Contents

IEEE 802.11 WLAN architecture

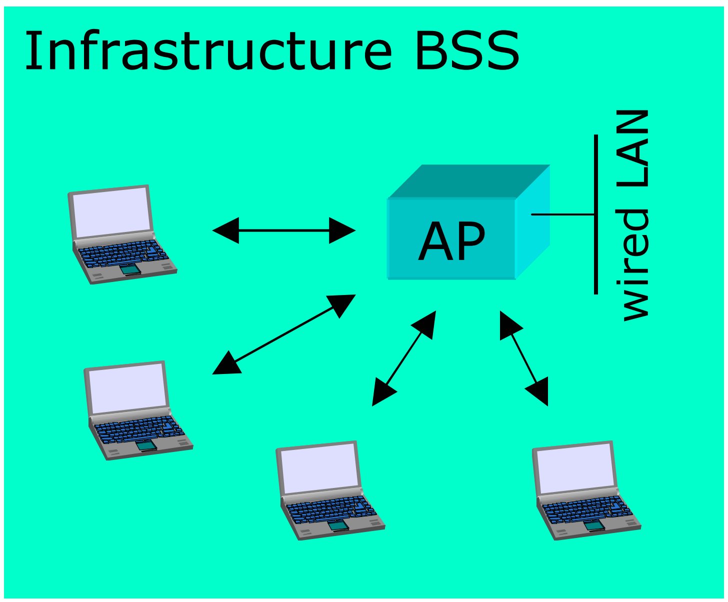
- Basic routing example
- IAPP and mobility management
- Basic frame structure
- MAC header structure
- Usage of MAC address fields

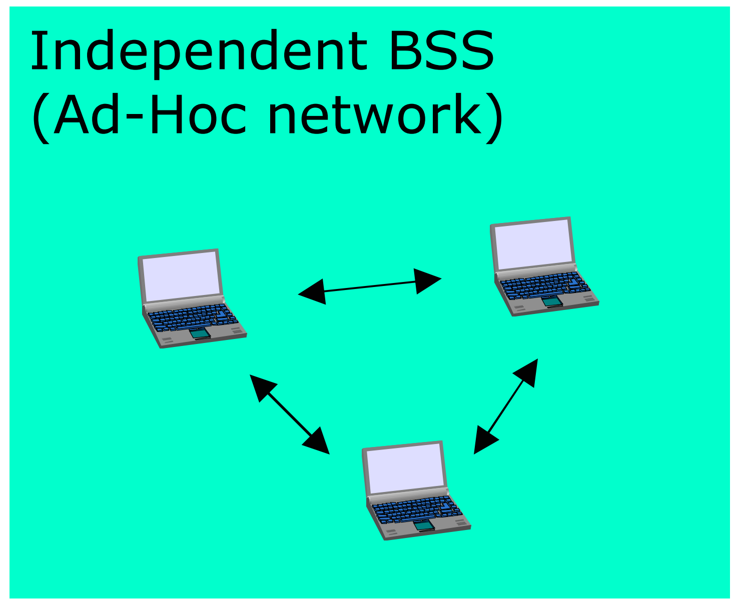
Management frames

Some IEEE 802.11 standard amendments

IEEE 802.11 WLAN architecture

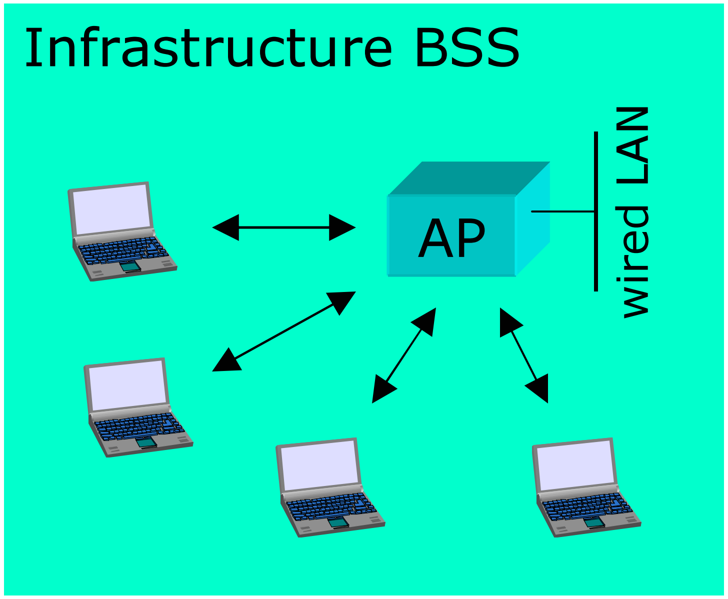
802.11 defines two BSS (Basic Service Set) options:





Infrastructure BSS

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



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

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

Before stations can use the BSS: Association.

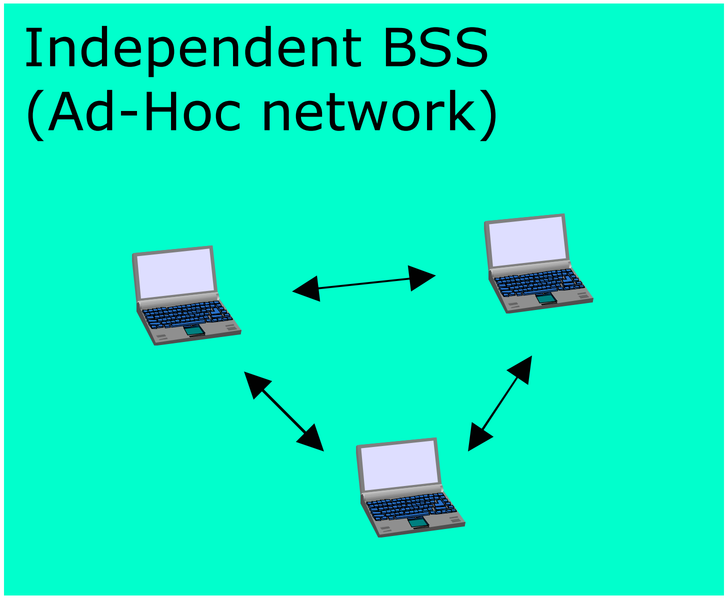
Independent BSS

Mainly of interest for military applications.

No access point is required, stations can communicate directly.

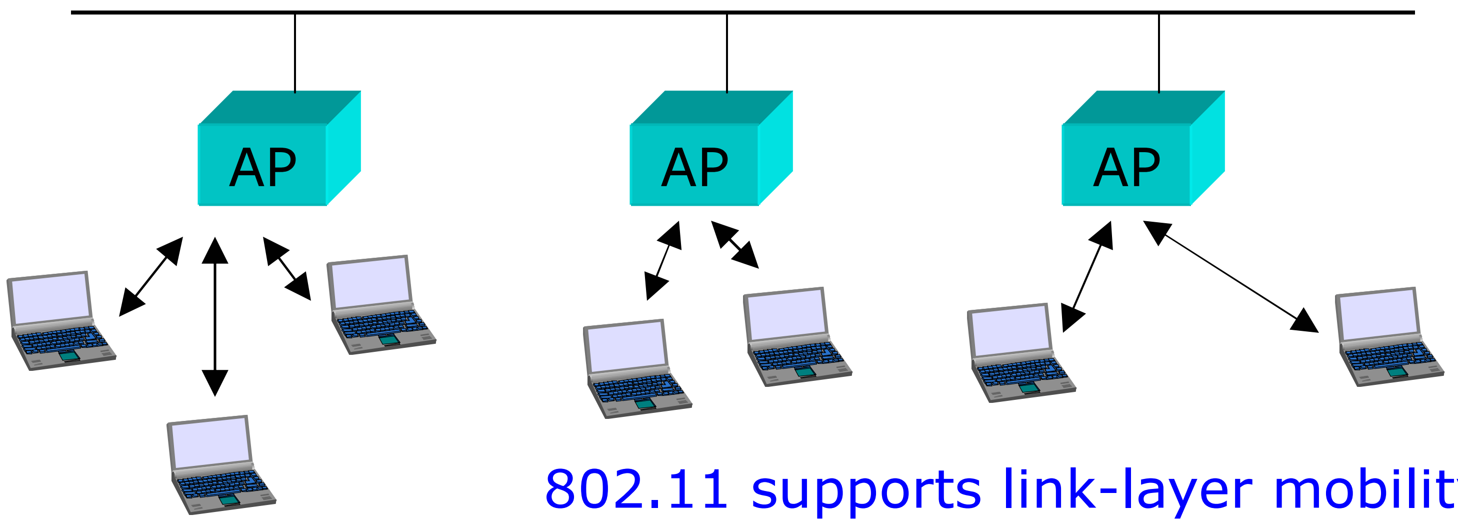
Efficient routing of packets is not a trivial problem (routing is not a task of 802.11).

Ad-Hoc WLAN networks are outside the scope of this course.



