IEEE 802.11 Wireless LAN Standard : MAC

CS-1699 Wireless Networks
Term : Spring 2018

Instructor : Xerandy

Important Terms

	Remarks
Access Point	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic Service Set	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive frames
Distribution System	A system used to interconnect a set of BSS and integrated LANs to create an ESS
Extended service set	A set of one or more interconnected BSS and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer entities using the service of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE802.11 conformant MAC and physical layer

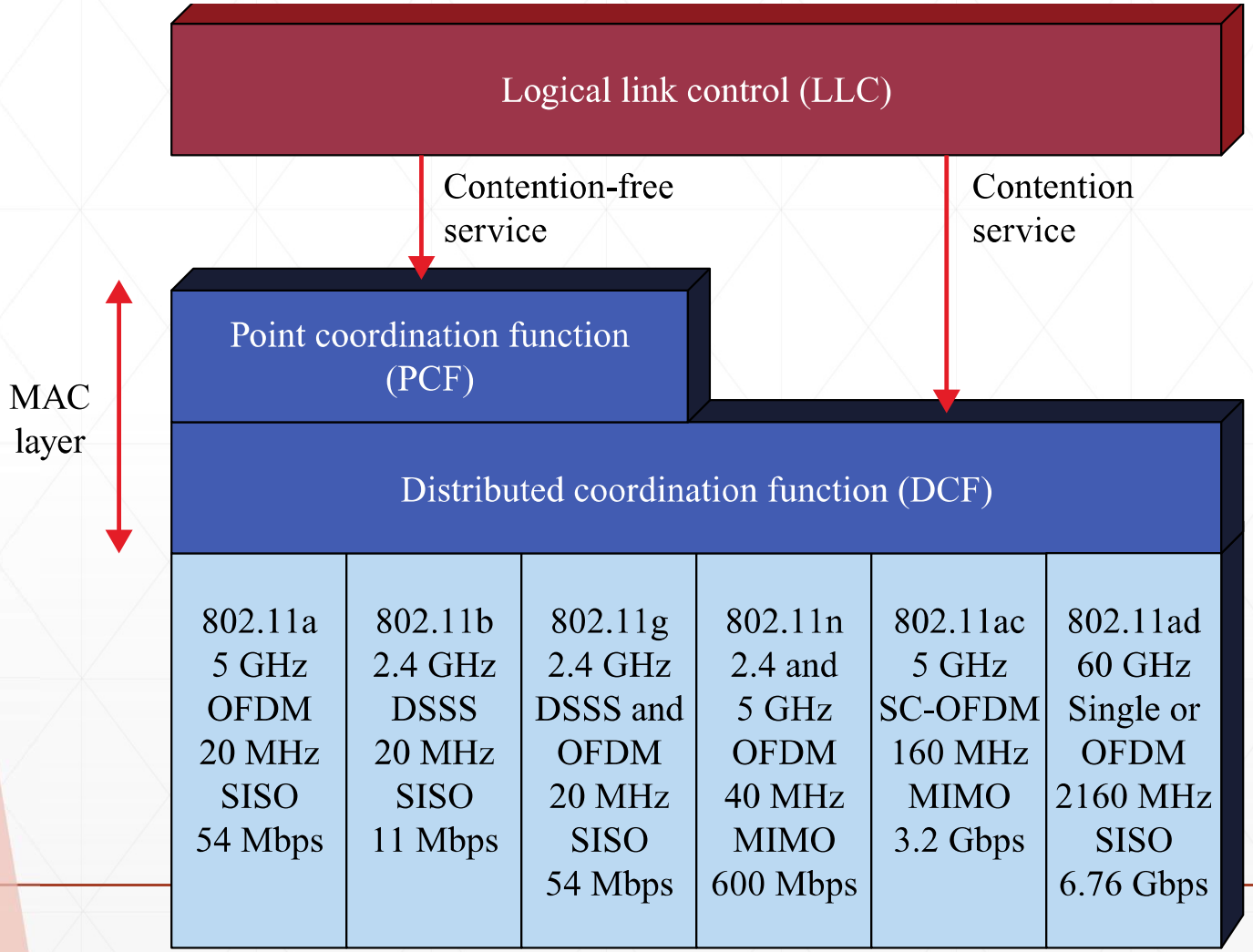
IEEE 802.11 Medium Access Control

- MAC layer covers three functional areas:
  - Reliable data delivery
  - Access control
  - Security
- Reliable Data Delivery
  - More efficient to deal with errors at the MAC level than higher layer (such as TCP)
  - Frame exchange protocol
    - Source station transmits data
    - Destination responds with acknowledgment (ACK)
    - If source doesn‘t receive ACK, it retransmits frame
  - Four frame exchange
    - Source issues request to send (RTS)
    - Destination responds with clear to send (CTS)
    - Source transmits data
    - Destination responds with ACK

IEEE 802.11 Access Control

- Centralized and decentralized mechanisms together
  - Distributed foundation wireless MAC (DFWMAC)
  - Distributed coordination function (DCF)
    - Decentralized
  - Point coordination function (PCF)
    - Centralized
  - Both are available to the LLC layer

