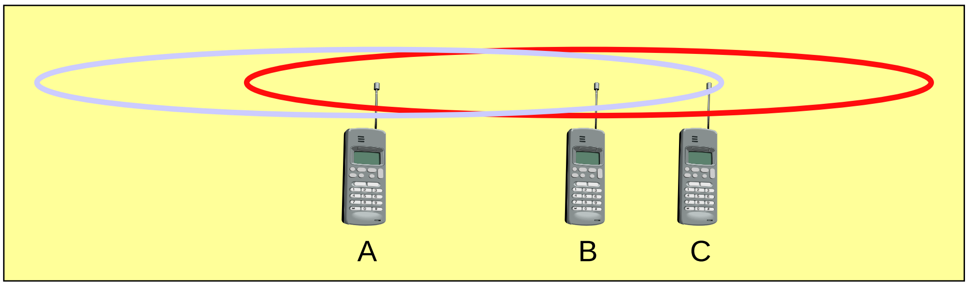


=> cf. subsection 3. Wireless Communication Basics

Near and far terminals

Terminals A and B send, C receives

- signal **strength decreases** proportional **to the square of the distance**
- the **signal** of terminal B therefore **drowns out** A’s signal
- **C cannot receive** A



If C for example was an arbiter for sending rights, terminal B would drown out terminal A already on the physical layer

=> cf. subsection 3. 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/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.

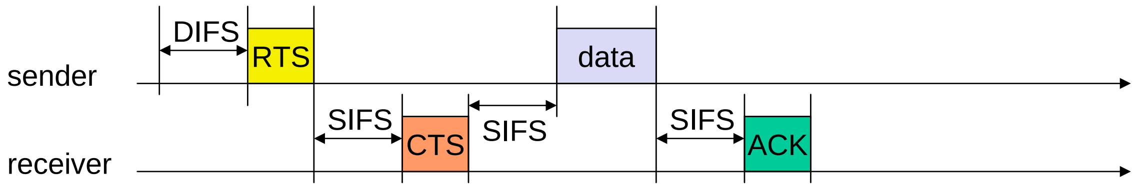
The medium access protocol allows for STAs to support different sets of data rates. All **STAs shall receive all the data rates in aBasicRateSet** and **transmit at one or more** of the aBasicRateSet data rates. To support the proper operation of the RTS/CTS and the virtual carrier-sense mechanism, all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

Example: RTS/CTS

JS

- 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



Virtual carrier sensing: Network allocation vector

The state of the medium is determined by

a physical carrier-sense mechanism
shall be **provided by the PHY**. The details of physical carrier sense are provided in the individual PHY specifications.

a virtual carrier-sense mechanism
shall be **provided by the MAC**. This mechanism is referred to as the **network allocation vector (NAV).**

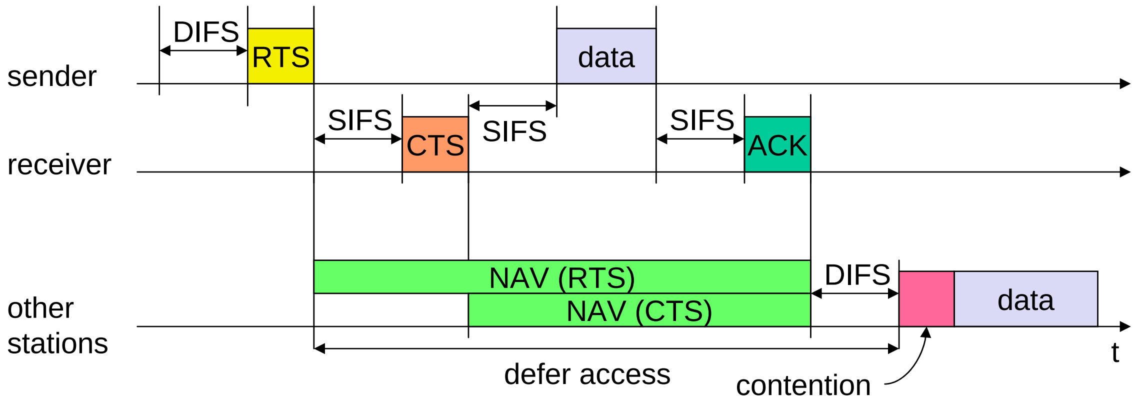
- The NAV maintains a **prediction of future traffic** on the medium based on duration information that is announced in RTS/CTS frames prior to the actual exchange of data.
- The duration information is also available in the **MAC headers of all frames** sent during the CP other than PS-Poll Control frames.

When either function indicates a busy medium, the medium is considered busy.

Example: NAV with RTS/CTS

JS

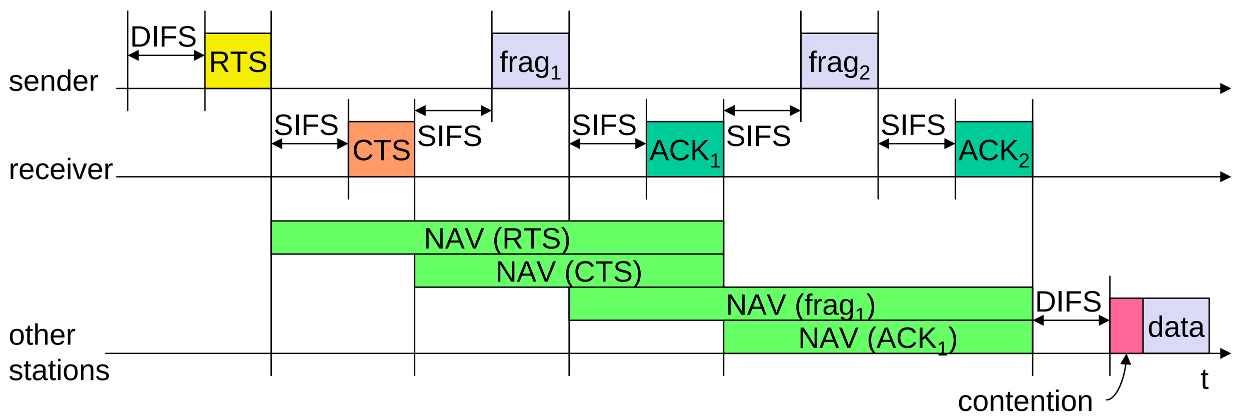
- station can **send RTS** with reservation parameter **after waiting for DIFS**
  (reservation determines amount of time the data packet needs the medium)
- **acknowledgement via CTS after SIFS** by receiver (if ready to receive)
- sender can now **send data at once, acknowledgement via ACK**
- **other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



