802.11 Framing in Detail

S-72.333, Postgraduate Course in Radio Communications

Juha Villanen, Radiolaboratory

Email: juha.villanen@hut.fi

Outline

- Introduction
- Contention-based/Contention-free service
- 802.11 addressing
- Data frames
- Control frames
- Management frames
- Contention-free service

Introduction

- Due to the wireless interface, 802.11 framing much more complicated than e.g. Ethernet framing
- Virtual carrier sensing implemented in two different ways: contention-based and contention-free
- In 802.11, three frame types exist:
  - Data frames
  - Control frames
  - Management frames

Contention-based/Contention-free

- Virtual carrier sensing in 802.11: contention-based and contention-free methods
  - *Contention-based*:
    - Stations manage ”independently” access to the medium; no central control!
    - Medium restricted for the time specified by NAV: if NAV > 0 ⟹ wait
  - *Contention-free*:
    - Centralized control method (Point Coordinator)
    - Near real-time, ”fair” access to the medium
    - Polling frame ⟹ licence to transmit (polling list)

802.11 adressing

- Up to four different address fields for variety of purposes:
  - Source address
  - Transmitter address
  - Receiver address
  - Destination address
  - Basic Service Set ID (BSSID)
    - Infrastructure BSS: MAC address of the infrastructure network access point (AP)
    - Independent BSS (IBSS): Random 46 bit BSSID

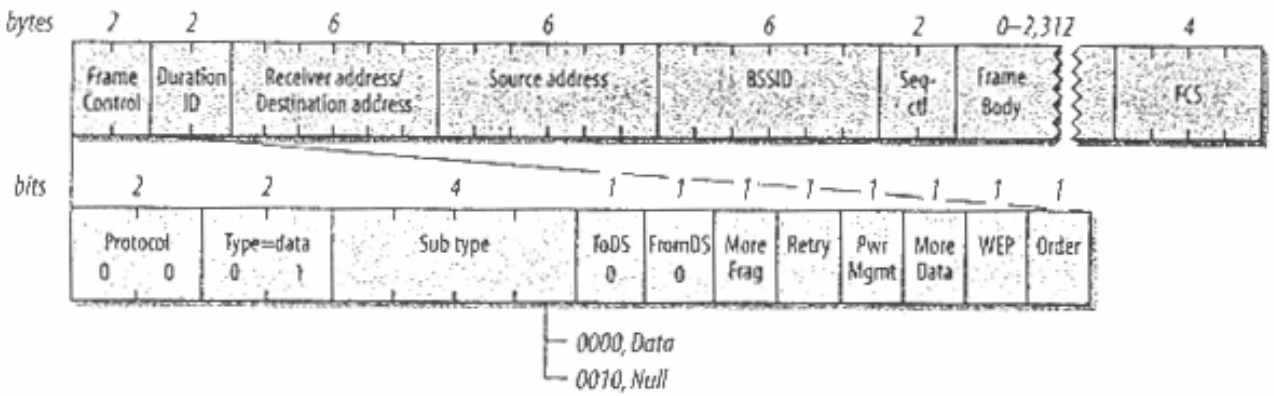
Data frames, generic

- Main taks: carry higher level protocol data
- Generic data frame structure

- The number and function of the address field depends on the type of the network (defined by the ToDS and FromDS-bits in the Frame Control field):
  - IBSS (Independent Basic Service Set), Ad Hoc
  - To Access Point (AP)
  - From Access Point (AP)
  - Wireless Distribution System (WDS), Wireless Bridge

Data frames, IBSS

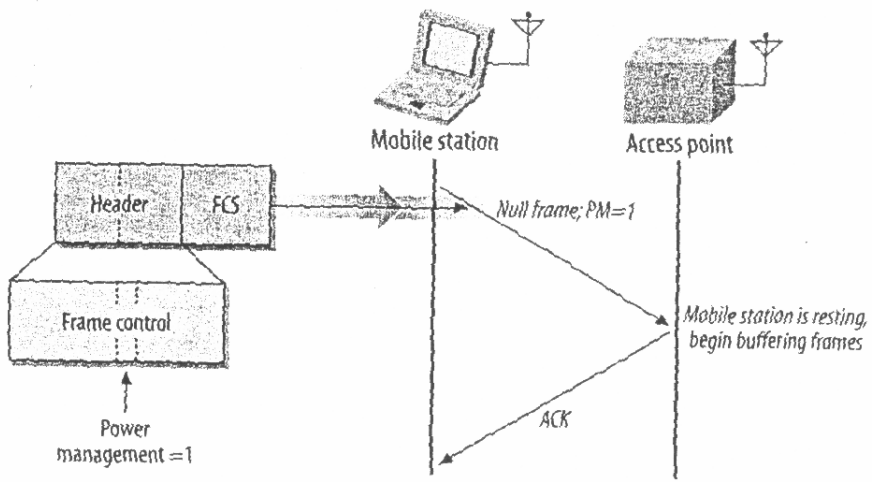
- No distribution systems and access points. Frame structure:



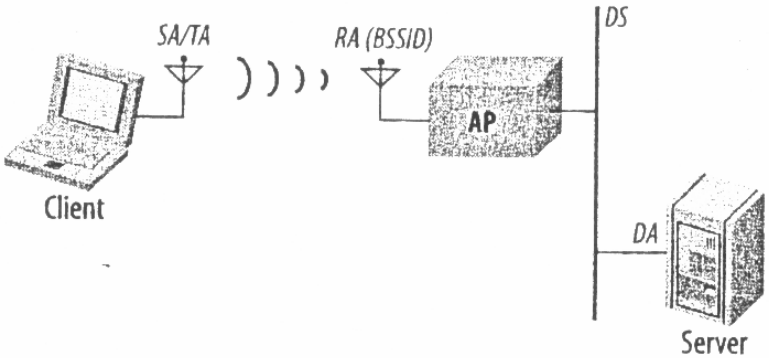
- Transmitter = source **and** receiver = destination
- Only messages with the clients current BSSID are passed to the higher protocol layers (filtering)

Data frames, IBSS cont.

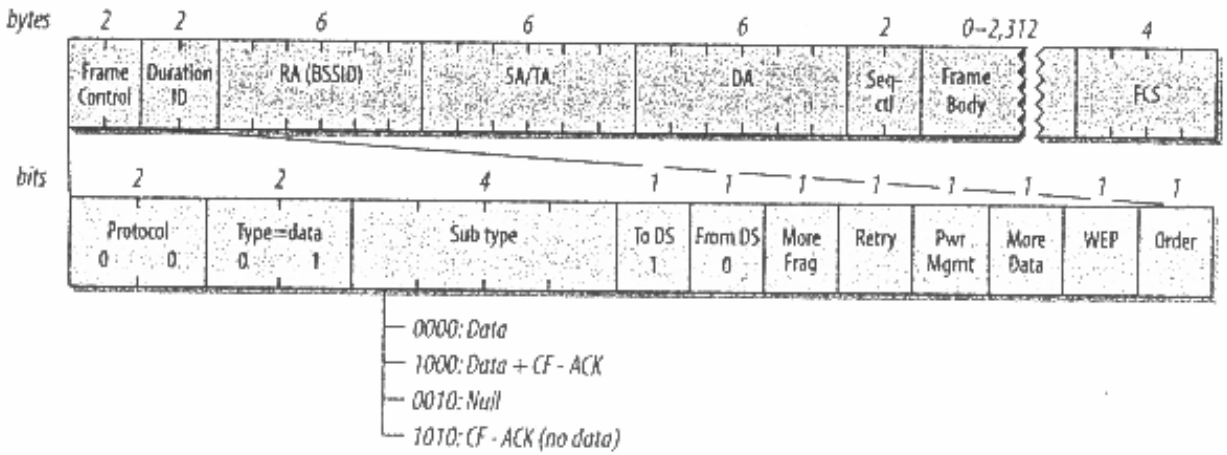
- Two data frame types
  - *Data*: Moving frame body from station to station. Transmitted only during contention based access periods.
  - *Null:* Just MAC header + FCS. No frame body. Used to inform access points of changes in power saving status (power management bit)