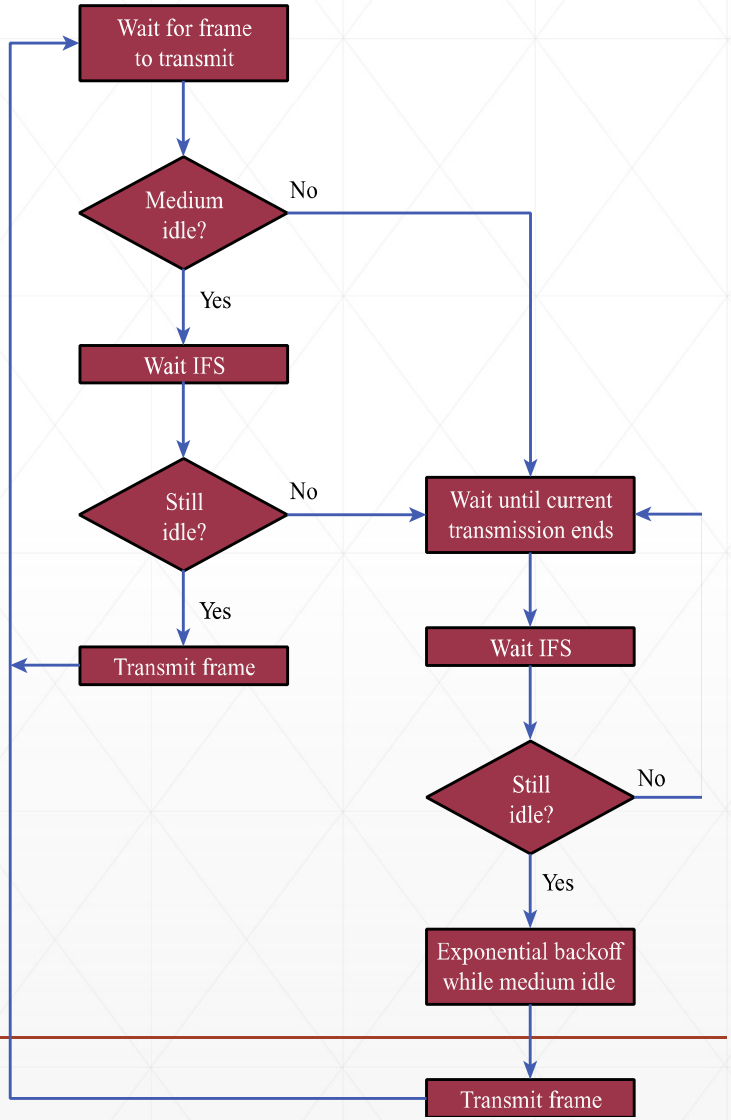
IEEE 802.11 Access Control



IEEE 802.11 : Distributed Coordination Function

- Decentralized
- Carrier sense multiple access (CSMA)
  - Listen to the medium
  - If idle, then transmit
  - If not, wait a random time
    - If busy again, expand the mean waiting time, randomly wait, and try again.
  - *Binary exponential backoff* describes this procedure
    - The backoff is the waiting process
    - Mean random waiting times get exponentially larger
      - By a factor of 2 each time, hence the term *binary*.
  - This process responds to heavy loads
    - Since nodes do not know the loads of other nodes trying to send.