NAV = Network Allocation Vector (in STAs)

RTS/CTS usage with fragmentation

JS



Summary: Distributed coordination function (DCF)

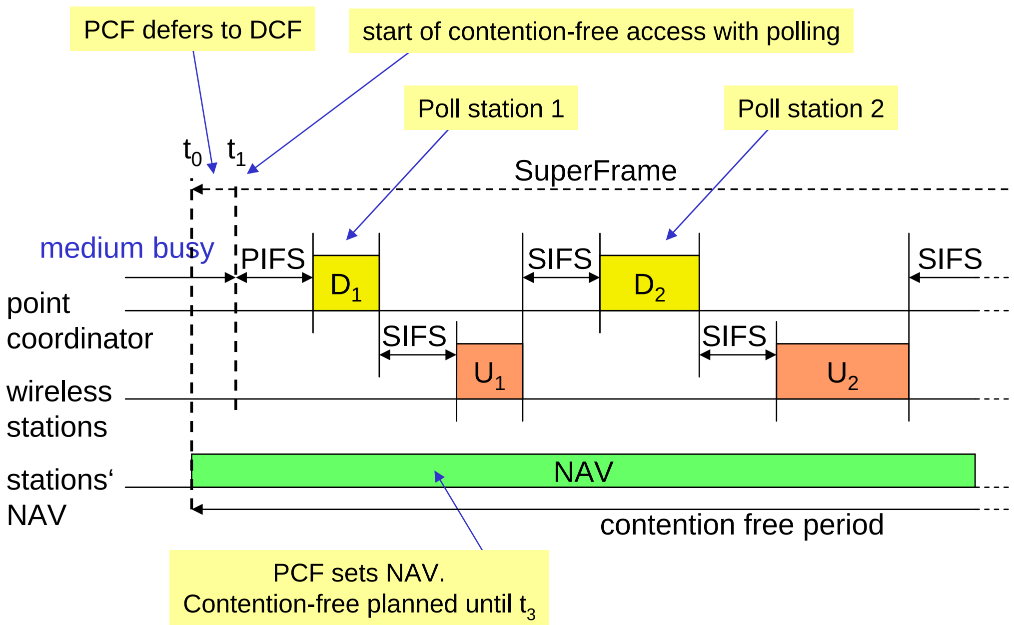
- For a STA to transmit, it shall **sense the medium** to determine if another STA is transmitting. If the medium is not determined to be busy … , the transmission may proceed.
- The CSMA/CA distributed algorithm mandates that a **gap** of a minimum specified duration exist **between contiguous frame sequences**.
- A transmitting STA shall ensure that the **medium is idle for this required duration** before attempting to transmit.
- **If the medium is** determined to be **busy**, the STA shall **defer until the end of the current transmission**.
- **After deferral, or prior to attempting to transmit again** immediately after a successful transmission, the STA shall **select a random backoff interval** and shall decrement the backoff interval counter while the medium is idle.
- A **refinement** of the method may be used under various circumstances to further minimize collisions—here the transmitting and receiving STA exchange short control frames [**request to send (RTS)** and **clear to send (CTS)** frames] **after determining that the medium is idle and after any deferrals or backoffs**, prior to data transmission.

IEEE 802.11-1999, p. 70

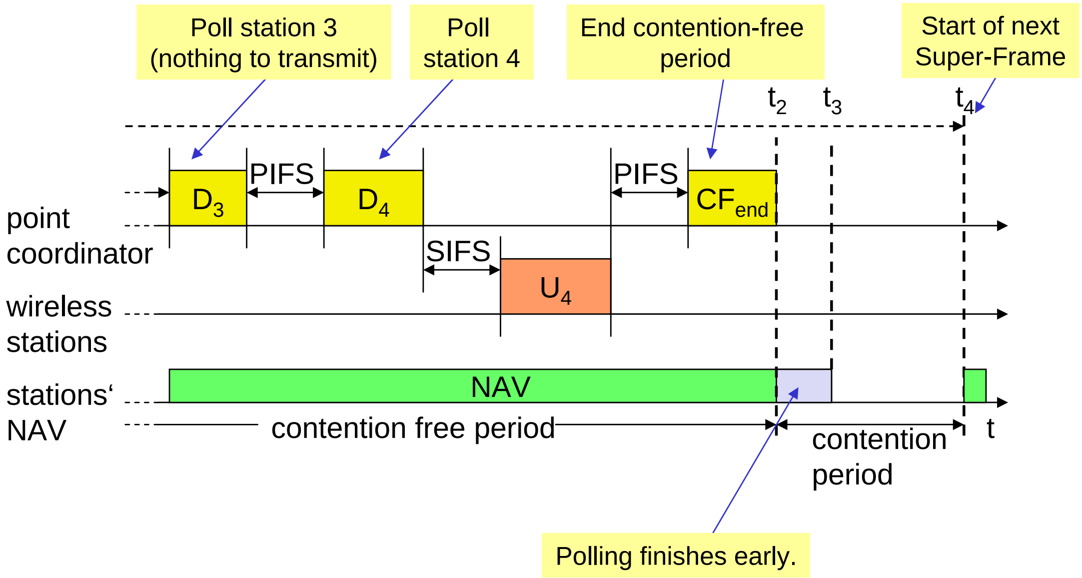
5.4.4. The point coordination function (PCF) *JS*

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**".



