

# EEC 687/787 Mobile Computing (Sprint, 2009)

## IEEE 802.11: MAC Management

Prof. Chansu Yu

<http://academic.csuohio.edu/yuc/>  
c.yu91@csuohio.edu

## 802.11: MAC Management

- ❑ Synchronization
  - Finding and staying with a WLAN
  - Synchronization function – TSF timer, beacon generation
- ❑ Power management
  - Sleeping without missing a message
  - periodic sleep, frame buffering, TIM (traffic indication map)
- ❑ Association/Reassociation
  - Joining a LAN
  - roaming, i.e. moving from one AP to another
  - scanning, i.e. active search for a network
- ❑ MIB - Management Information Base
  - managing, read, write

## (1) 802.11 MAC Management: Synchronization

Timing synchronization function (TSF) is used for

- Power management
  - Wakeup/sleep management
- Point coordination timing
  - TSF timer used to predict start of CF burst
- Hop timing for FH PHY
  - TSF timer used to time dwell interval
  - All stations are synchronized, so they hop at the same time

3

*c.yu91@csuohio.edu*

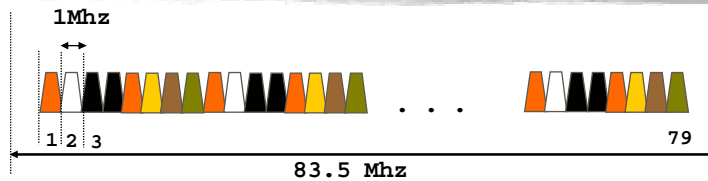
## FHSS : Frequency Hopping Spread Spectrum

- Discrete changes of carrier frequency
  - sequence of frequency changes determined via pseudo random number sequence
- Two variations:
  - Fast Hopping: several frequencies per user bit
  - Slow Hopping: several user bits per frequency

4

*c.yu91@csuohio.edu*

## Bluetooth/802.11 uses FHSS



### ❑ Bluetooth

- Channels:  $2.402 \text{ GHz} + k \text{ MHz}$ ,  $k=0, \dots, 78$
- Hopping rate: 1,600 hops per second
- Dwell time in each carrier frequency: 625- $\mu\text{s}$
- During each 625- $\mu\text{s}$  time slot, it transmits one packet

### ❑ IEEE 802.11 standard

- IR / DSSS / FHSS are defined as its physical layers
- FHSS: 2.5 hops per second<sub>5</sub>

*c.yu91@csuohio.edu*

## Synchronization: TSF

### ❑ Timing synchronization function (TSF) is used for

- Power management
  - Wakeup/sleep management
- Point coordination timing
  - TSF timer used to predict start of CF burst
- Hop timing for FH PHY
  - TSF timer used to time dwell interval
  - All stations are synchronized, so they hop at the same time

6

*c.yu91@csuohio.edu*

# Synchronization: Beacons

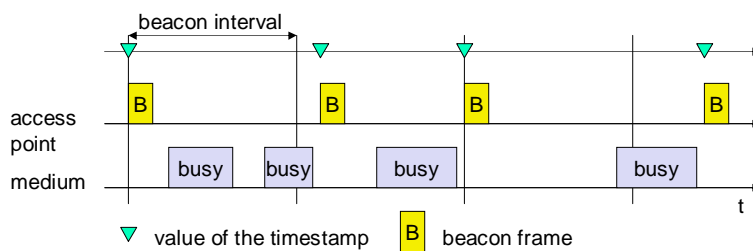
## □ Beacons

- Beacons are sent at well known intervals (beacon interval)
  - Beacons contain timestamp for the entire BSS
  - All station timers in BSS are synchronized
  - Transmission may be delayed by CSMA deferral (not relative to the last beacon transmission)
- Who sends beacons?
  - AP controls in infrastructure networks
  - Distributed function for IBSS

7

*c.yu91@csuohio.edu*

# Synchronization using a Beacon in infrastructure network



8

*c.yu91@csuohio.edu*

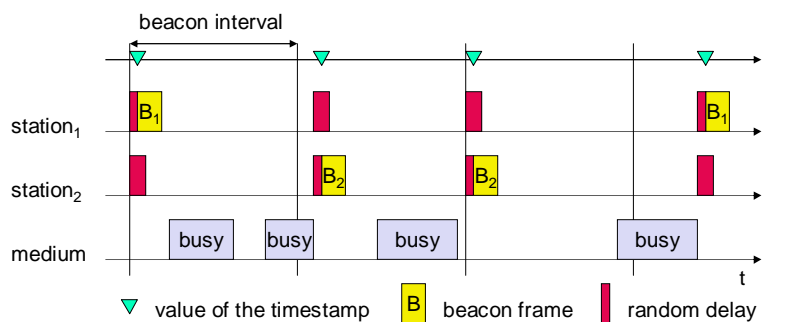
## Synchronization using a Beacon in Ad-hoc network