Extended Service Set (ESS)

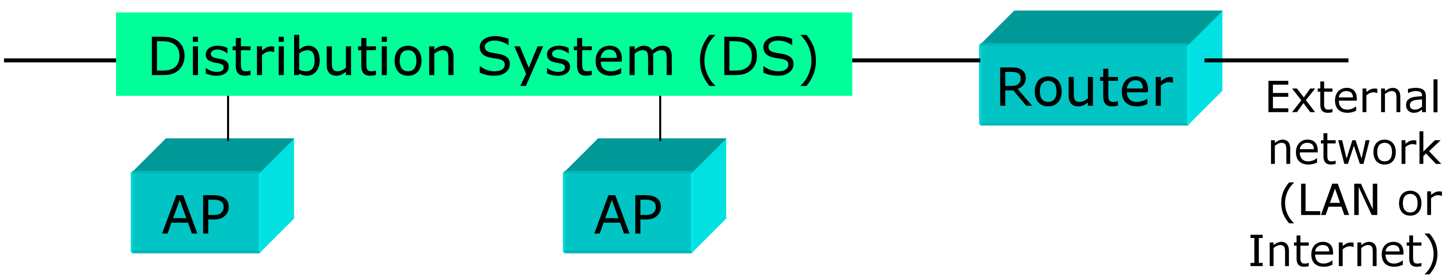
This is a larger WLAN network consisting of a number of BSS networks interconnected via a common backbone



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

Distribution system

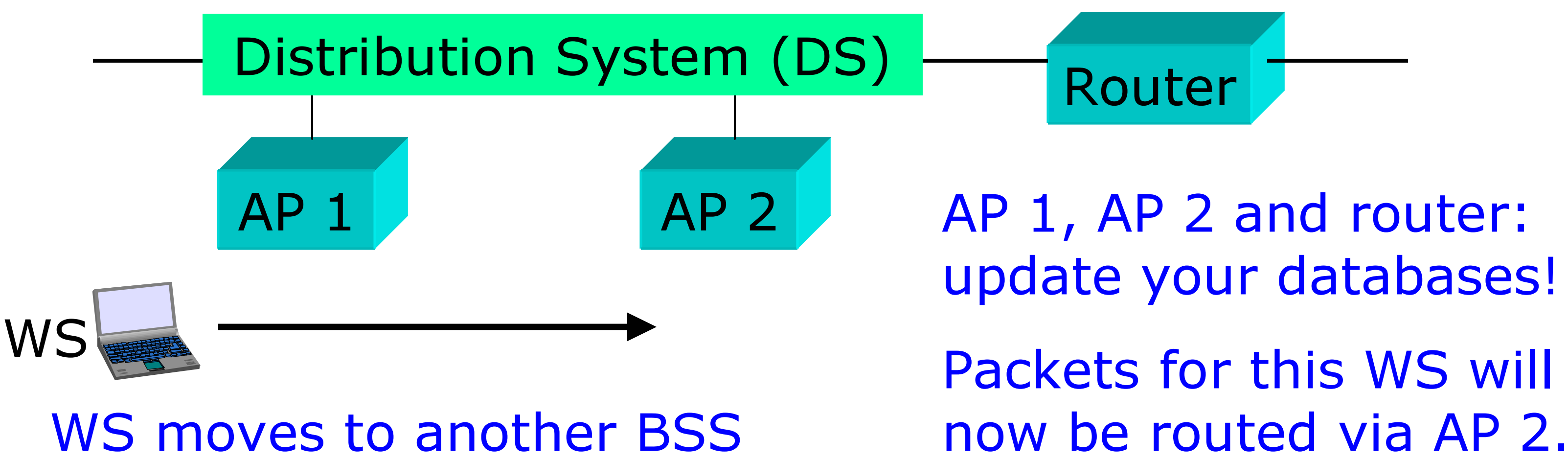
This is the mechanism by which APs and other nodes in the wired IP subnetwork communicate with each other.



This communication, using the Inter-Access Point Protocol (IAPP), is essential for link-layer mobility (=> stations can seamlessly move between different BSS networks).

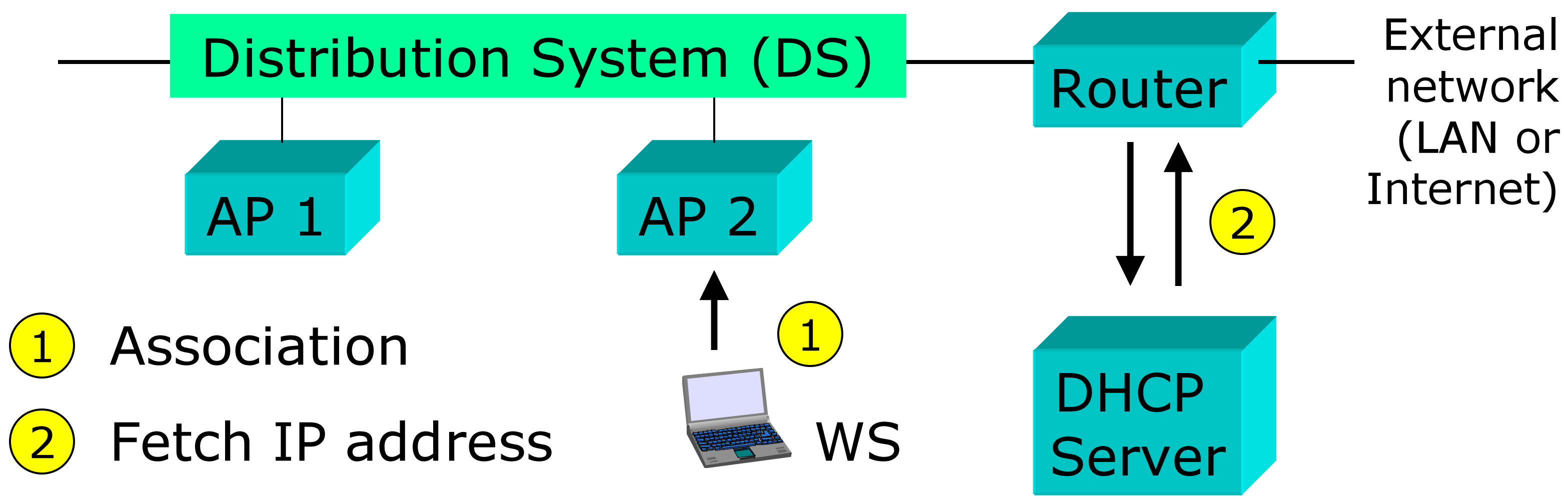
Distribution system (cont.)

For instance, when a wireless station moves from one BSS to another, all nodes must update their databases, so that the DS can distribute packets via the correct AP.



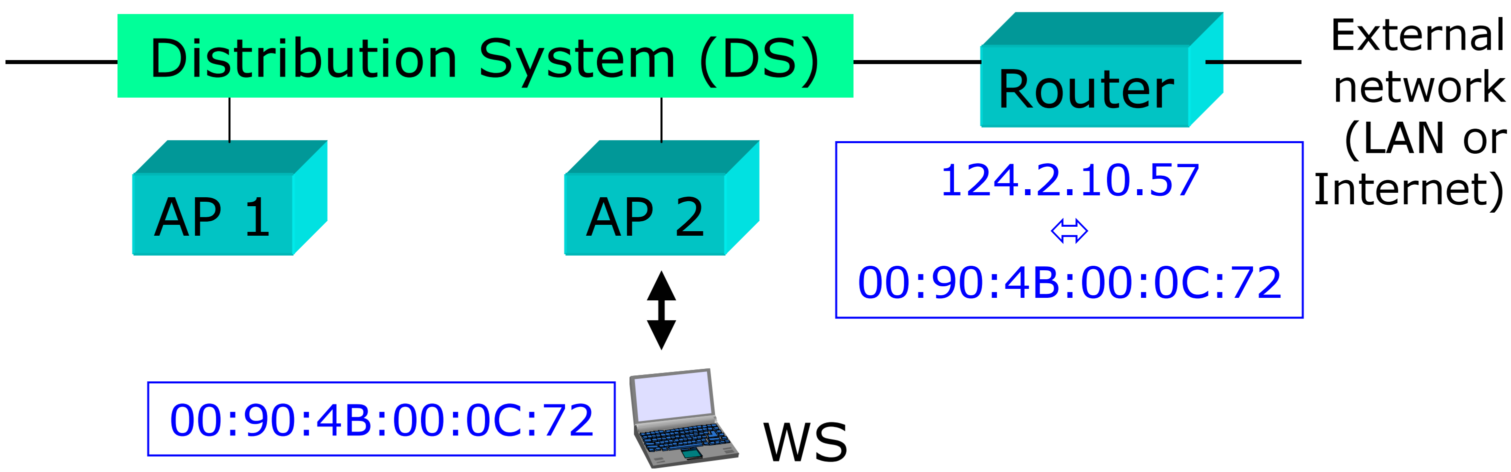
Basic routing example

When WS associates with AP 2, the router in charge of the IP subnet addressing obtains an IP address from the DHCP (Dynamic Host Configuration Protocol) server.