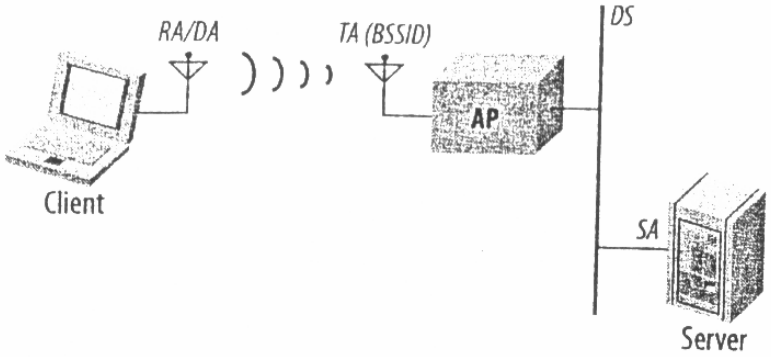
Data frames, to Access Point



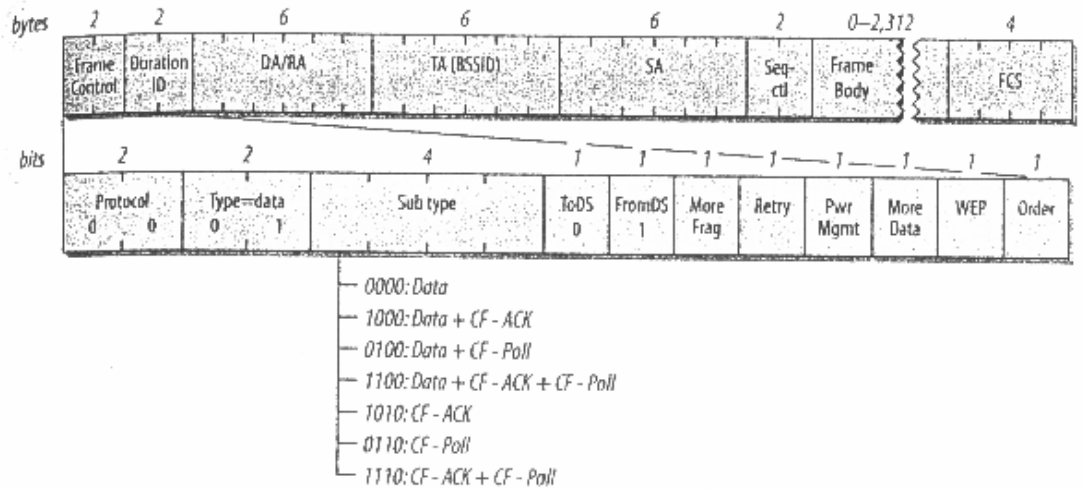
- Transmitter = source **but** receiver ≠ destination
- AP's use the third address (DA) to forward the frames



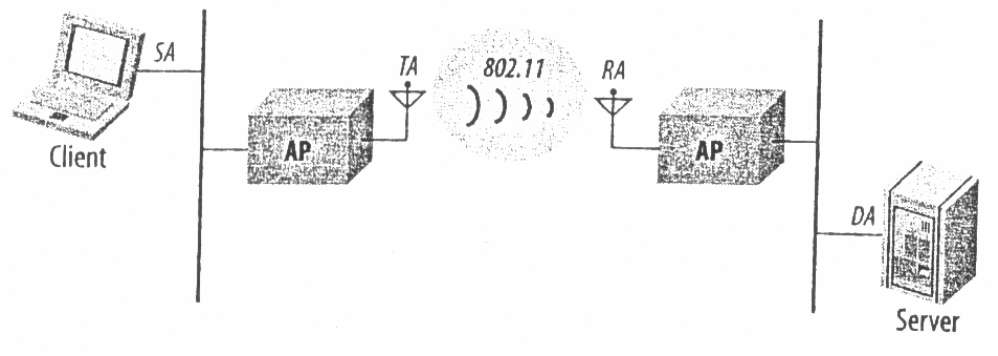
Data frames, from Access Point



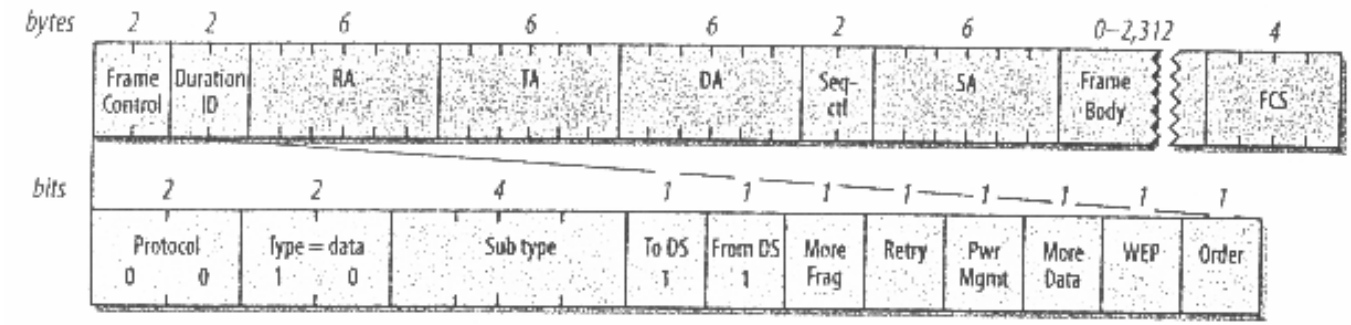
- Transmitter ≠ source **but** receiver = destination
- AP's don't need power saving ⇒ no null frames