PCF (2)



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

5.5. Frame formats

The MAC protocol data units (MPDUs) or frames in the MAC sublayer are described as a sequence of fields in specific order.

Each frame consists of the following basic components:

a) MAC header (frame control, duration, addresses, and sequence control information).

b) Frame body (variable length, which contains information specific to the frame type).

c) Frame check sequence (FCS, an IEEE 32-bit cyclic redundancy code, CRC).

5.5.1. General frame format *JS*

- **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

5.5.2. Type / subtype combinations

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	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved

Type / subtype combinations (2)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
01	Control	0000-1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear to Send (CTS)
01	Control	1101	Acknowledgement (ACK)
01	Control	1110	Contention Free (CF) - End
01	Control	1111	CF-End + CF-Ack
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

MAC address format

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

Important message: Four (!) address fields

5.5.3. Special Frames: ACK, RTS and CTS *JS*

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

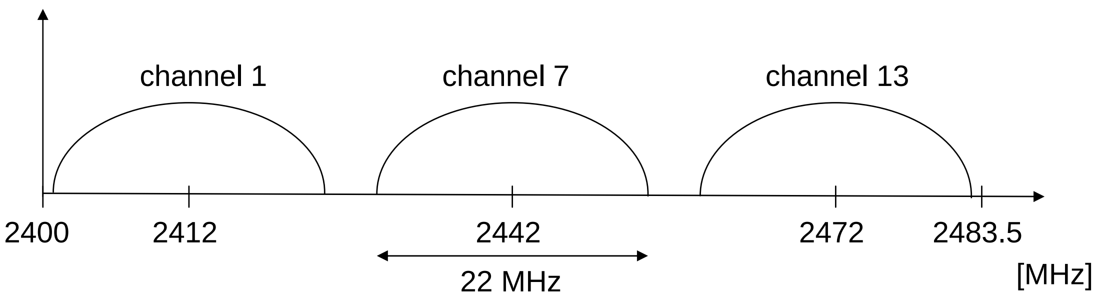
5.6. Physical channel usage

The **base document** (IEEE 802.11) already includes **3 different PHYs:**
- Clause 14: Frequency Hopping Spread Spectrum (FHSS)
- Clause 15: Direct Sequence Spread Spectrum (DSSS)
- Clause 16: Infrared

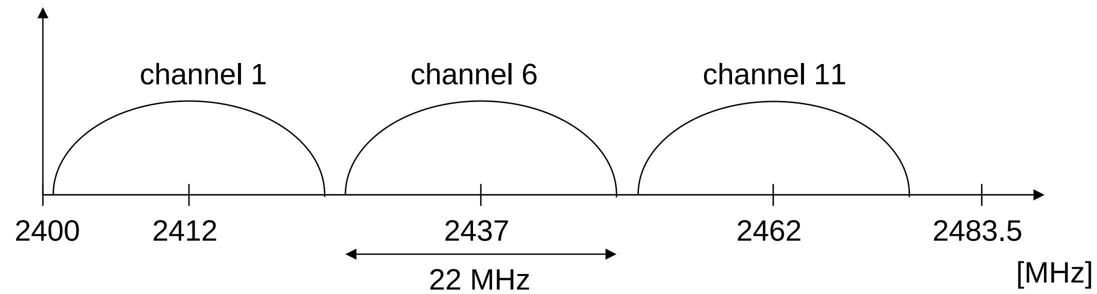
Additional PHYs are specified in **supplements.**

5.6.1. Channel selection for 802.11b (non-overlapping) *JS*

Europe (ETSI)

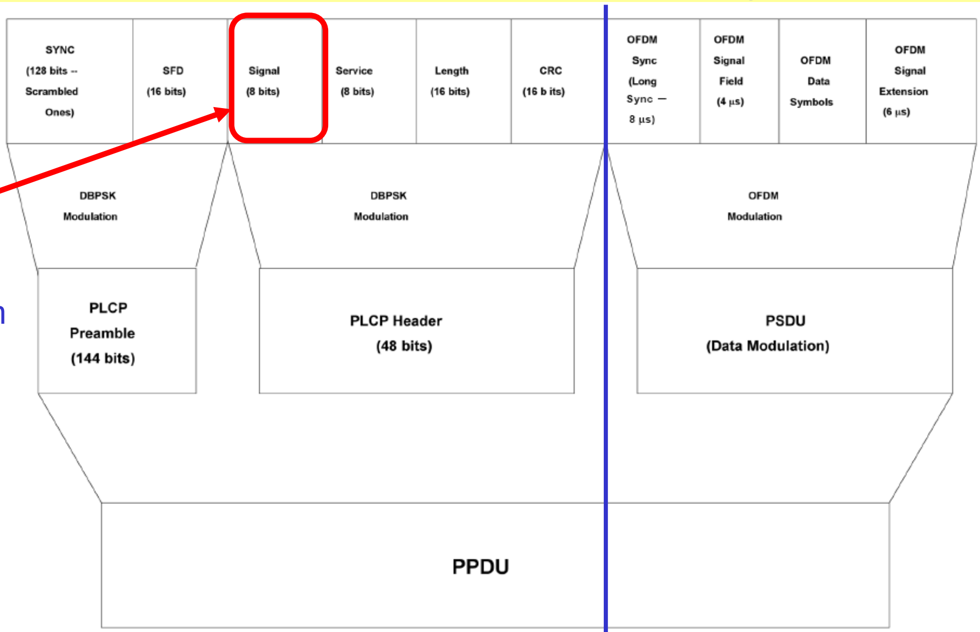


US (FCC)/Canada (IC)