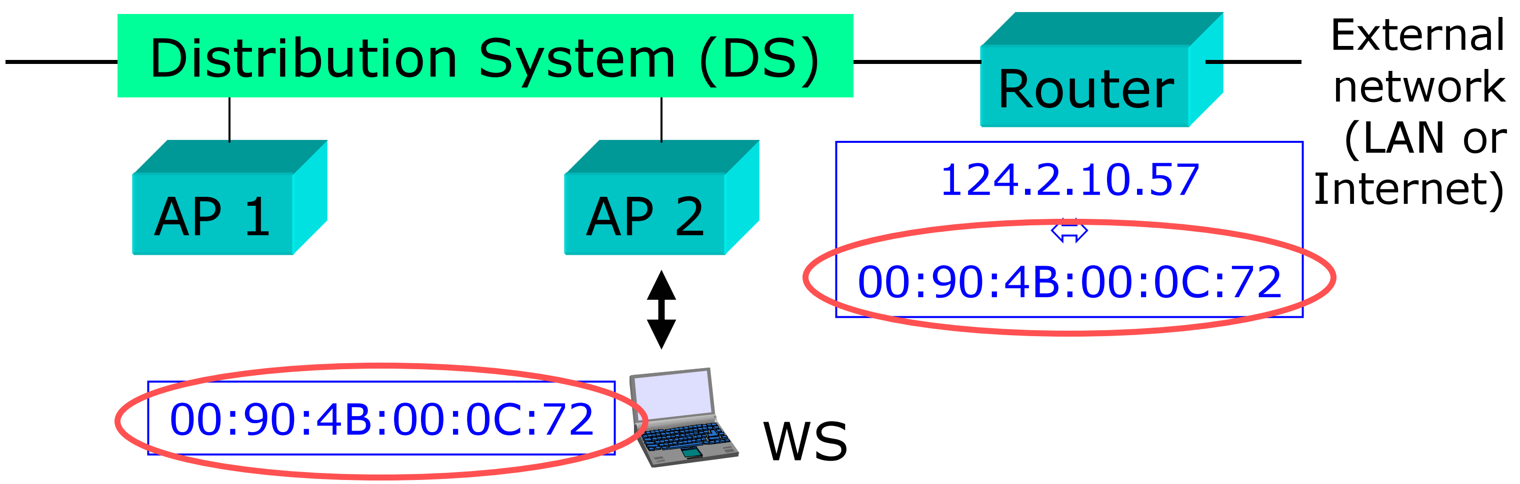
Basic routing example (cont.)

The router must maintain binding between this IP address and the MAC address of the wireless station.



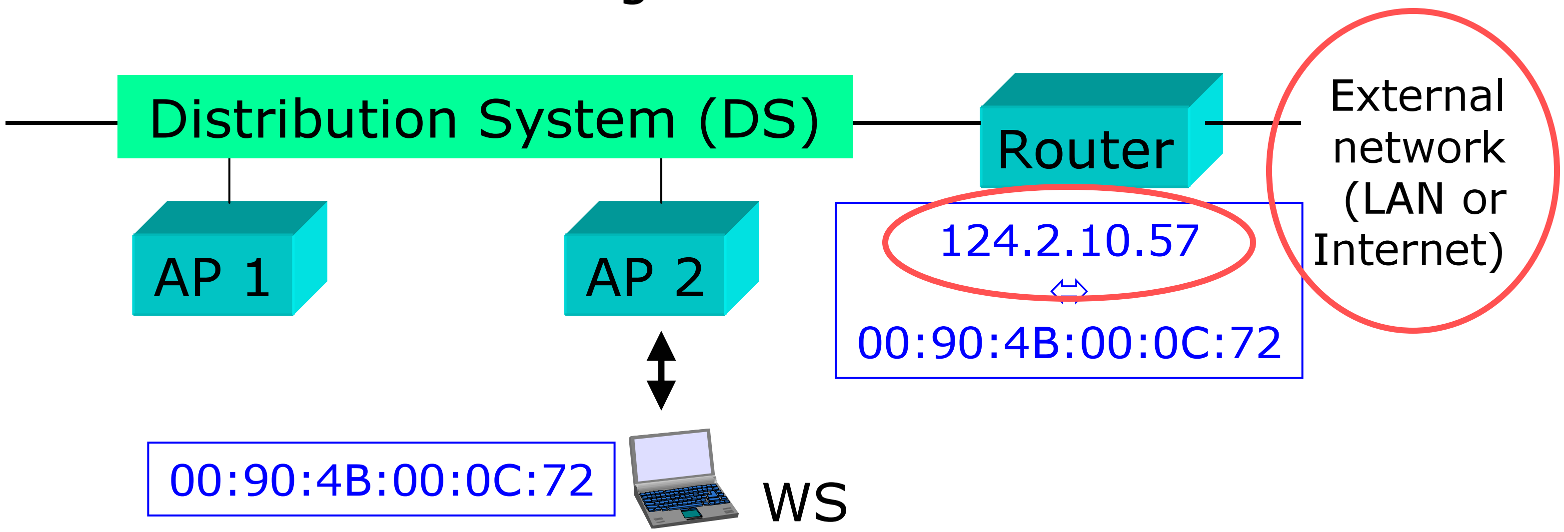
Basic routing example (cont.)

The globally unique MAC address of the wireless station is used for routing the packets within the IP subnetwork (DS + attached BSS networks).



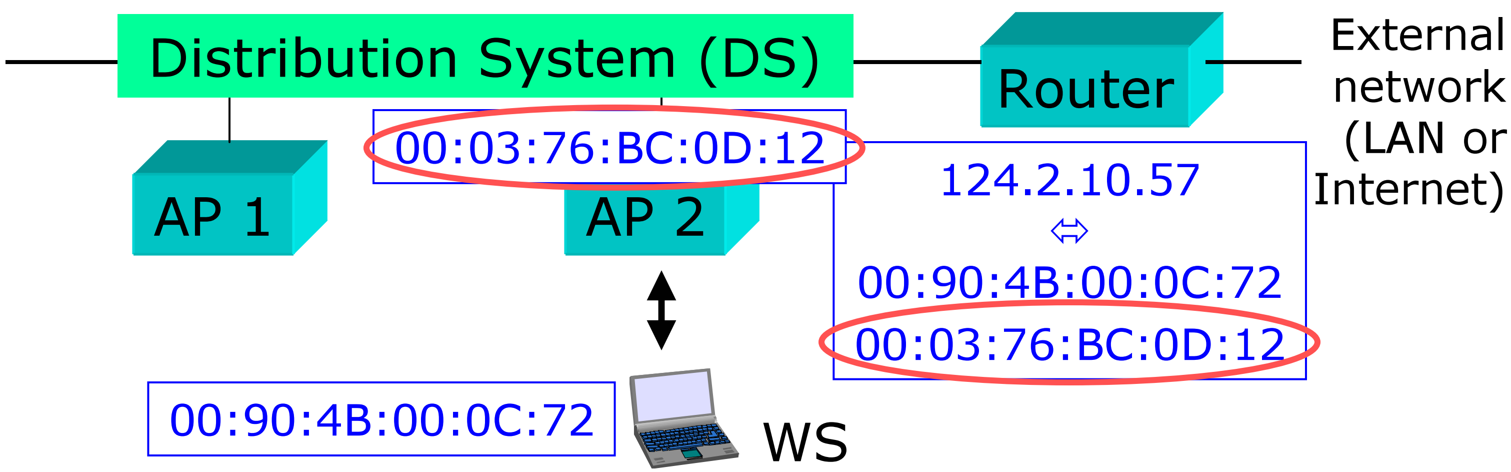
Basic routing example (cont.)

The dynamic and local IP address of the wireless station is only valid for the duration of attachment to the WLAN and is used for communicating with the outside world.



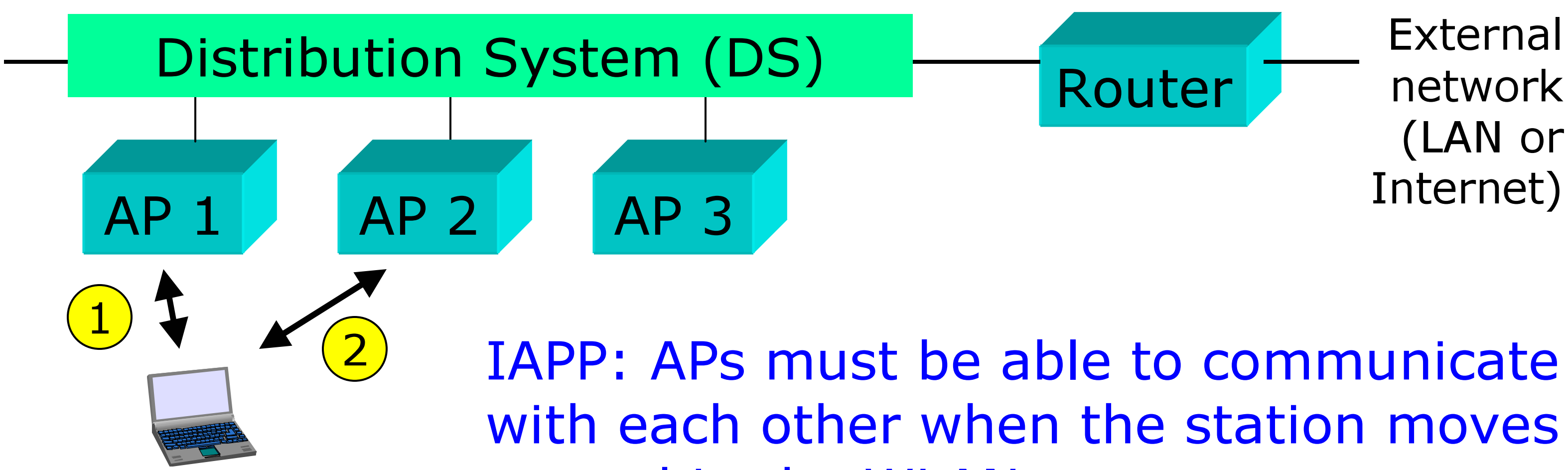
Basic routing example (cont.)