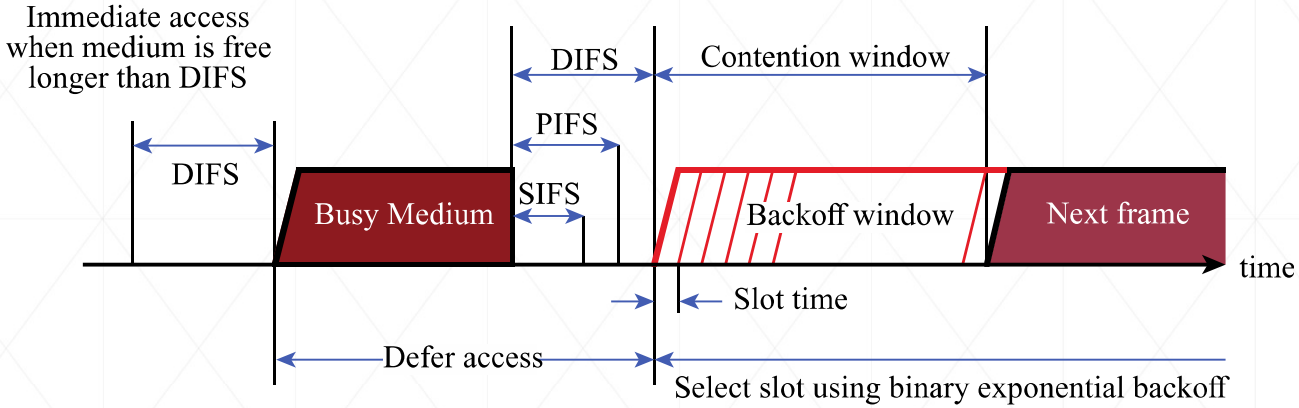
IEEE 802.11 Medium Access Control Logic



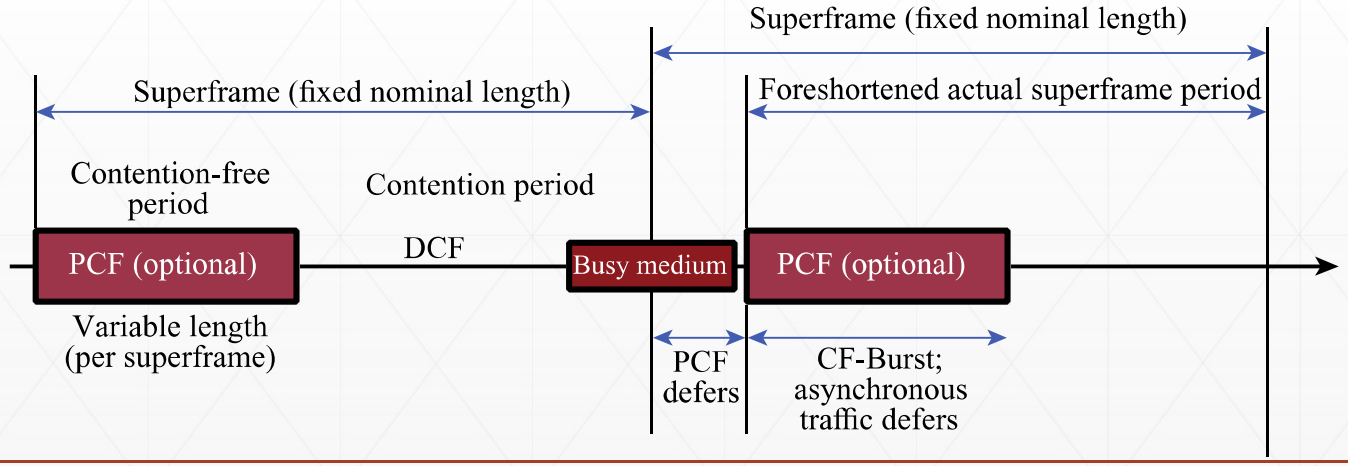
IEEE 802.11 : Interframe Space (IFS) Values

- Short IFS (SIFS)
  - Shortest IFS
  - Used for immediate response actions, such as ACK, Poll response, CTS
- Point coordination function IFS (PIFS)
  - Mid-length IFS
  - Used by centralized controller in PCF scheme when using polls
- Distributed coordination function IFS (DIFS)
  - Longest IFS
  - Used as minimum delay of asynchronous frames contending for access

IEEE 802.11 (IFS) MAC Timing



(a) Basic access method

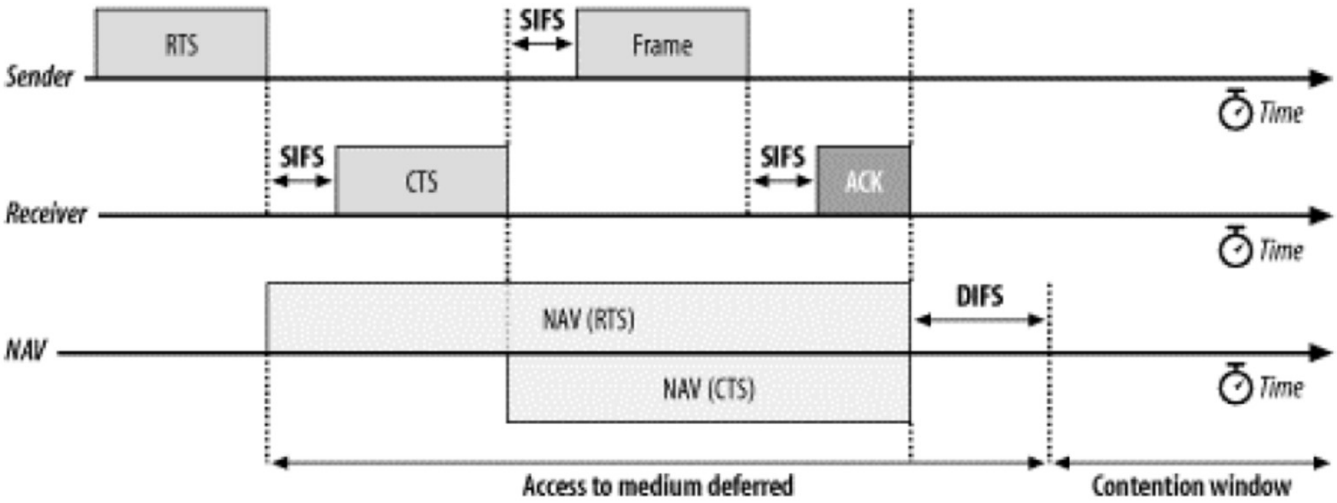


(b) PCF superframe construction

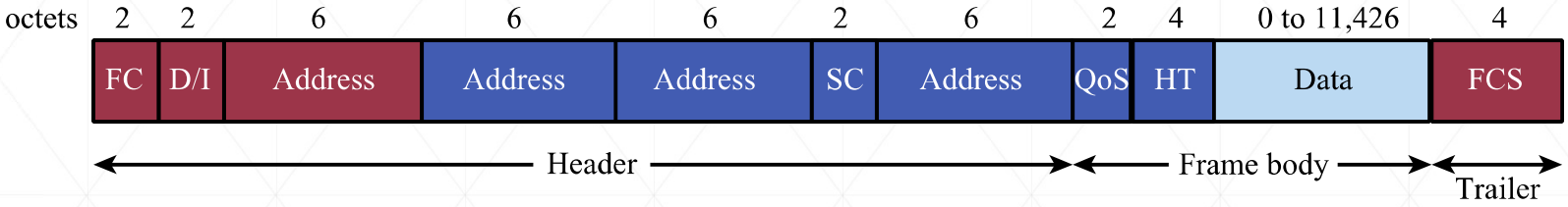
IEEE 802.11 : Point Coordinated Function and Network Allocation Vector (NAV)