IEEE 802.11 g **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

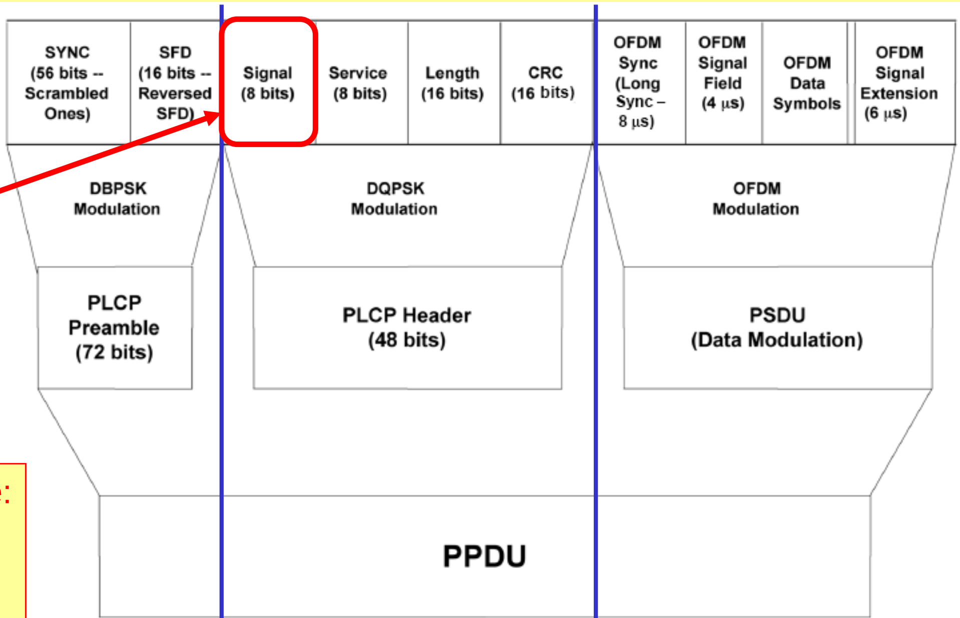
ERP Enhanced rate PHY using DSSS or OFDM

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

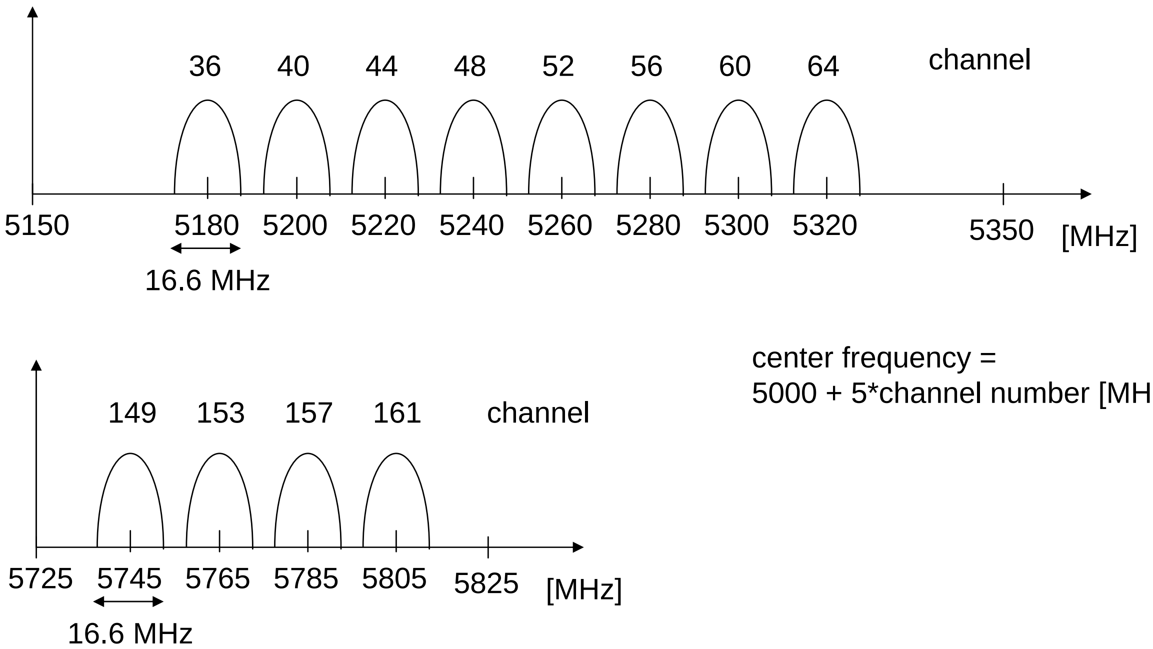
backwards compatibility

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

(DQPSK = Differential Quadrature Phase Shift Keying)