Data frames, WDS – wireless bridge



- Transmitter ≠ source **and** receiver ≠ destination
- Usually no mobile stations ⟹ contention-free period not used. Power management bit always 1.

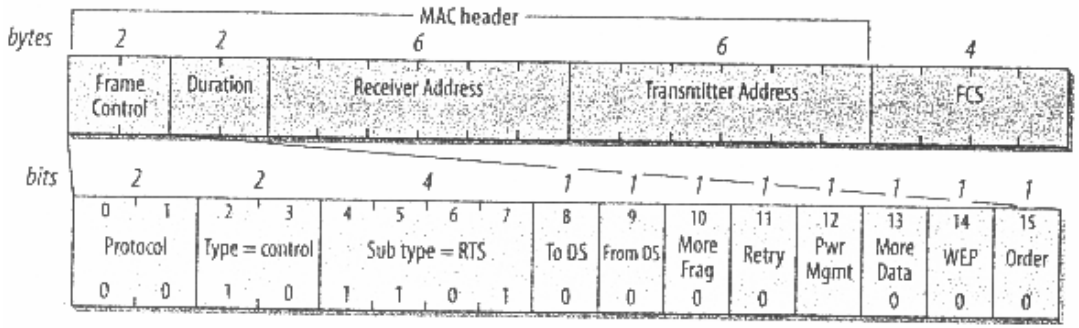


Control frames

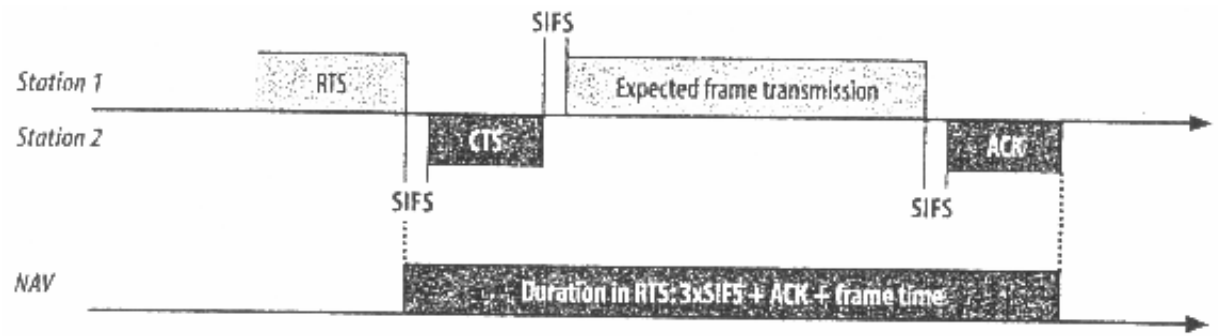
- Administration of the access to the wireless medium
- MAC-layer reliability functions
- Control frame types:
  - *Request to send (RTS)*
  - *Clear to Send (CTS)*
  - *Acknowledgement (ACK)*
  - *Power-save Poll (PS-Poll)*

Control frames, RTS

- Used to gain control of the medium for transmission of large frames
- No data transmitted in the body:

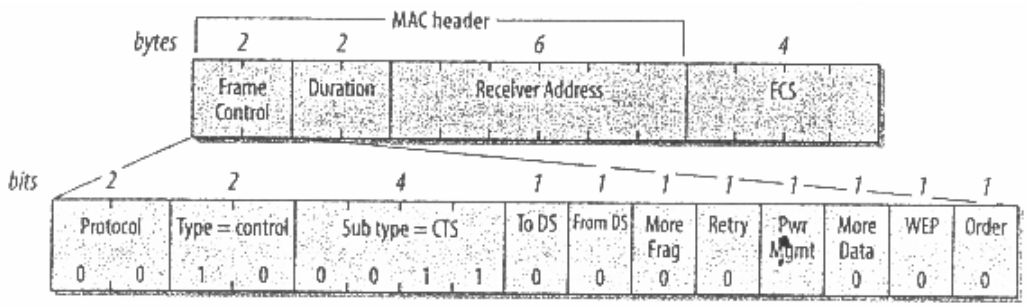


- NAV: 3xSIFS + ACK + frame time:

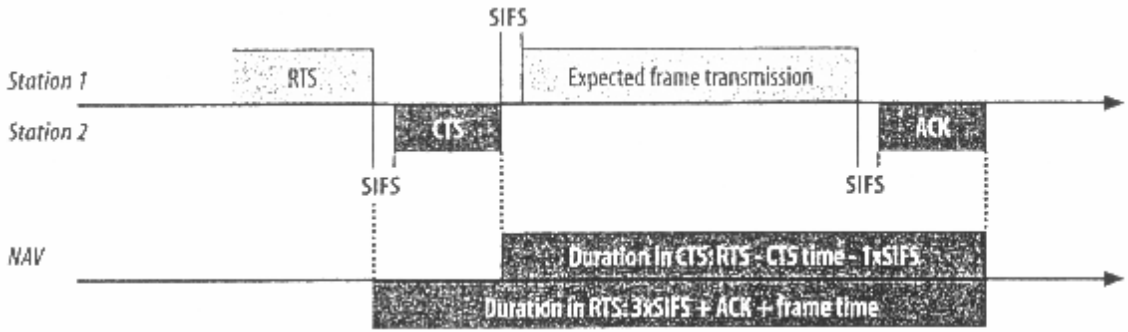


Control frames, CTS

- Used to answer for the RTS frame
- The transmitter address of the RTS frame copied into the receiver address:

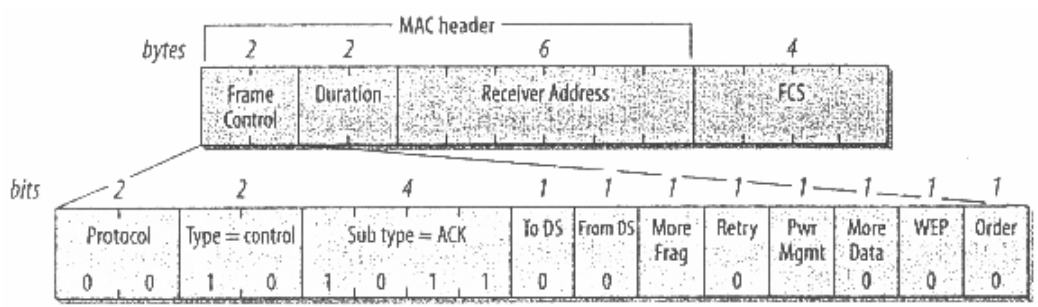


- NAV: Duration in RTS – CTS time – 1xSIFS

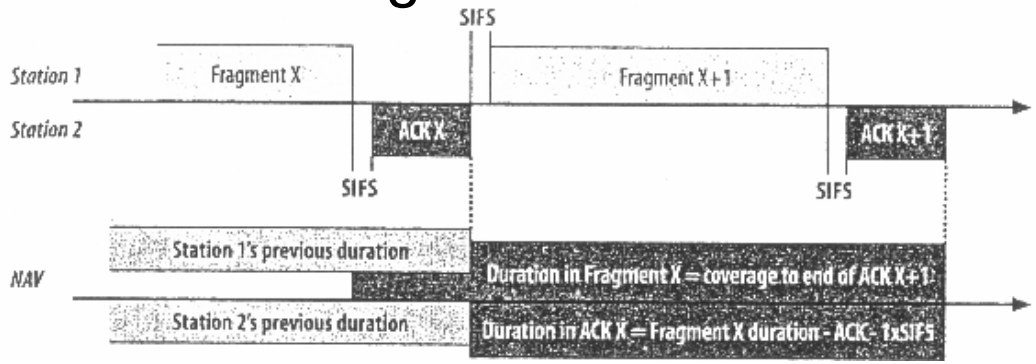


Control frames, ACK

- Used to acknowledge all data transmission
- Receiver address copied from the frame being acknowledged:

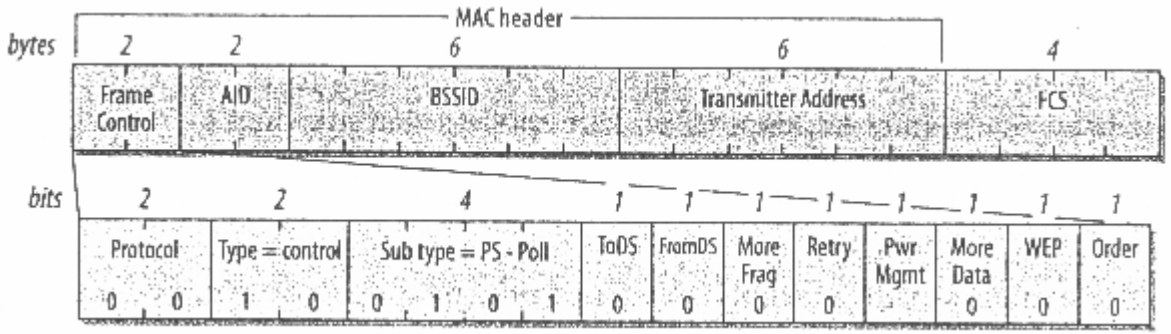


- *CASE1*: Final fragment or complete frame ⟹ NAV = 0
- *CASE2*: More fragments bit = 1 ⟹ NAV like in CTS



Control frames, PS-Poll

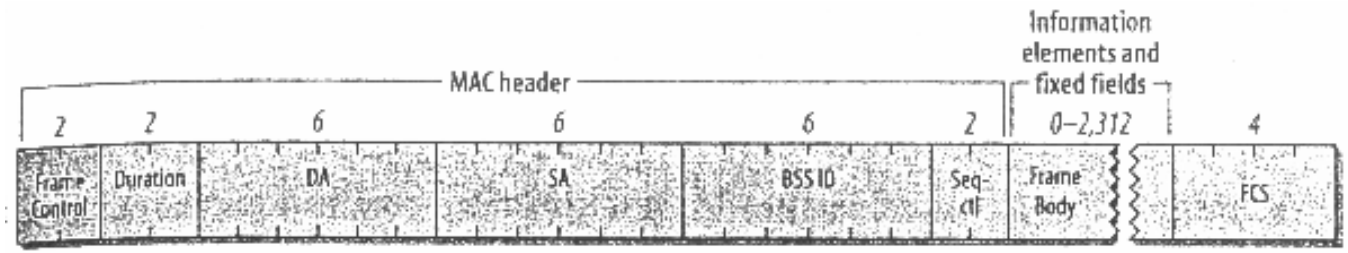
- Transmitted when MS wakes from power-saving mode ⇨ retrieval of buffered frames from AP.
- AID (Association ID) instead of a Duration field:



- For each MS within the range of some AP, an AID is assigned. Used by AP to find the frames buffered for the specified MS.
- All stations receiving a PS-Poll frame update the NAV in the following way: NAV = SIFS + ACK

Management frames

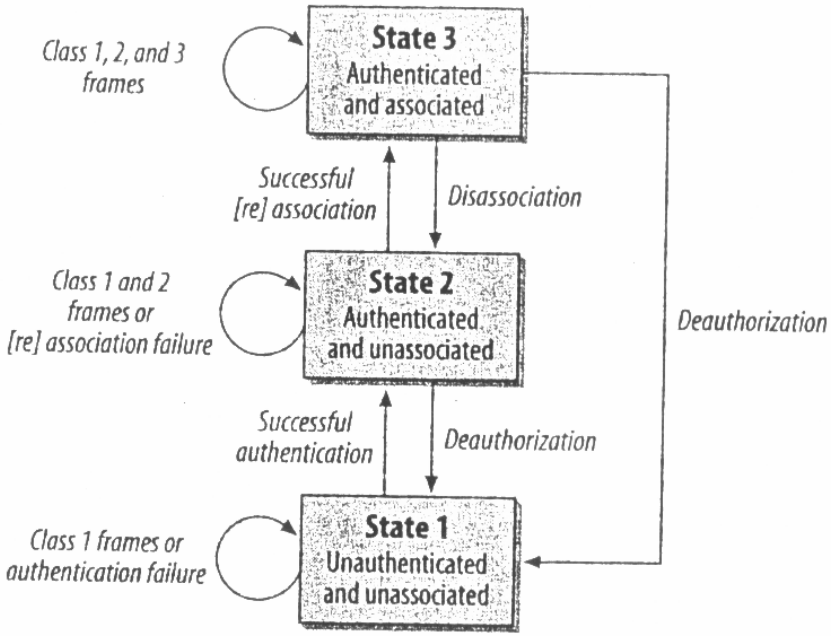
- BSSID used to filter out frames associated with other Access Points.
- Frame body: *fixed fields* and *information elements*
- The generic management frame structure:



- The three main management functions:
  1. Searching of a compatible wireless network
  2. Authentication of the MS
  3. Association of an MS with some AP

Management frames, cont

- MS's have three allowed states
  1. Initial state; not authenticated, not associated
  2. Authenticated but not associated
  3. Authenticated and associated



- 802.11 frames divided into three classes. Frame class restricts the use of frames into certain states.

Management frame types

- Different management frame types:
  - *Beacon*
  - *Probe Request*
  - *Probe Response*
  - *IBSS Announcement Traffic Indication Map (ATIM)*
  - *Disassociation and Deauthentication*
  - *Association Request*
  - *Reassociation Request*
  - *Association Response and Reassociation Response*
  - *Authentication*

Management frame types, cont.

- *Beacon*:
  - Are transmitted at regular intervals to allow MS's to find and identify networks + match parameters with the AP.
  - AP of an infrastructure network responsible

    for transmission of beacons
- *Probe Request*:
  - Used by MS's to scan an area for existing 802.11 networks
  - AP's use probe request to determine whether the MS can join the network. *RULE:* MS must support all the data rates supported by the network

Management frame types, cont.

- *Probe Response*:
  - If the parameters of MS compatible ⇒ AP sends a Probe Response frame
  - Station that send the last Beacon is responsible for sending a Probe Response
  - Parameters same than in the Beacon frame
- *Authentication:*
  - Used to authenticate to an Access Point
  - Different authentication algorithms exist
  - May take several steps ⇒ a sequence number in the frames

Management frame types, cont.

- *Association Request:*
  - MS indentified a compatible network and authenticated to it ⇨ MS joins the network by sending a Association Request frame
- *Reassociation Request*:
  - Needed when MS temporarily leaves the coverage area of an AP or when MS moves between two APs of some basic service area
- *Association Response and Reassociation Response:*
  - Transmitted by AP in response to Association Request or Reassociation Request. Association ID (AID) assigned

Management frame types, cont.

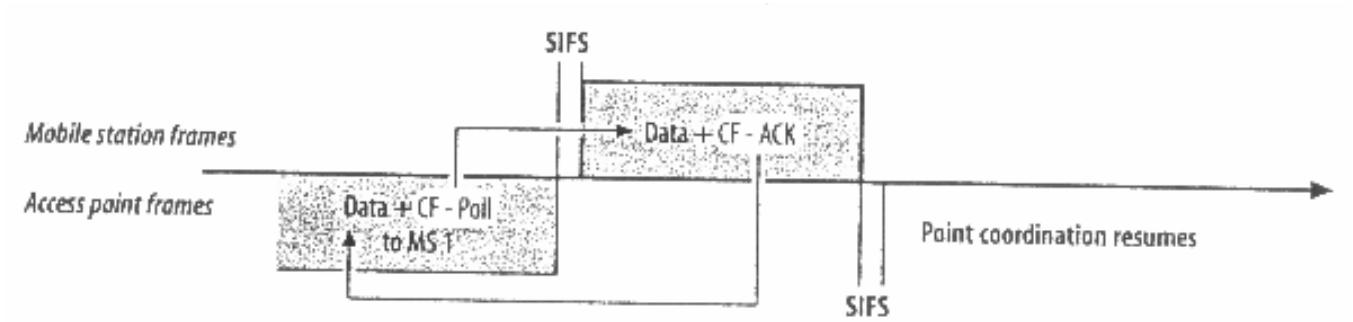
- *Disassociation and Deauthentication*:
  - Used to end an association or authentication relationship.
  - Both frames include the so-called Reason Code to indicate what the MS has done incorrectly
- *IBSS Announcement Traffic Indication Map (ATIM)*:
  - No access points in IBSSs ⇨ announcements of buffered data has to be handled somehow
  - ATIM used to notify the recipient it has buffered data