- Point Coordinated Function (PCF)
  - Centralized control
  - Point coordinator polls devices
    - To give them permission to send
    - On a schedule the point coordinator determines
  - The *superframe* allows time to be shared between DCF and PCF
    - PCF starts the superframe and can only use a certain part of the superframe time
- Network Allocation Vector (NAV)
  - Stations in 802.11 can also “reserve” medium
  - To inform other stations that a series of data exchange needs to be performed without interruption.
  - Make use of Duration field in MAC frame

IEEE 802.11 : Network Allocation Vector (NAV)



IEEE 802.11 : MAC Frame Format



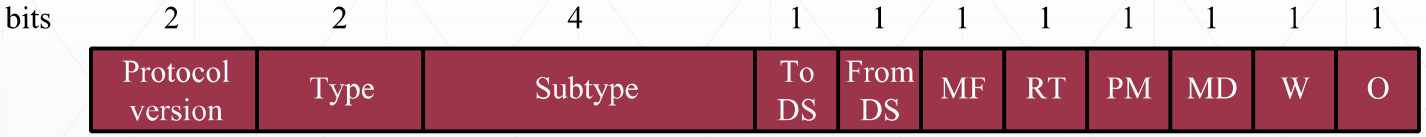
FC = frame control
D/I = duration/connection ID
QoS = QoS control

SC = sequence control
FCS = frame check sequence
HT = high throughput control

Always present

Present only in certain frame types and sub-types

(a) MAC frame



DS = distribution system
MF = more fragments
RT = retry
PM = power management

MD = more data
W = wired equivalent privacy bit
O = order

(b) Frame control field

IEEE 802.11 : MAC Frame Format

- MAC Frame Fields
  - Frame Control – frame type, control information
    - Protocol version – 802.11 version
    - Type – control, management, or data
    - Subtype – identifies function of frame
    - To DS – 1 if destined for DS
    - From DS – 1 if leaving DS
    - More fragments – 1 if fragments follow
    - Retry – 1 if retransmission of previous frame
    - Power management – 1 if transmitting station is in sleep mode
    - More data – Indicates that station has more data to send
    - WEP – 1 if Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) is implemented
    - Order – 1 if any data frame is sent using the Strictly Ordered service

IEEE 802.11 : MAC Frame Format

- MAC Frame Fields (cont'd)
  - Duration/connection ID – channel allocation time
  - Addresses – context dependent, types include source and destination
  - Sequence control – numbering and reassembly
  - Frame body – MSDU or fragment of MSDU
  - Frame check sequence – 32-bit CRC

IEEE 802.11 : MAC Frame: Type Field: Management

Subtype Value	Subtype Description
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message
1010	Dissociation
1011	Authentication
1100	Deauthentication

IEEE 802.11 : MAC Frame Format: Control

Subtype Value	Subtype Description
1010	Power save poll
1011	Request to send
1100	Clear to send
1101	Acknowledgement
1110	Contention-free (CF)-end
1111	CF-end+CF-ack

IEEE 802.11 : MAC Frame Format: Data

Subtype value	Subtype description
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll
0011	Data+CF-Ack+CF-Poll
0100	Null function(no data)
0101	CF-Ack(no data)
0110	CF-poll (no data)
0111	CF-Ack+CF-Poll

IEEE 802.11 : Management of Operation

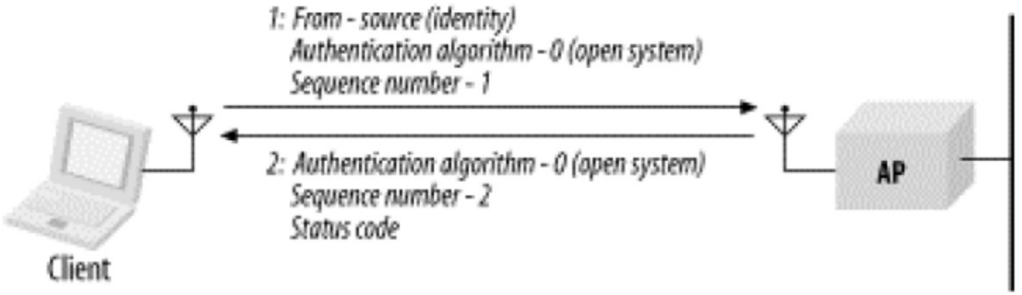
- Scanning
  - The process of finding existing network
    - Default values:
      - BSSType, BSSID, SSID (“Network name”), scan type, channel list, probe delay,
  - Type of scan
    - Passive scanning
      - Mobile stations waits for Beacon frame
    - Active scanning
      - Probe request frames are used to solicit responses from access point or other stations