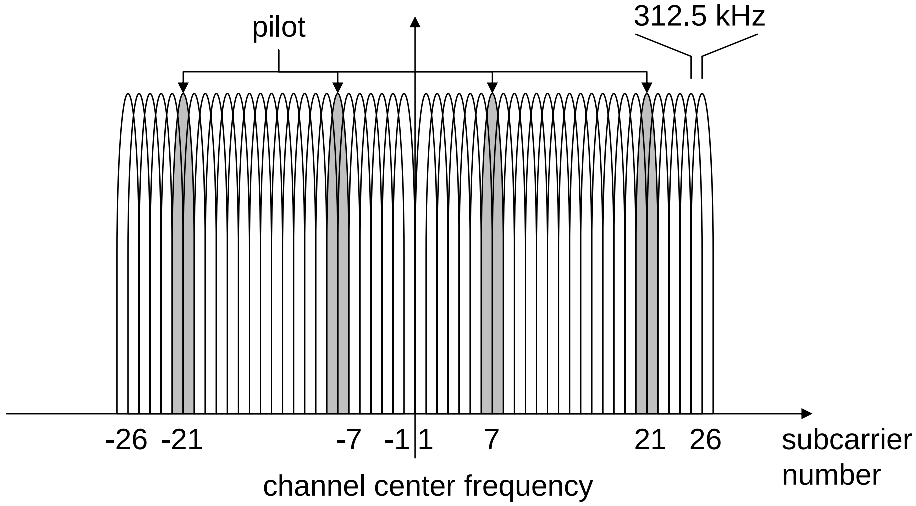
5.6.2. Channel selection for 802.11a (non-overlapping) *JS*



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

OFDM in IEEE 802.11a *JS*

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



5.7. QoS Support in the new WLAN Standards

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

… but WLAN medium access is (still) Best Effort !!!

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**

Standard IEEE 802.11e-2005

- **MAC QoS Enhancements**

IEEE 802.11g-2003

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

IEEE 802.11n Task Group (**Work in progress**)

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

The distributed coordination function (DCF)

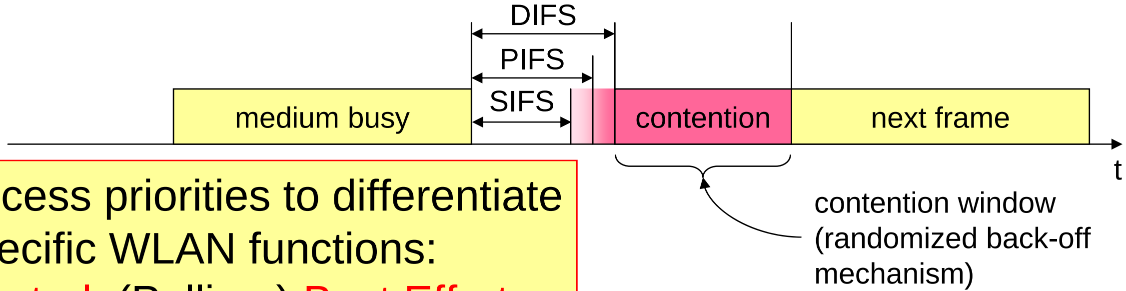
Reminder from earlier subsection

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:**

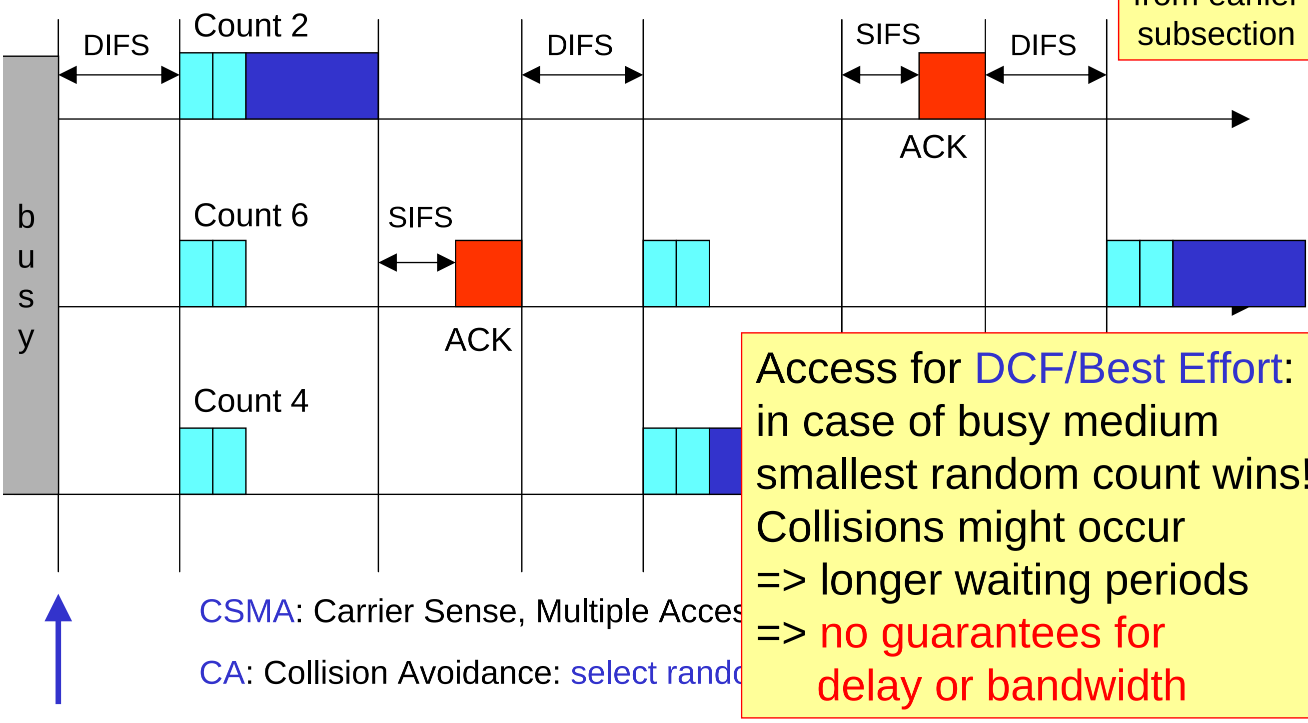
- **SIFS** (Short Inter Frame Spacing)
  - **highest priority**, for ACK, CTS, polling response
- **PIFS** (PCF IFS)
  - **medium priority**, for time-bounded service using PCF
- **DIFS** (DCF, Distributed Coordination Function IFS)
  - **lowest priority**, for asynchronous data service