- ❑ TSF is complicated for ad hoc networks
  
- ❑ Master Election steps
  - Every station is responsible for generating a beacon
  - All stations compete for transmission of the beacon using the standard backoff algorithm
  - The first wins the race and all others cancel their beacon transmission and adjust their local timers to the timestamp of the winning beacon

9

c.yu91@csuohio.edu

## Synchronization using a Beacon in Ad-hoc network



10

c.yu91@csuohio.edu

## (2) 802.11 MAC Management: Power management

- ❑ Mobile devices are battery powered
- ❑ Current LAN protocols assume stations are always ready to receive (promiscuous mode)
- ❑ Idle receive state dominates LAN adapter power consumption over time
  - Absolute value is slightly less than transmit/receive power
  - But, time duration in idle state is larger
  
- ❑ How can we power off during idle periods, yet maintain an active session?
- ❑ PS (Power Save) mode
  - A station sleeps most of the time
  - But wakes up periodically to receive regular beacon from AP (Access Point)
  - This is to check if there is any packet destined to it

11

c.yu91@csuohio.edu

## Power Save Mode in IEEE 802.11

| 802.11 (WaveLAN-II)  |                   | Bluetooth (Nokia) |                  |            |
|----------------------|-------------------|-------------------|------------------|------------|
| Hardware State       | Mode of Operation | Mode of Operation | Hardware State   |            |
| Awake                | Active            | Transmit (300mA)  | Active (40-60mA) | Connection |
|                      |                   | Receive (250mA)   |                  |            |
| Idle(Listen) (230mA) |                   |                   |                  |            |
| Doze                 | Power Save        | Sniff             | Standby          |            |
|                      | Sleep (9mA)       | Hold              |                  |            |
|                      |                   | Park              |                  |            |
|                      |                   | Standby (0.55mA)  |                  |            |

2 Mbps, 250 meters

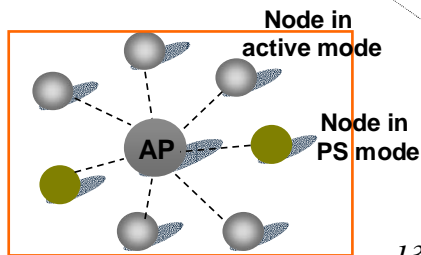
768 Kbps, 10-100 meters

12

c.yu91@csuohio.edu

# Power Save Mode in IEEE 802.11

- ❑ AP can transmit data frames to an active node at any time
- ❑ For nodes in PS mode,
  - AP buffers data frames
  - AP announces buffered traffic at a predetermined time
  - AP transmits the data frames



13

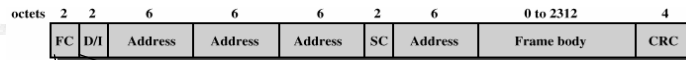
Requires synchronization (beacons)

Uses TIM (Traffic Indication Map)

AP maintains nodes' mode of operation

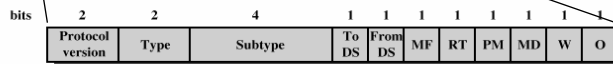
c.yu91@csuohio.edu

# Power Save Mode in IEEE 802.11



FC = Frame control  
D/I = Duration/Connection ID  
SC = Sequence control

(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

PM field indicates the power management mode of a station in which it will be after the successful completion of the current frame.  
PM=1 indicates that the station will be in PS mode.  
PM=0 indicates active mode.

c.yu91@csuohio.edu

## Power Management in infrastructure network

- ❑ The AP is responsible for generating beacons, which contains time information
- ❑ Beacon also contains a traffic indication map (TIM)
  - All unicast packets for stations in doze mode are announced in the TIM
  - Broadcast/multicast frames are announced in TIM and are sent immediately after
- ❑ Devices in PS mode
  - have to be synchronized to wake up at one particular time, in which the AP announces buffered frames for receivers with TIM
  - A station that receives such an announcement stays awake until the frame is delivered