IEEE 802.11 : Management of Operation

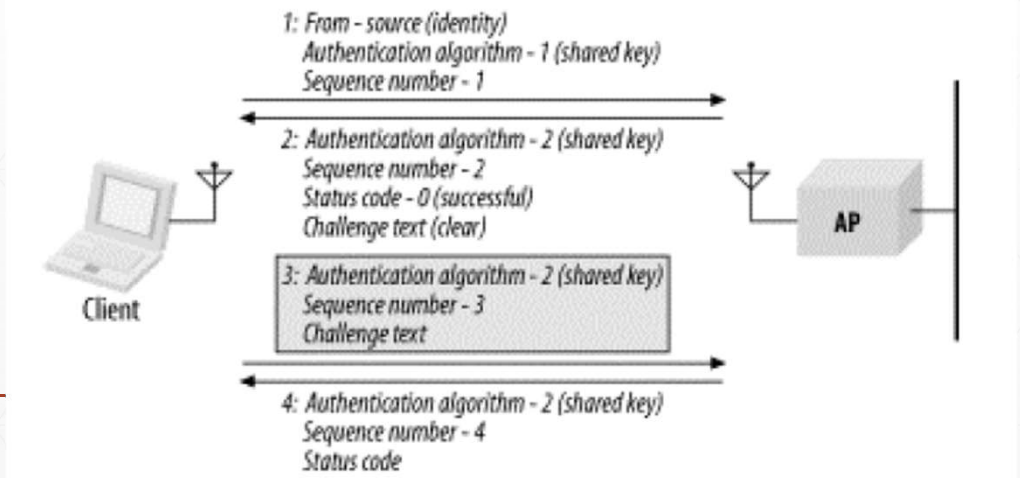
- Joining
  - Precursor to association
  - Does not enable network access
  - Implementation specific decision and may even involve user intervention
- Authentication
  - To ensure a station that attempts to associate with the network is allowed to do so
  - Two major approaches in IEEE 802.11
    - Open system authentication
    - Shared key -- based on WEP (Wired Equivalent Privacy)

IEEE 802.11 : Management of Operation: Authentication

- Open system authentication system



- Shared-key authentication

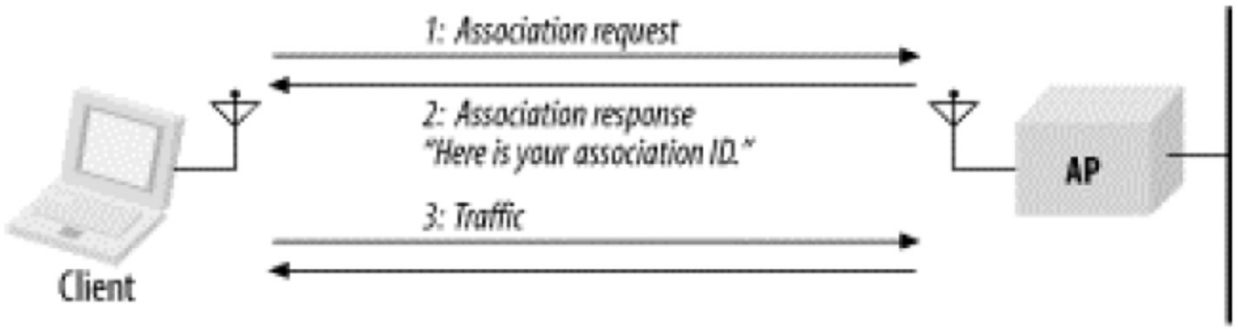


IEEE 802.11 : Management of Operation: Authentication

- WEP makes use of RC4 cipher key
  - Non technical issues :
    - RC4 is the intellectual property of RSA Security and must be licensed
    - Restricted to maximum 40 bits key to get approval from US export regulation
  - Requiring manual key distribution
    - Organization with large numbers of authorized users must publish the key to the user population, which effectively prevent it from being secret
    - Re-use of key is vulnerable to deciphering analysis
  - WEP does not authenticate the users, but authenticate the MAC address of device
  - WEP doesn’t provide encryption beyond the access point.