Access priorities to differentiate specific WLAN functions:
Control, (Polling,) Best Effort

CSMA/CA MAC: Example 3 stations

Reminder from earlier subsection



Access for DCF/Best Effort:
in case of busy medium
smallest random count wins!
Collisions might occur
=> longer waiting periods
=> no guarantees for
delay or bandwidth

t = 0, medium gets idle

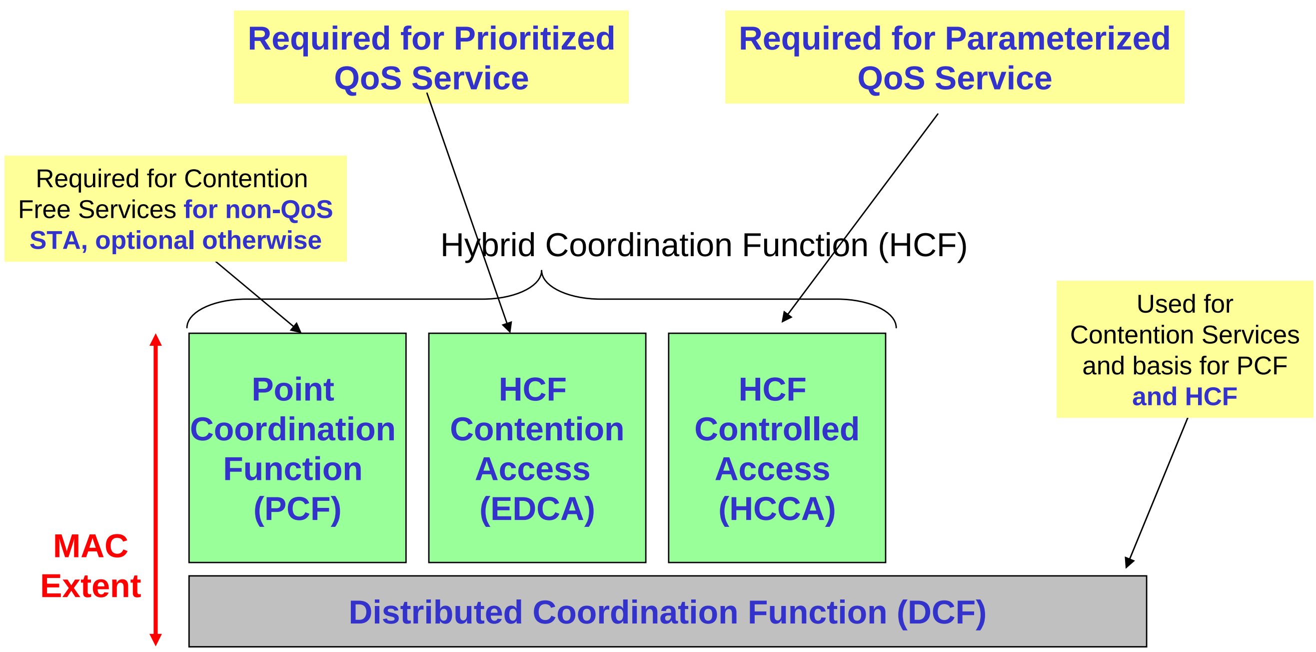
CSMA: Carrier Sense, Multiple Acces

CA: Collision Avoidance: select rando

Collision Detection is not possible (wireless!)
=> receiver sends ACKnowledgement with highest priority (SIFS)
lack of ACK triggers retransmission

The new MAC Architecture for WLAN QoS Support

New MAC architecture extending the existing PCF + DCF:



Prioritized QoS Service: EDCA

HCF Contention-based Channel Access:

EDCA – Enhanced Distributed Channel Access

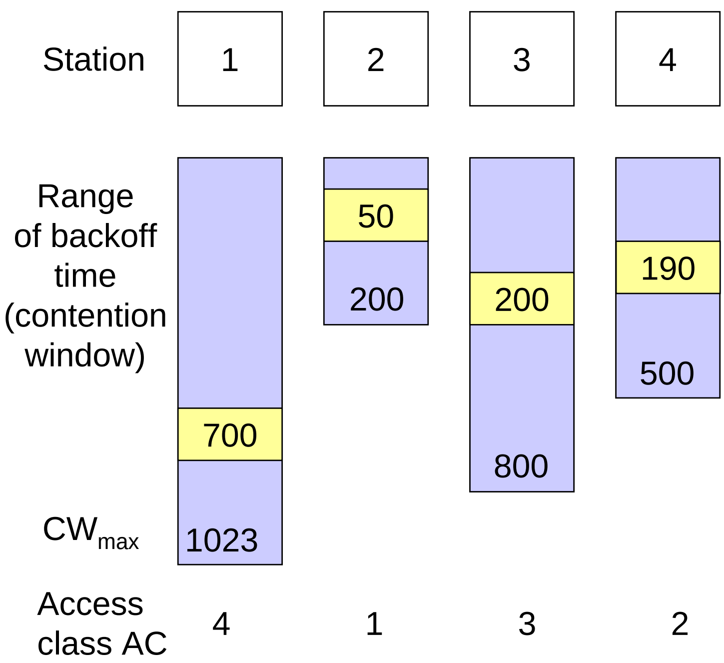
EDCA provides differentiated, distributed access to the medium using 8 different **UPs** (**user priorities**, same as IEEE 802.1D)