15

*c.yu91@csuohio.edu*

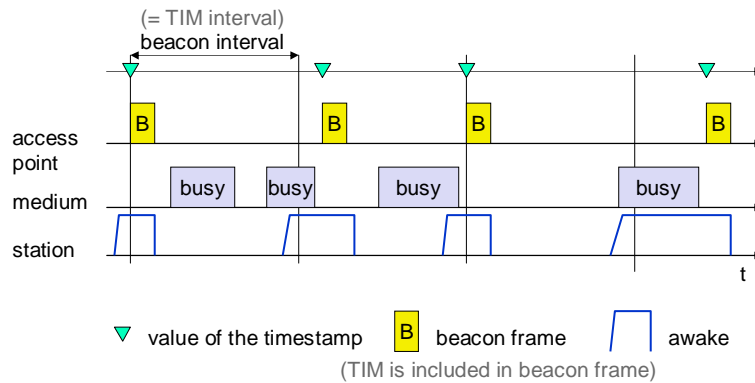
## Power Management in infrastructure network

- ❑ TSF assures AP and stations are synchronized
- ❑ TIM: Infrastructure network
  - TIM: list of unicast receivers transmitted by AP
- ❑ DTIM (Delivery TIM): Broadcast/multicasts
  - Broadcast frames are also buffered in AP
  - DTIM: list of broadcast/multicast receivers transmitted by AP
  - All broadcast/multicasts are buffered
  - Broadcast/multicasts are only sent after DTIM
  - DTIM interval is a multiple of TIM interval
- ❑ ATIM (Ad-hoc TIM): Ad-hoc network
  - IBSS also have power management
  - Similar in concept, distributed approach
    - announcement of receivers by stations buffering frames
    - more complicated, collision of ATIMs possible - no central AP

16

*c.yu91@csuohio.edu*

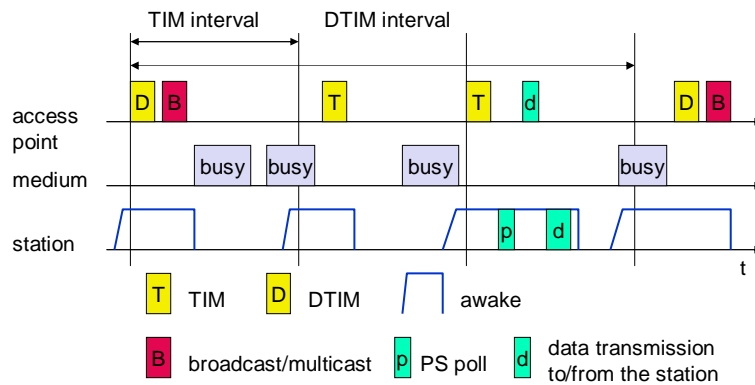
# Power Management in infrastructure network



17

c.yu91@csuohio.edu

# Power Management in infrastructure network



18

c.yu91@csuohio.edu

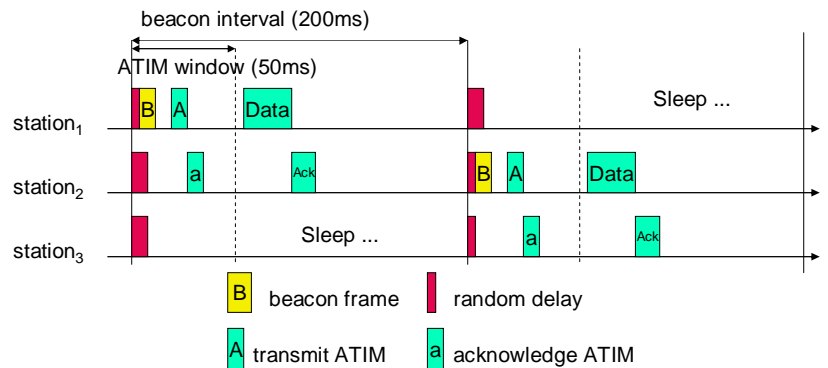
# Power Management in Ad-hoc network

- ❑ Beacon is followed by ATIMs announced during ATIM window
- ❑ ATIM (Ad-hoc TIM): Ad-hoc network
  - Announcement of receivers by stations buffering frames
  - More complicated, collision of ATIMs possible - no central AP
- ❑ Data transmission
  - Data is announced by ad hoc TIMs (ATIMs) in special time interval called "ATIM Window" after a beacon
  - Packets for a station in doze state have to be buffered by the sender (not the master) until the end of the beacon interval