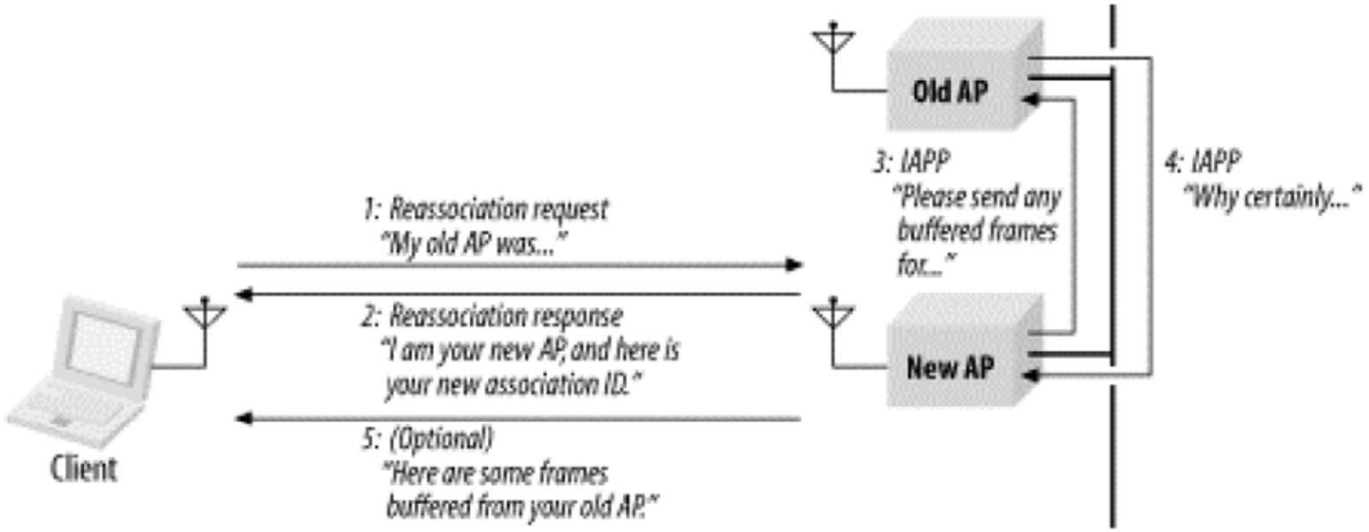
IEEE 802.11 : Management of Operation

- Association
  - Record keeping procedure that allows the distribution system to track the location of each mobile station



IEEE 802.11 : Management of Operation

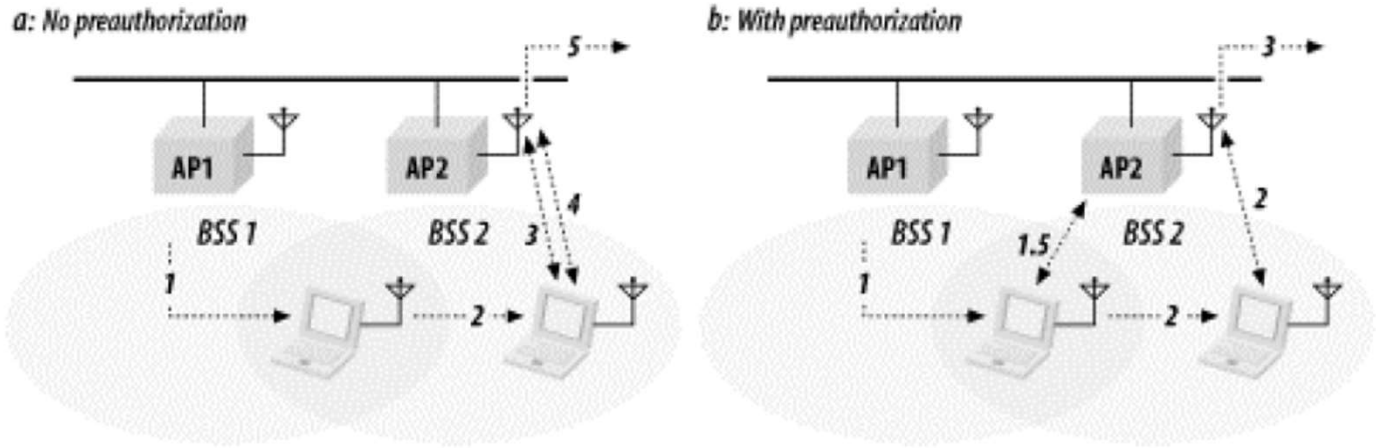
- Re-association
  - The process of moving an association from an old access point to a new one



IEEE 802.11 : Management of Operation

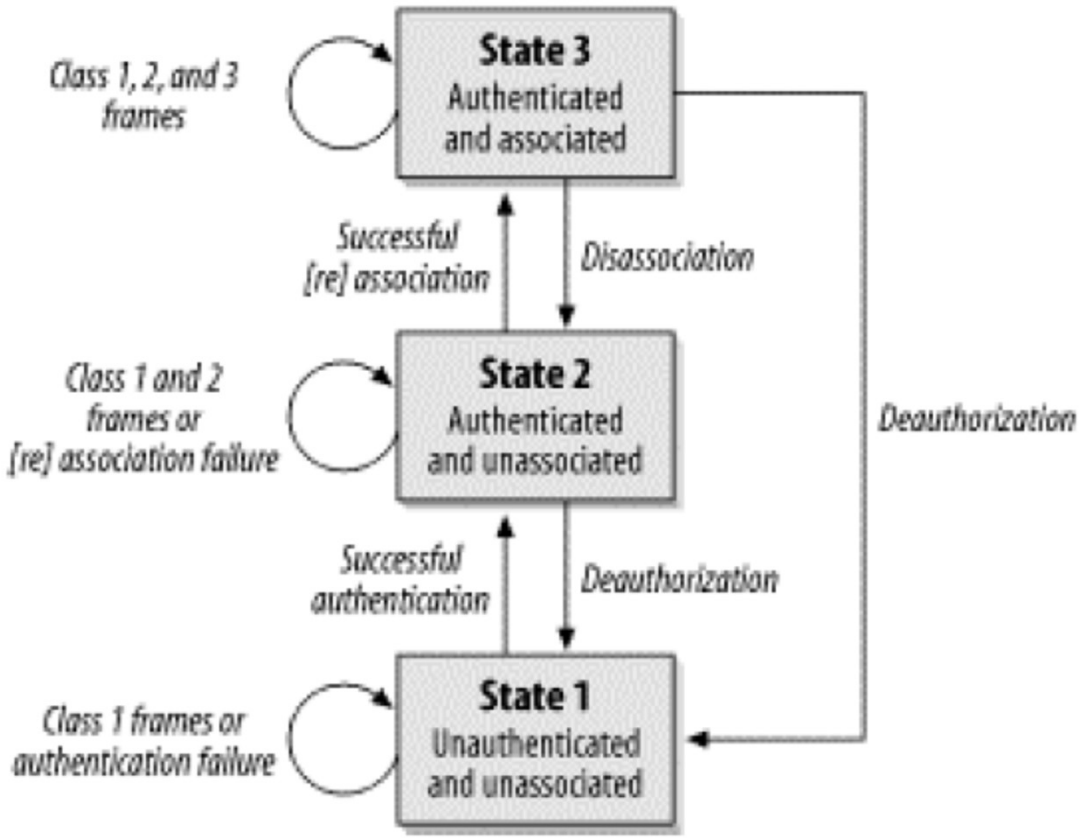
- Pre-authentication
  - IEEE 802.11 standard does not require Authentication procedure takes place immediately before association
  - Can be performed by mobile stations during scanning process with several access points
  - To enable smooth and faster transfer between different BSS