The router must also know (and use) the MAC address of the access point via which the packets must be routed. For this purpose, a special protocol (IAPP) is needed!



IAPP (Inter-Access Point Protocol)

IAPP (defined in IEEE 802.11f) offers mobility in the Data link layer (within an ESS = Extended Service Set).



IAPP: APs must be able to communicate with each other when the station moves around in the WLAN

In addition to IAPP …

IAPP alone is not sufficient to enable seamless handovers in a WLAN. The stations must be able to measure the signal strengths from surrounding APs and decide when and to which AP a handover should be performed (no 802.11 standardised solutions are available for this operation).

In 802.11 networks, a handover means reassociating with the new AP. There may be two kinds of problems:

- will handover work when APs are from different vendors?
- will handover work together with security solutions?

Mobility Management (MM)

There are basically two objectives of Mobility Management:

1. MM offers seamless handovers when moving from one network/subnetwork/BSS to another

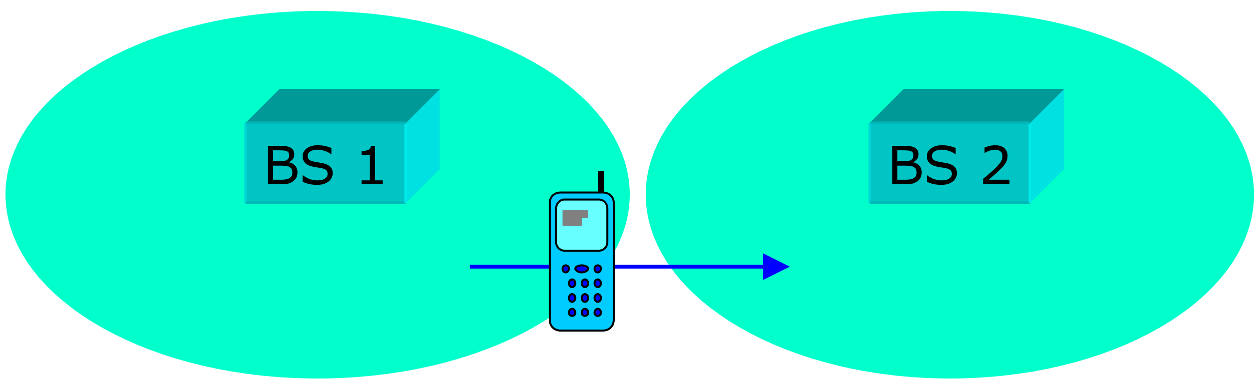
   Active network connection – handover

2. MM makes sure that users or terminals can be reached when they move to another network/subnetwork/BSS

   Passive user/terminal – reachability

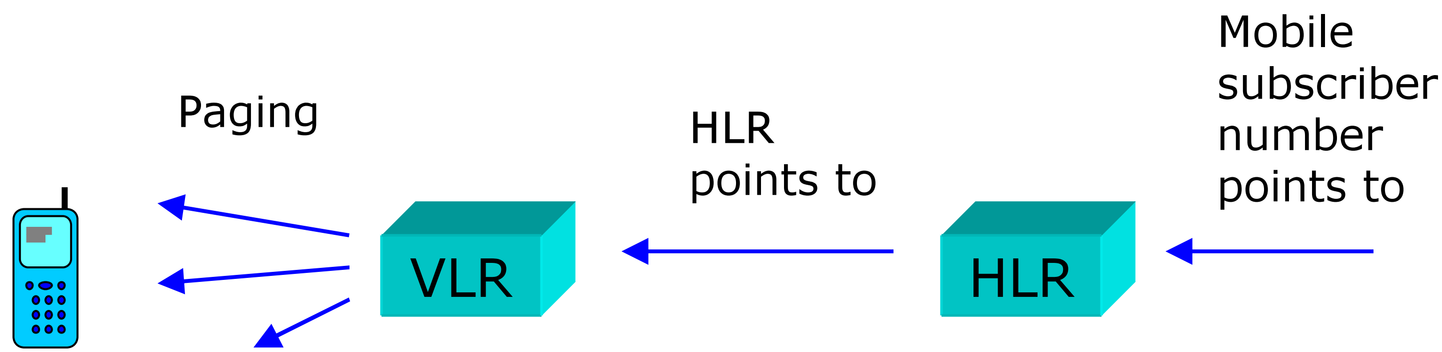
MM in cellular wireless networks (1)

1. Handover: In a cellular wireless network (e.g. GSM), the call is not dropped when a user moves to another cell. Handovers are based on measurements performed by the mobile terminal and base stations.



MM in cellular wireless networks (2)

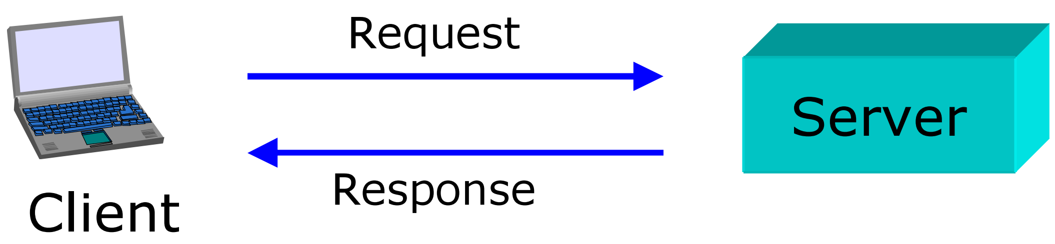
2. Reachability: In a cellular wireless network, the HLR (Home Location Register) knows in which VLR (Visitor Location Register) area the mobile terminal is located. The VLR then uses paging to find the terminal.



MM in cellular wireless networks (3)

3. IP services (e.g. based on GPRS): Reachability in this case is kind of a problem. Conventional IP services use the client – server concept where reachability is not an important issue.

Typical client - server transaction:



MM in three different OSI layers

Mobility Management (MM) schemes are possible in three different layers of the OSI protocol layer model:

Application layer	e.g. SIP (Session Initiation Protocol)	*Personal mobility*
…		
…		
Transport layer		
Network layer	e.g. Mobile IP	*Terminal mobility*
Data link layer	IAPP (Inter-Access Point Protocol)	
Physical layer		*Handovers*

MM in the Data link layer

Mobility Management (MM) schemes are possible in three different layers of the OSI protocol layer model:

Application layer
…
…
Transport layer
Network layer
Data link layer
Physical layer

IAPP (IEEE 802.11f):

Seamless roaming within an ESS network (= IP subnet).

Handover is not possible when moving from one ESS network to another.

No reachability solutions.

MM in the Network layer

Mobility Management (MM) schemes are possible in three different layers of the OSI protocol layer model:

Application layer
…
…
Transport layer
Network layer
Data link layer
Physical layer

Mobile IP:

Seamless roaming between ESS networks (= IP subnetworks).

Handover is possible when moving from one ESS (or WLAN) network to another.

MM in the Application layer

Mobility Management (MM) schemes are possible in three different layers of the OSI protocol layer model:

Application layer
...
...
Transport layer
Network layer
Data link layer
Physical layer

SIP (or other application layer solutions):

No seamless handovers as such...

However, the terminal can be reached from the outside network, like with Mobile IP.