User Priority to Access Category mappings (802.11e Draft)

Priority	User priority (UP – Same as 802.1D User Priority)	802.1D Designation	Access Category (AC)	Designation (Informative)	
lowest	1	BK	AC_BK	Background	Background
	2	-	AC_BK	Background	
	0	BE	AC_BE	Best Effort	Best Effort
	3	EE	AC_BE	Best Effort	
	4	CL	AC_VI	Video	Video
	5	VI	AC_VI	Video	
	6	VO	AC_VO	Voice	Voice
highest	7	NC	AC_VO	Voice	

UPs are mapped to four **access categories (AC)** for medium access.

EDCA Example: Four Stations – four classes



Access for EDCA as DCF: in case of busy medium smallest random count wins!

Properties:

CW_{max} in higher access class is smaller
=> (on average) higher AC has more opportunities to send

Randomness => on average!

Collisions still might occur
=> longer waiting periods
=> no guarantees for delay or bandwidth

Parameterized QoS Service: HCCA

HCF Controlled Channel Access: **HCCA**

Common to PCF – Point Coordination Function:

- centralized point coordinator (typically access point AP)
- polling function: Stations are only allowed to send when polled from the coordinator

In practice: PCF rarely implemented !!!

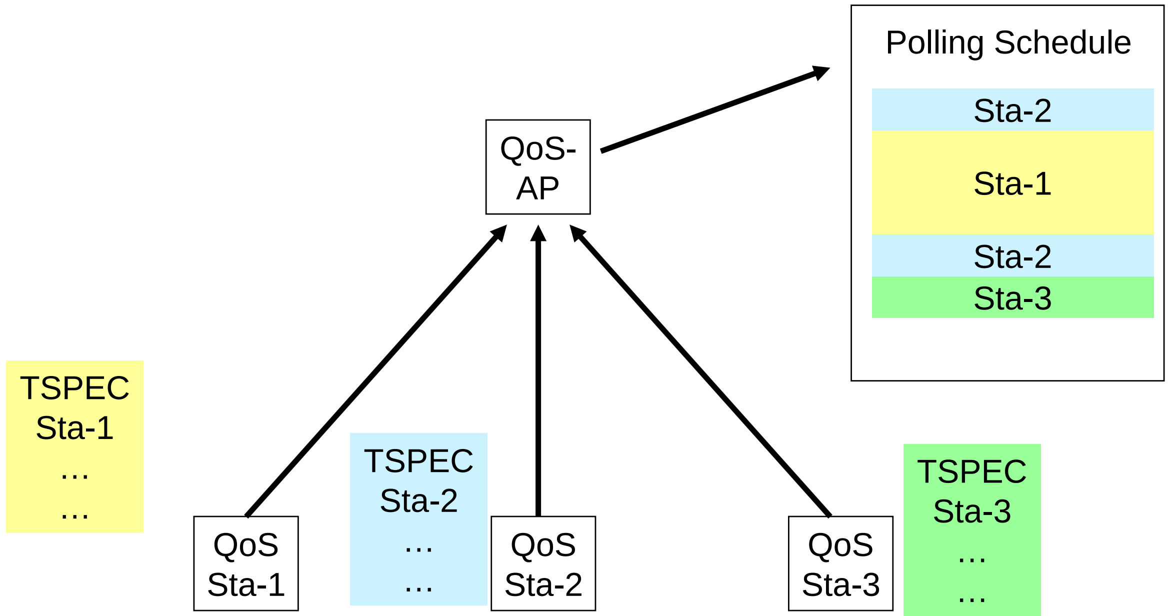
Different to PCF: (new!)

- HCCA coordinator is "QoS aware"
- operating rules are different from coordinator of PCF

- QoS-Stations have to negotiate their demand with the HC using TSPEC (traffic specification)
- HC has knowledge of all QoS requirements
- Access Control is used to accept/deny TSPEC reservation

=> the HC can set up a polling-schedule that serves (and "guarantees") all reservations

HCCA Example:

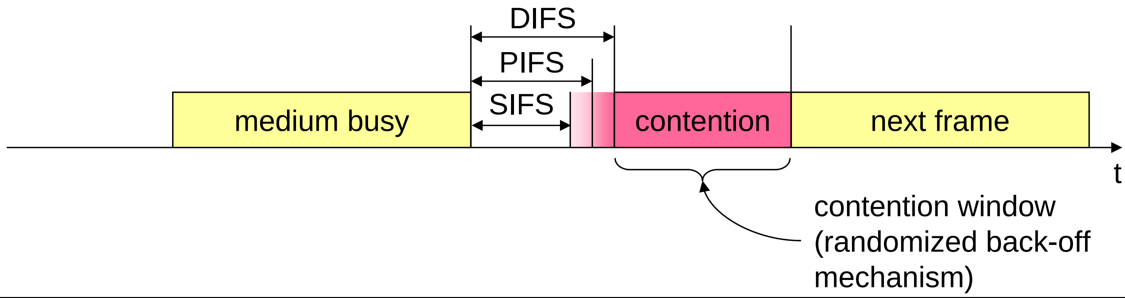


- QoS-Stations have to negotiate their demand with the HC using TSPEC (traffic specification)
- HC has knowledge of all QoS requirements
- Access Control is used to accept/deny TSPEC reservation