IEEE 802.11 : Pre-Authentication



0	Station associated with AP1	Station associated with AP1
1	Station moves right into the overlap between BSS1 and BSS2	Station moves right into the overlap between BSS1 and BSS2 and detects the presence of AP2
1.5		Station preauthenticates to AP2
2	AP2's signal is stronger, so station decides to move association to AP2	AP2's signal is stronger, so station decides to move association to AP2
3	Station authenticates to AP2	Station begins using the network
4	Station reassociates with AP2	
5	Station begins using the network	

IEEE 802.11 : State Diagram



IEEE 802.11 : Class 1 Frames

- Can be transmitted in any state and are used to provide the basic operations used by 802.11 stations
- Allow stations to find an infrastructure network and authenticate to it

Control	Management	Data
RTS, CTS, Acknowledgement (ACK), CF-End, CF-End+CF-Ack	Probe Request, Probe Response, Beacon, Authentication, Deauthentication, Announcement Traffic Indication Message (ATIM)	Any frame, ToDS and FromDS false (0)

IEEE 802.11 : Class 2 Frames

- Can only be transmitted only after a station has successfully authenticated to the network
- Manage association
- When a station receive a class 2 frames from non authenticated peer, it responds with Deauthentication frame, make the peer moves back to state 1

Control	Management	Data
None	Association, Reassociation, Disassociation	None

IEEE 802.11 : Class 3 Frames

- Are used when a station has been successfully authenticated and associated with an access point
- If Access Point (AP) receives frame from a mobile station that is authenticated but not associated, the access point responds with Disassociation frame and send mobile station back to state 2
- If the mobile station is not even authenticated, AP will respond with a Deauthentication frame to force the station back to State

Control	Management	Data
PS-Poll	Deauthentication	Any frame, including those with either the ToDS and FromDS set

IEEE 802.11 : Addressing

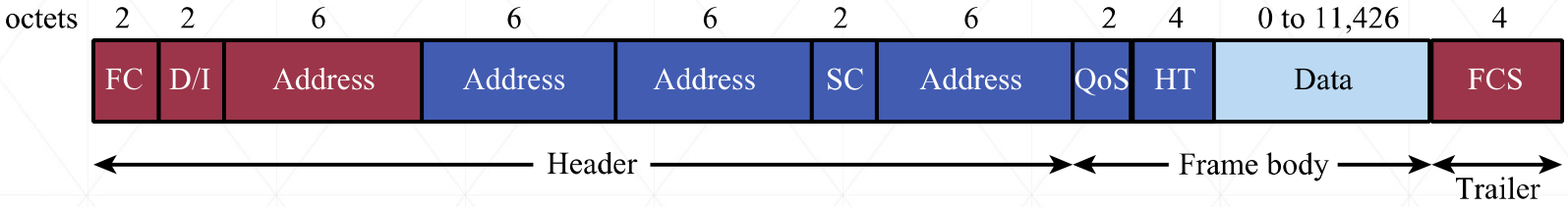
- Destination Address
  - 48 bit IEEE MAC identifier that corresponds to the final recipient
- Source Address
  - 48 bit IEEE MAC identifier that identifies the source of transmission
- Receiver Address
  - 48 bit IEEE MAC identifier that indicates which wireless station should process the frame
- Transmitter Address
  - 48 bit IEEE MAC address to identify the wireless interface that transmitted the frame onto the wireless medium

IEEE 802.11 : Addressing

- Basic Service Set ID (BSSID)
  - Identify different cells in the same area. In infrastructure wireless LAN, BSSID is the MAC address used by the wireless interface in the access point
  - The all -1s BSSID is the broadcast BSSID.
    - Used to locate network by sending a probe frame