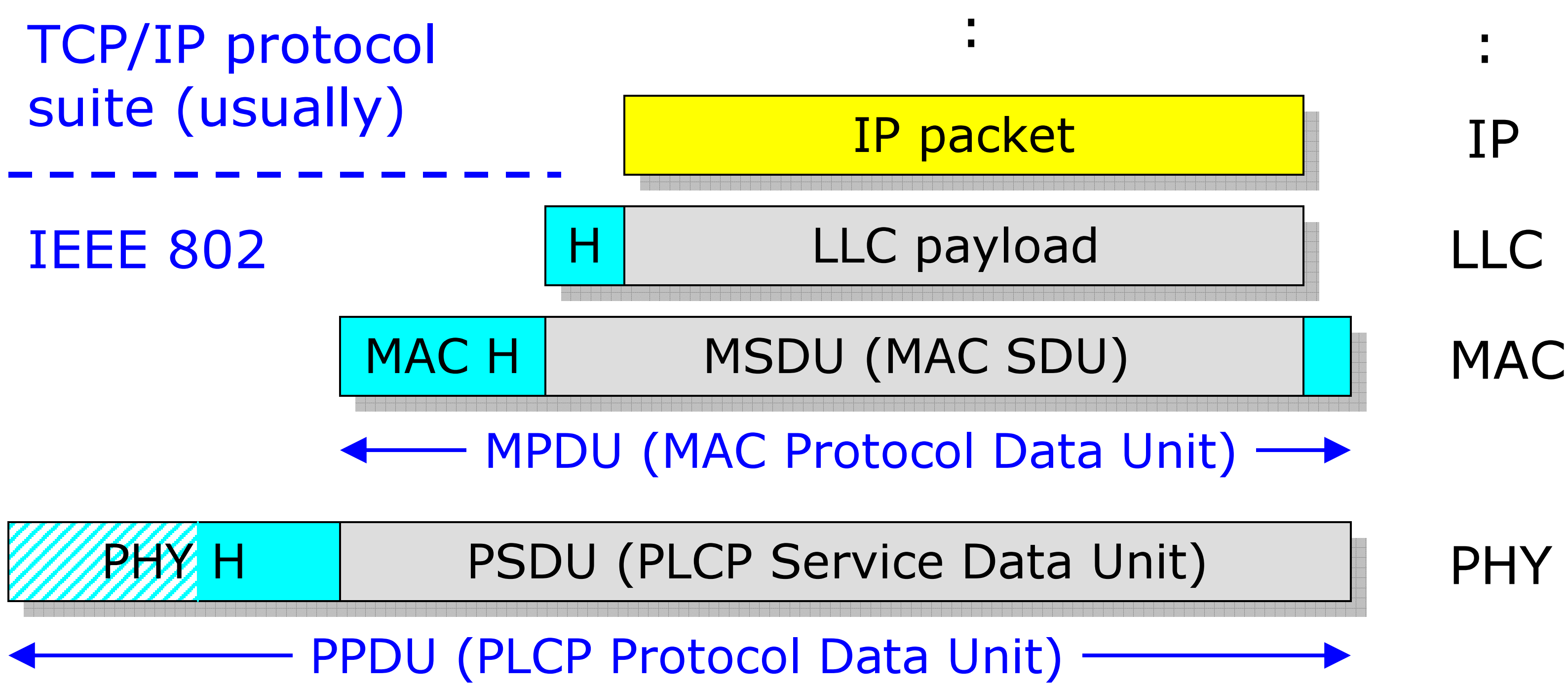
Mobility management summary

Within a WLAN, handovers are possible (based on IAPP + proprietary solutions in equipment), but there is no IEEE-supported reachability solution available.

Handovers between different WLANs require Mobile IP (which offers also reachability). Unfortunately, Mobile IP includes a non-transparent mechanism (Discovering Care-of Address) that must be implemented in all APs.

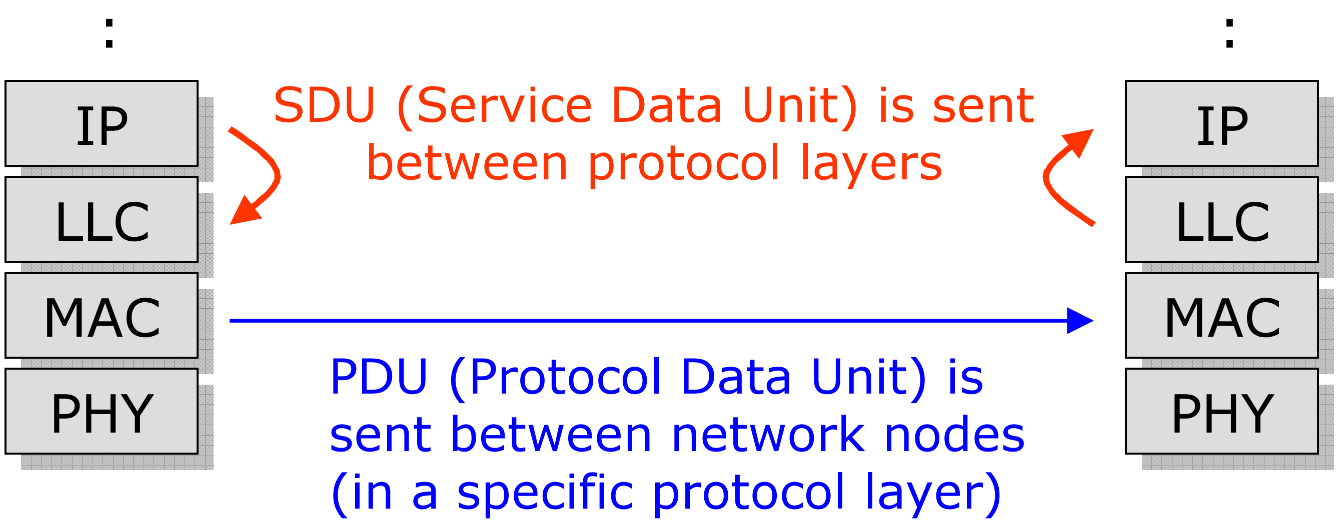
Global reachability of wireless stations can be achieved using SIP or similar Application layer concepts. SIP does not require changes to APs.