=> the HC can set up a polling-schedule that serves (and "guarantees") all reservations

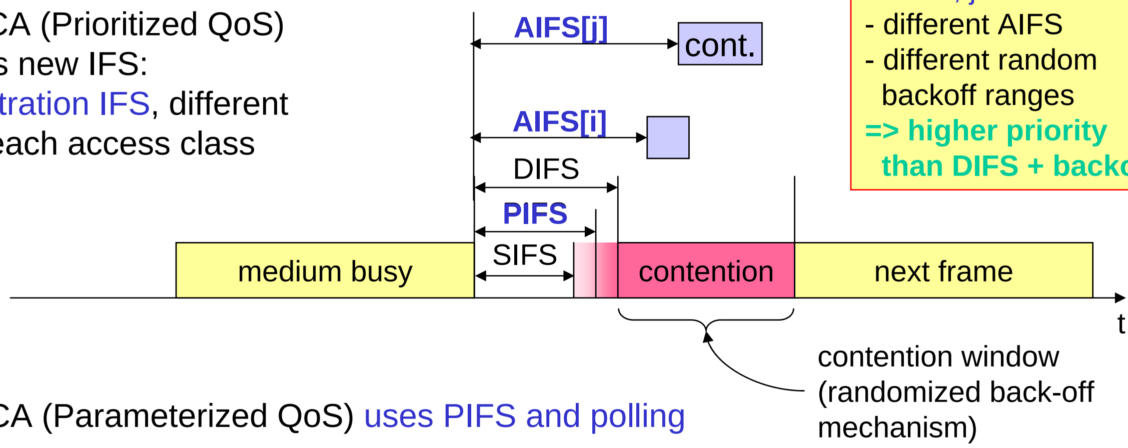
Coexistence of DCF, PCF and HCF: inter frame spaces

Access priorities through different inter frame spaces:



QoS enabled WLAN APs + mobile stations:

EDCA (Prioritized QoS) uses new IFS: Arbitration IFS, different for each access class



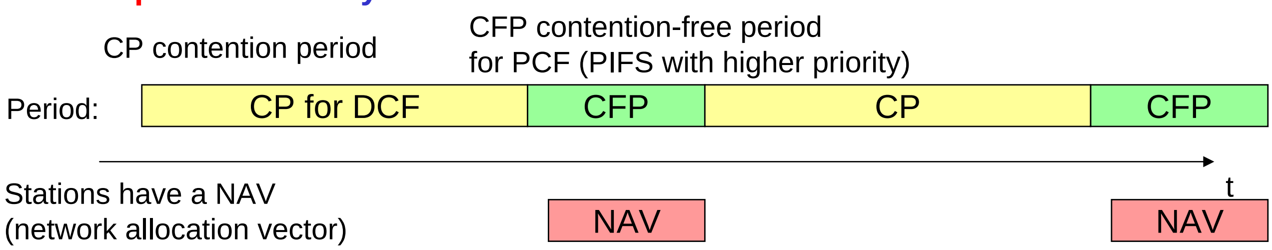
Class i, j
- different AIFS
- different random backoff ranges

=> higher priority than DIFS + backoff

HCCA (Parameterized QoS) uses PIFS and polling

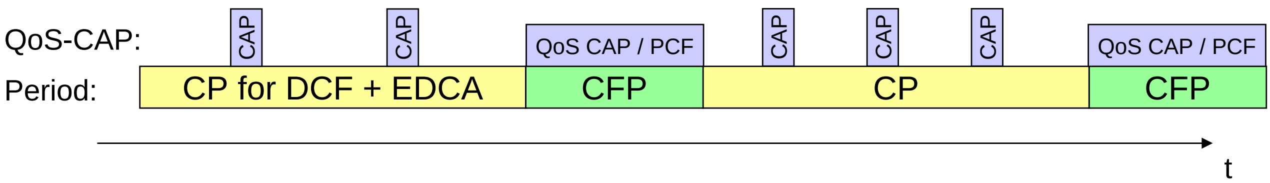
Coexistence of DCF, PCF and HCF: access periods

Access periods already existed with DCF and PCF:



Stations have a NAV (network allocation vector) to virtually mark the network as busy

Controlled Access Phases (CAP) may occur in both CFP and CP:



Controlled Access Phase:
- during CFP for PCF and HCCA
- during CP for HCCA
  separation with PIFS, smaller than DIFS/AIFS[]

=> due to PIFS, HCCA/CAP also working **in presence of non-QoS WLAN stations**

Product Implementation of QoS in WLAN

WMM of the Wi-Fi-Alliance

- "*WMM stands for Wi-Fi Multimedia, features that improve the user experience for audio, video and voice applications over a Wi-Fi® network.*
  WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard."

- WMM implements EDCA (prioritized QoS) of 802.11e
- HCCA (parameterized QoS) may be added as optional module to WMM (future!)

- e.g. Atheros Communication WLAN Wi-Fi-certified for WMM

- more information at http://www.wi-fi.org/knowledge_center_overview.php

EDCF of Cisco

- "*For WLAN QoS, Cisco APs and 7920 Wireless IP Phones use a technique similar to IEEE 802.11e, called enhanced DCF (EDCF). EDCF enables endpoint devices that have delay-sensitive multimedia traffic to modify their CWmin and CWmax values to allow for statically greater (and more frequent) access to the medium*".

- more information at http://www.cisco.com/ and/or Search "cisco WLAN EDCF"