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	not used
To AP (infra.)	1	0	BSSID	SA	DA	not used
From AP (infra.)	0	1	DA	BSSID	SA	not used
WDS (bridge)	1	1	RA	TA	DA	SA

IEEE 802.11 : Addressing : Illustrated



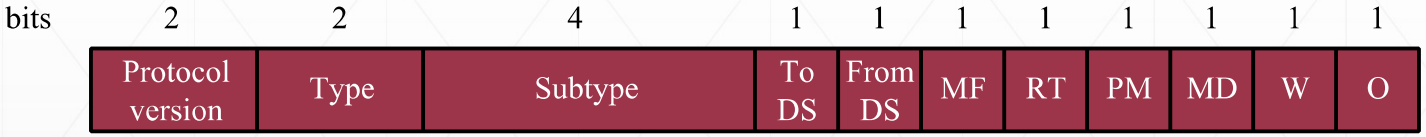
FC = frame control
D/I = duration/connection ID
QoS = QoS control

SC = sequence control
FCS = frame check sequence
HT = high throughput control

Always present

Present only in certain frame types and sub-types

(a) MAC frame

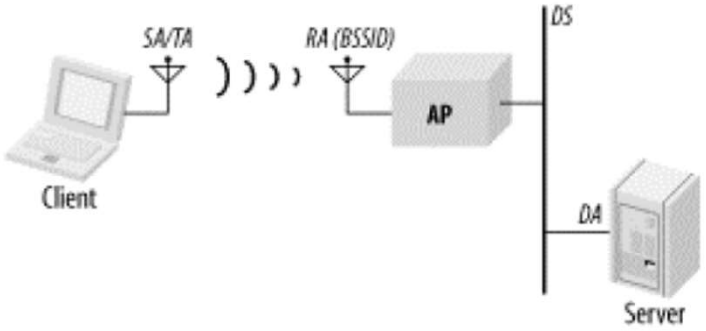


DS = distribution system
MF = more fragments
RT = retry
PM = power management

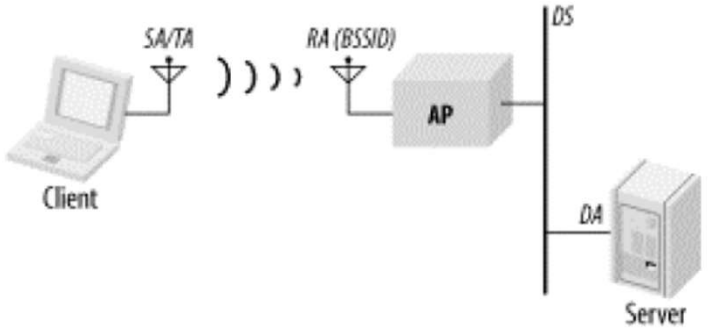
MD = more data
W = wired equivalent privacy bit
O = order

(b) Frame control field

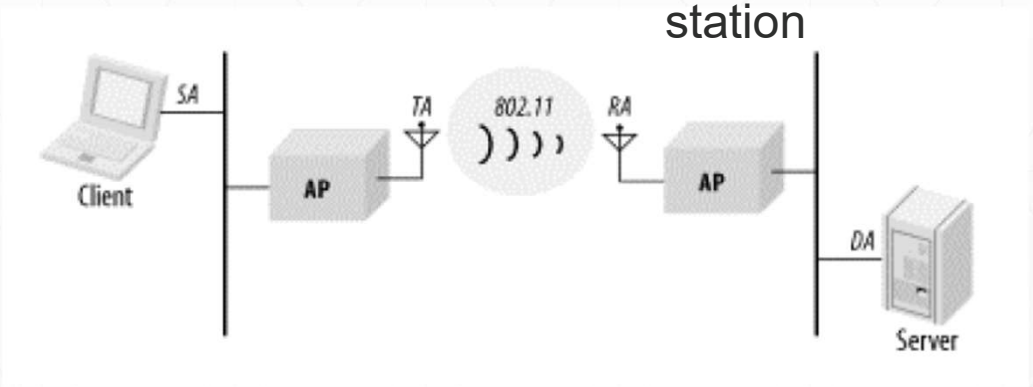
IEEE 802.11 : Addressing : Illustrated



From station to distribution system



From distribution system to station



Wireless distribution system

IEEE 802.11 : Power Management

- Infrastructure Wireless Network
  - Access point generally doesn't have power issue, since it is not battery-powered
    - They must remain active during operation
  - Power savings is mainly performed by mobile stations
    - Power to transmit is typically higher than the power to receive
  - In this type of infrastructure:
    - All packets go through access point, then access point becomes the ideal location to buffer traffic
    - Since it is remain active, access point is aware the location of mobile stations and a mobile stations can communicate its power management state to access point

IEEE 802.11 : Power Management

- Two Power Management Related-task at access point
  - It can determine whether a frame should be delivered to the wireless network
  - Announce periodically which stations have frame waiting for them
    - Through beacon frame, using Traffic Indication Map
    - Mobile stations only spend energy to listen this periodic announcement
      - Implemented through periodic listen interval
    - Mobile stations needs to wake up whenever a frame is waiting
      - Mobile stations should transmit PS-Poll frame to retrieve frame(s) from access point
- Infrastructure-less Wireless Network
  - Use Announcement Traffic Indication Message