IEEE 802.11 frame structure

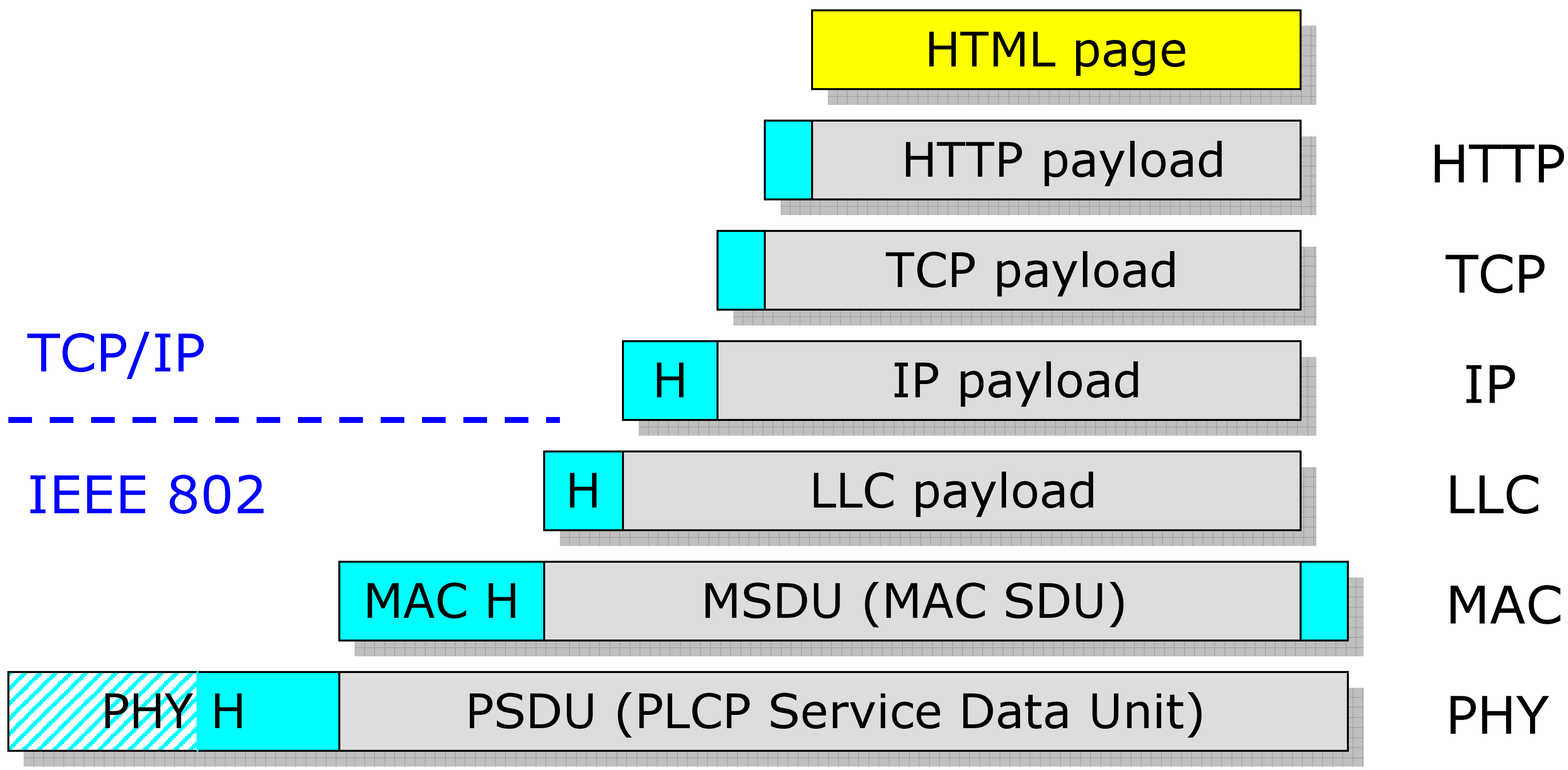


PDU vs. SDU

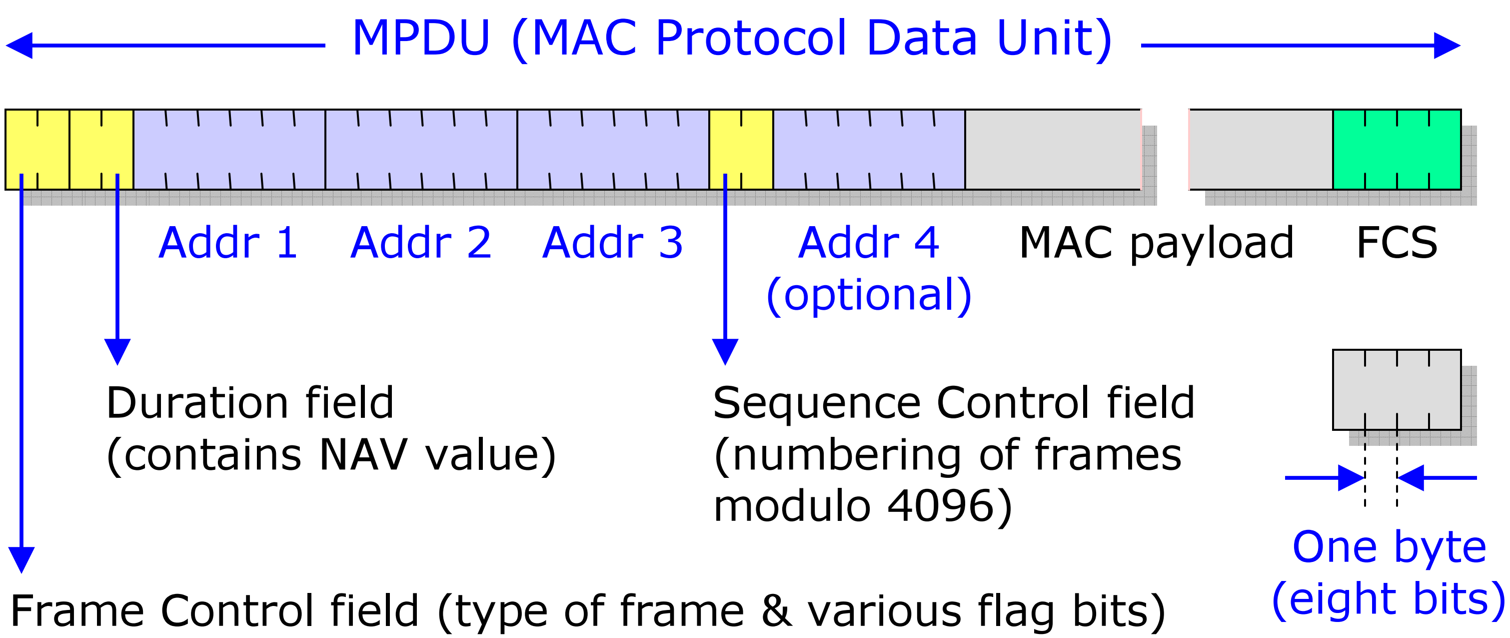
Payload of a PDU in layer N = SDU to/from the layer N+1



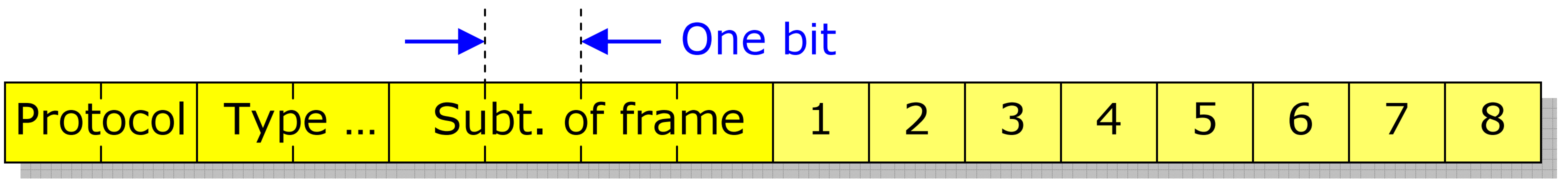
Overall frame structure (application = HTML)



MAC header structure



Content of Frame Control field

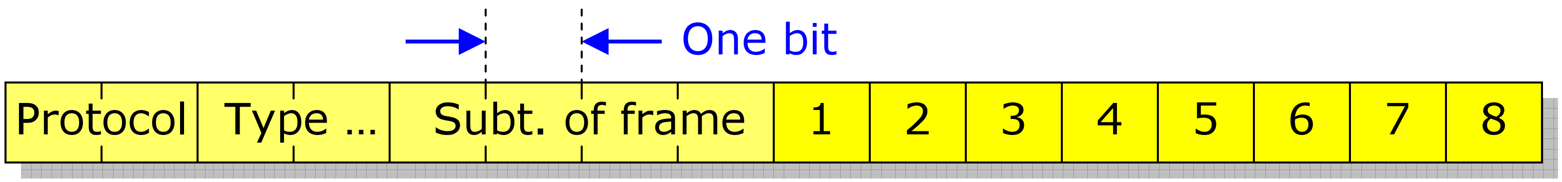


Protocol: Indicates IEEE 802.11 MAC

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

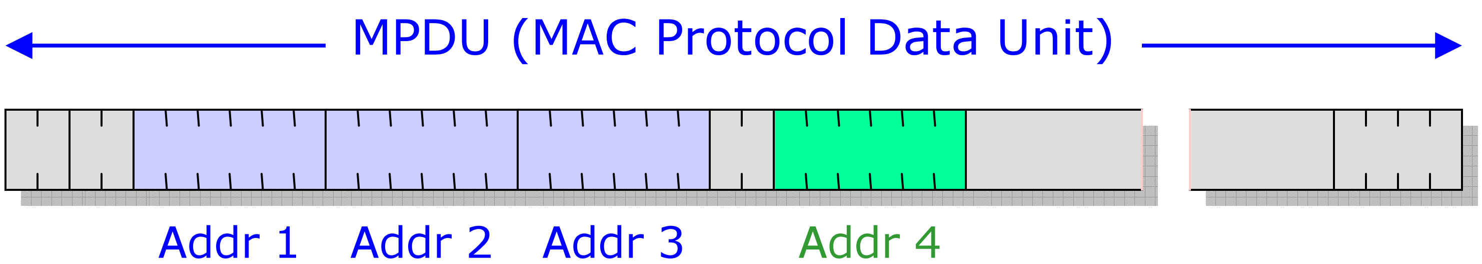
Subtype of frame: Describes type of management, control, or data frame in more detail (e.g. ACK => 1101)

Flags in Frame Control field



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

Usage of MAC address fields

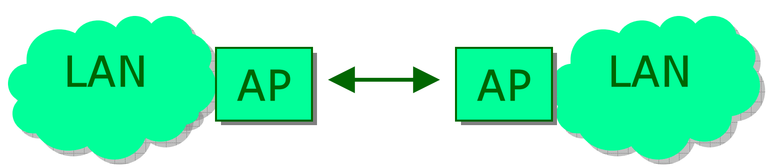


Address 1: Receiver (wireless station or AP)

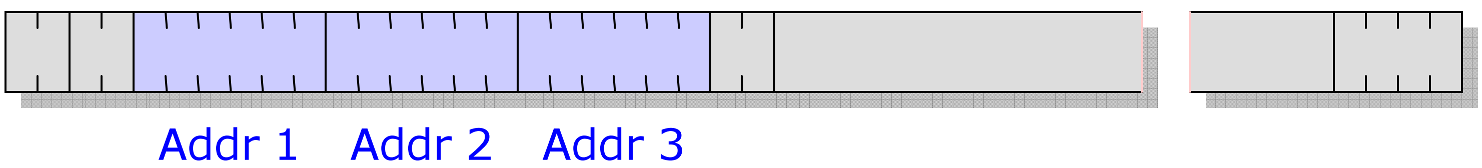
Address 2: Sender (wireless station or AP)

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

Address 4: Only used in Wireless Bridge solutions:



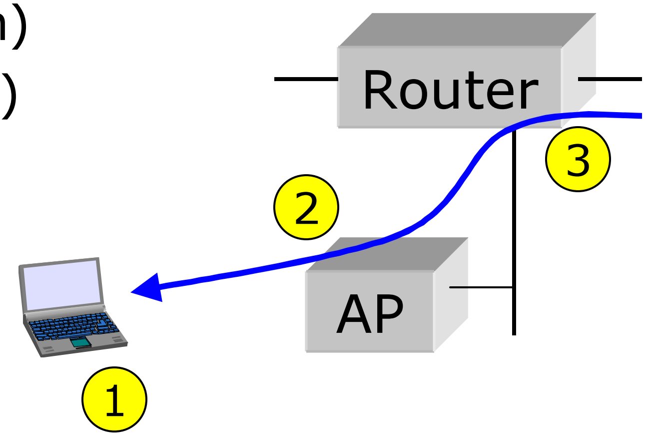
Direction: AP => wireless station



Addr 1: Receiver (wireless station)

Addr 2: Transmitter = BSSID (AP)

Addr 3: Ultimate source (router)