Contention-free service

- Refresher:
  - Centralized control method (Point Coordinator)
  - Efficient, ”fair” access to the medium
  - Polling list of priviledged stations
  - Polling frame ⇨ licence to transmit
- Frames in the contention-free service can combine data transmission, acknowledgements and polling
- Different frame types:

Contention-free frame types

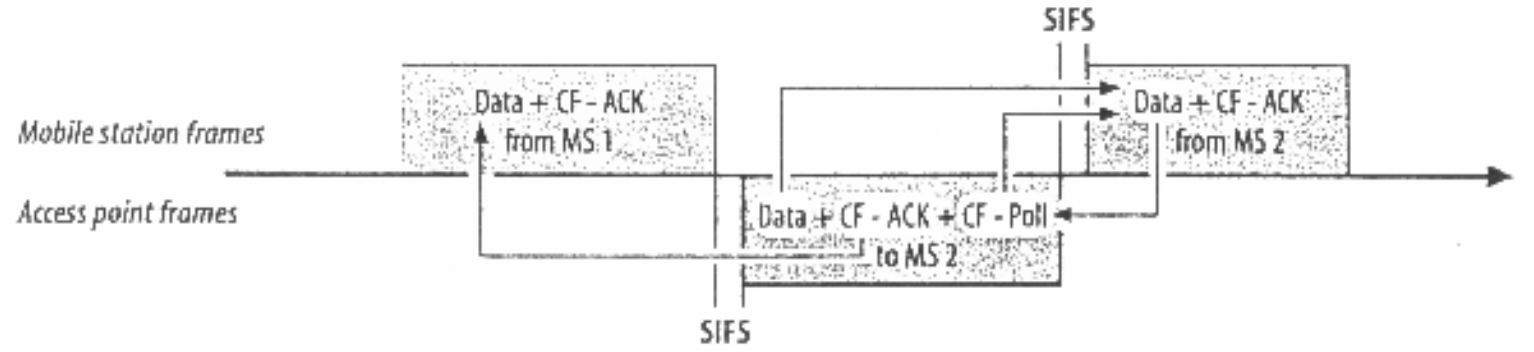
- *Data+CF-Poll:*
  - Sent by an Access Point to MS
  - Permission for MS to transmit one frame
  - Data must be intended for the recipient
  - *CF-Poll* frame when no data to transmit



- *Data+CF-Ack:*
  - Data and Acknowledge intended for separate stations
  - *CF-Ack* frame when no data to transmit

Contention-free frame types, cont.

- *Data+CF-Ack+CF-Poll:*
  - Sent by an Access Point to MS
  - Data and Polling must be intended for the same MS
  - Acknowledge for the previous transmission
  - *CF-Ack+CF-Poll* frame when no data to be transmitted for Mobile Station

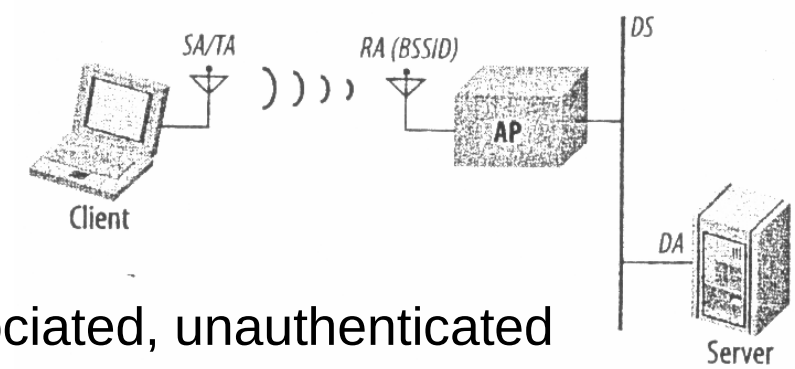


Contention-free frame types, cont.

- *CF-End:*
  - When the contention-free period ends
  - Release of the Mobile Stations from contention-free period access rules and begin of contention-based service
- *CF-End:*
  - Same as *CF-End* but receipt of previous frame is acknowledged simultaneously

Homework

- Consider the following arrangement:



- At the beginning, client is unussociated, unauthenticated and do not know about the existence of the network. The following steps occur (contention-based service):

  1. Client performs the required Management frame handshaking with the Access Point (AP)
  2. Client wants to send data (in single fragment) to the Server
  3. Client leaves the network

- List the types of the frames (in the order of appearance) transmitted in the wireless medium. Describe briefly the purpose of each transmitted frame.

Thank You!

Questions?