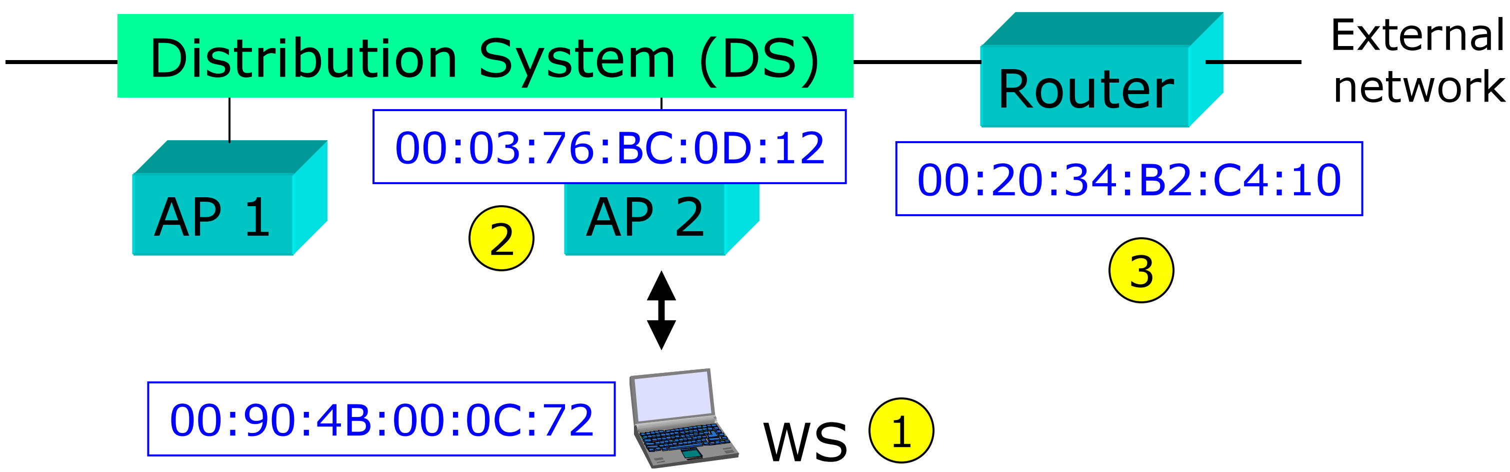


BSSID: MAC address of AP

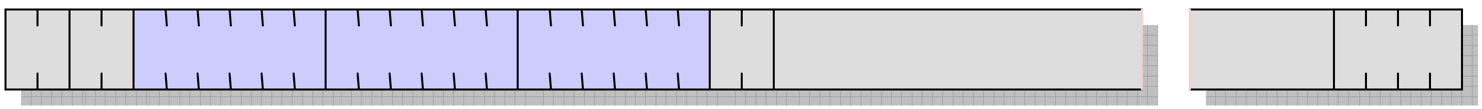
SSID: Alphanumeric name of AP (or BSS)

MAC addressing example

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

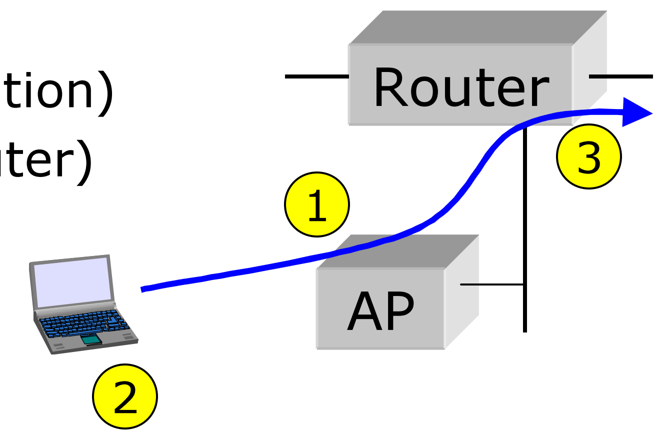


Direction: Wireless station => AP



Addr 1 Addr 2 Addr 3

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



Management frames

In addition to the data frames (containing the user data to be transported over the 802.11 network) and control frames (e.g. acknowledgements), there are a number of management frames.

Note that these management frames compete for access to the medium in equal terms (using CSMA/CA) with the data and control frames.

Some of these management frames are presented on the following slides.

Beacon frames

Beacon frames are broadcast (mening that all stations shall receive them and read the information) at regular intervals from the Access Point. These frames contain (among others) the following information:

- Timestamp (8 bytes) is necessary, so that stations can synchronise to the network
- Beacon interval (2 bytes) in milliseconds
- Capability info (2 bytes) advertises network capabilities
- SSID (0 ... 32 bytes), alphanumeric “network name”
- The channel number used by the network (optional).

Probe request & response frames

A probe request frame is transmitted from a wireless station during active scanning. Access points within reach respond by sending probe response frames.

Probe request frames contain the following information:

- SSID (0 ... 32 bytes), alphanumeric "network name"
- Bit rates supported by the station. This is used by APs to see if the station can be permitted to join the network.

Probe response frames actually contain the same kind of "network information" as beacon frames.

Association request & response frames

Before a station can join an 802.11 network, it must send an association request frame. The AP responds with an association response frame.

Association request frames contain (among others):

- SSID, capability info, bit rates supported.

Association response frames contain (among others):

- Capability info, bit rates supported
- Status code (success or failure with failure cause)
- Association ID (used for various purposes)

Passive and active scanning

Wireless stations can find out about 802.11 networks by using passive or active scanning.

During passive scanning, the station searches beacon frames, moving from channel to channel through the complete channel set (802.11b => 13 channels).

During active scanning, the station selects Channel 1 and sends a probe request frame. If no probe response frame is received within a certain time, the station moves to Channel 2 and sends a probe request frame, and so on.

Case study 1: Station connecting to a WLAN

When a station moves into the coverage area of a WLAN, the following procedures take place:

1) Scanning: the station searches for a suitable channel over which subsequent communication takes place

2) Association: the station associates with an AP

3) IP address allocation: the station gets an IP address, for instance from a DHCP server

4) Authentication: only if this security option is required.

Case study 2: Handover to another AP

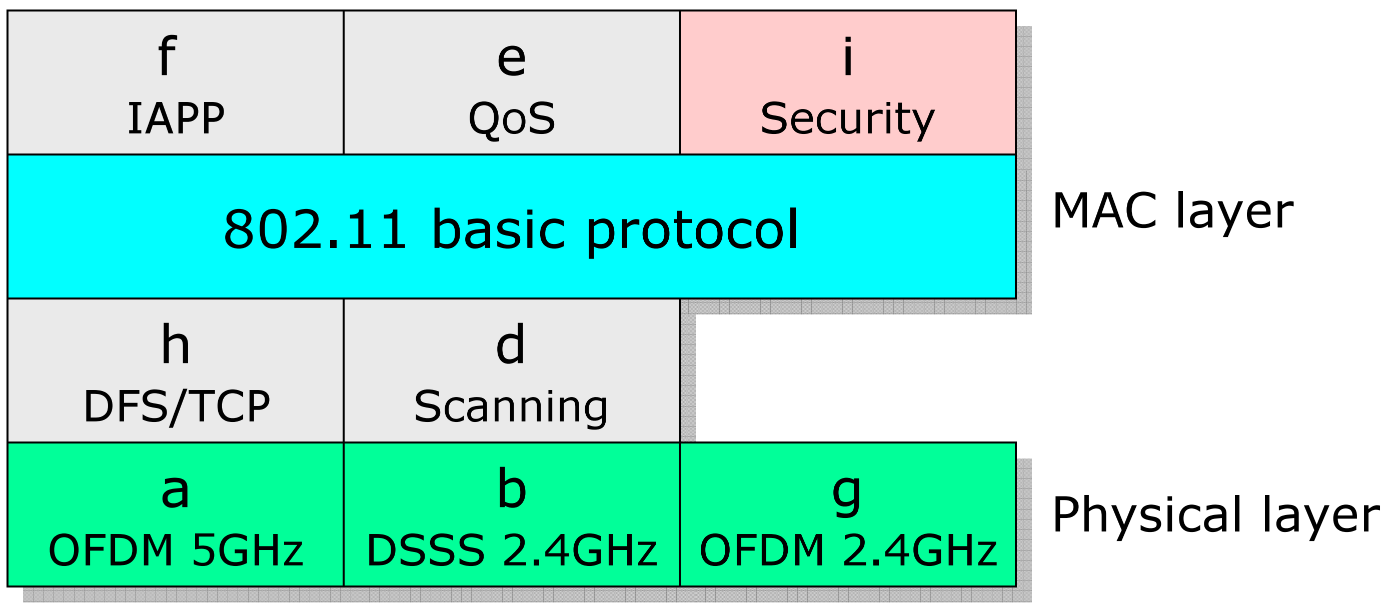
When a station has noticed that the radio connection to another AP is a better than the existing connection:

1) Reassociation: the station associates with another AP

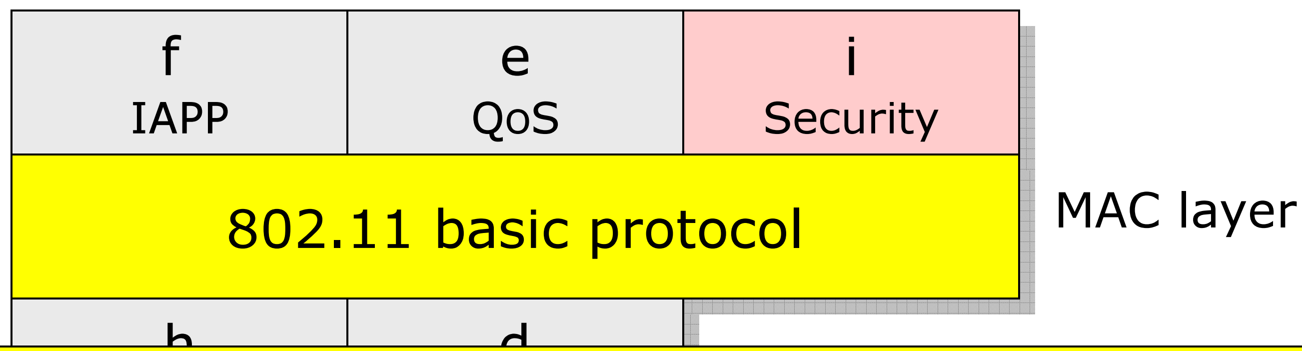
2) No new IP address is needed; however, the WLAN must be able to route downlink traffic via the new AP

3) Authentication: this security option, if required, will result in a substantially increased handover delay (complete procedure sequence: deauthentication, disassociation, reassociation, authentication).

Some IEEE 802.11 standard amendments

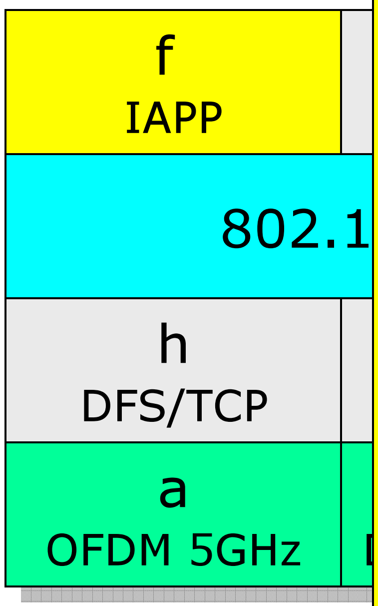


IEEE 802.11 basic protocol



Since the 802.11 standard is ”frozen”, additions must be specified in various amendments. Many of these are still in the draft phase.

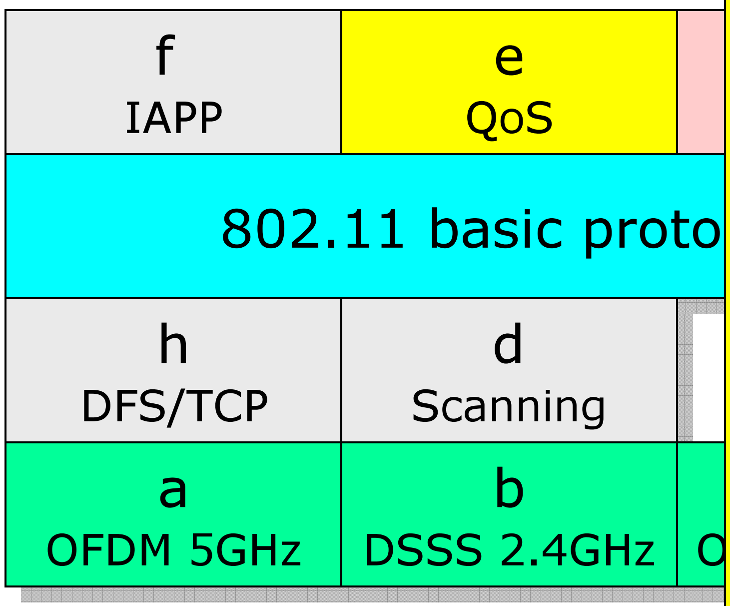
IEEE 802.11f



The objective: to specify the Inter-Access Point Protocol (IAPP) that enables seamless roaming between different Access Points within an ESS.

Note: 802.11f is not concerned with roaming between ESS networks. For this purpose, non-802.11 solutions must be used.

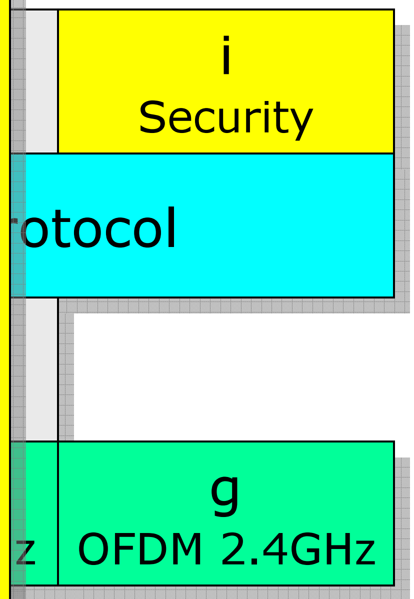
IEEE 802.11e



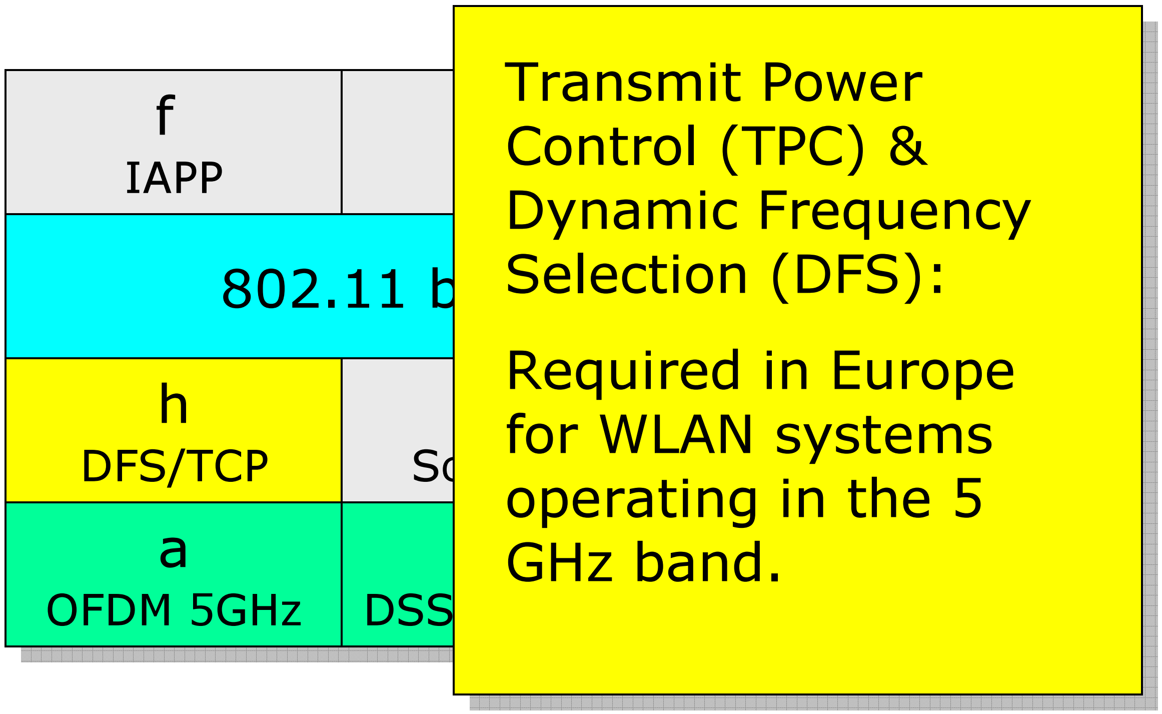
Quality of Service (QoS) for better handling of voice traffic, by finding ways of minimizing jitter and delay variations and maximising access point throughput.

IEEE 802.11i

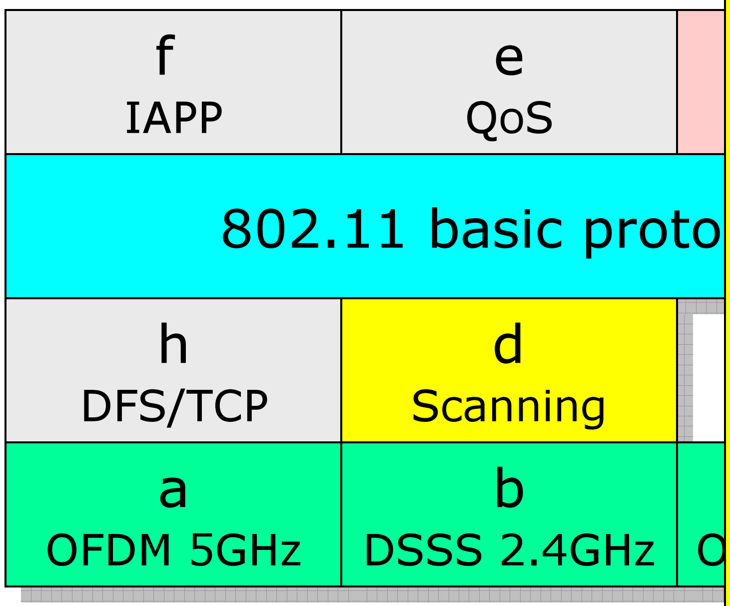
Security issues such as TKIP (Temporary Key Integrity Protocol) e.g. for improved key management, and 802.1x for authentication (note: can also be used in wired LAN).



IEEE 802.11h


f
IAPP
802.11 b
h
DFS/TCP
Sc
a
OFDM 5GHz
DSS
Transmit Power Control (TPC) & Dynamic Frequency Selection (DFS):
Required in Europe for WLAN systems operating in the 5 GHz band.

IEEE 802.11d



802.11d supplements the MAC layer to promote worldwide usage of 802.11 networks (through further development of active & passive scanning schemes).