19

c.yu91@csuohio.edu

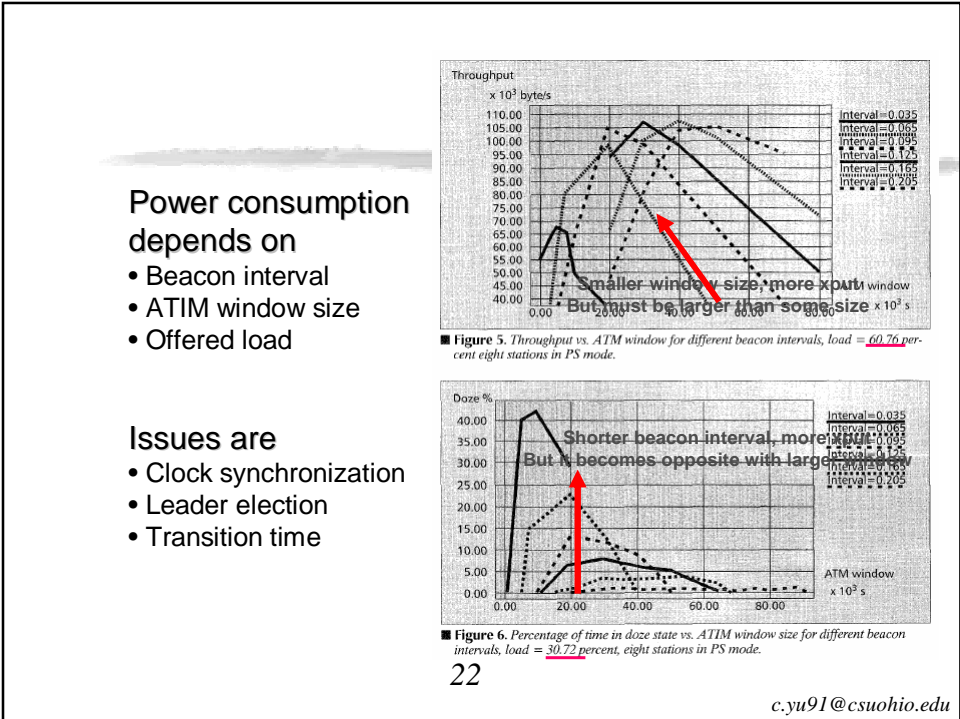
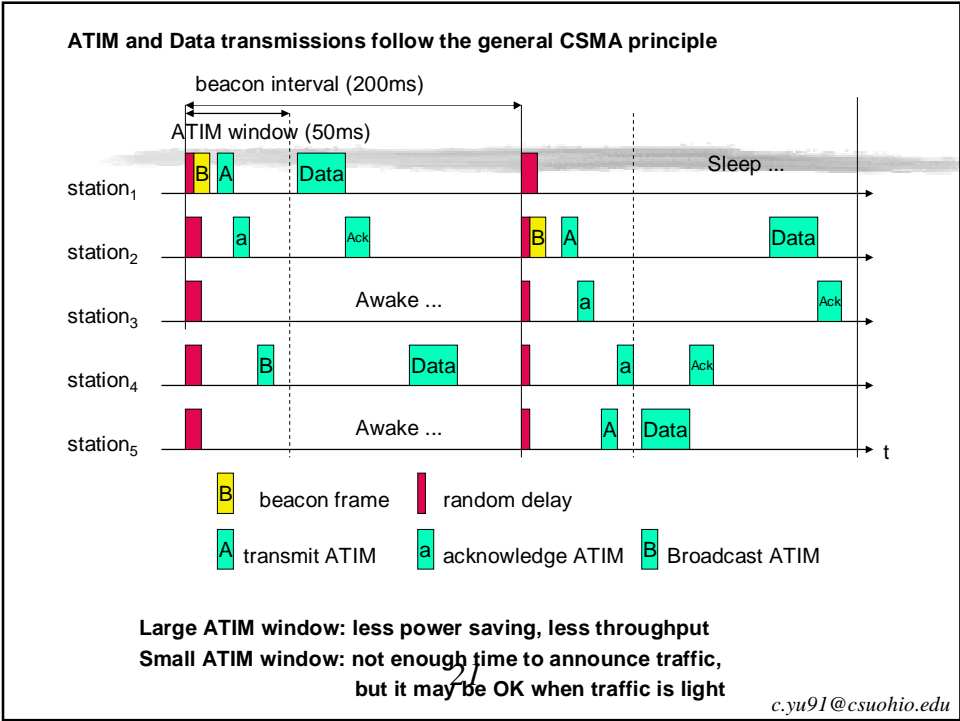
# Power Management in Ad-hoc network



**Nodes that are not addressed during the ATIM window can sleep during the rest of the beacon interval.**

20

c.yu91@csuohio.edu



## Dynamic ATIM Window

- ❑ Power-Saving Mechanisms in Emerging Standards for Wireless LANs: The MAC Level Perspective
  - Hagen Woesner, Jean-Pierre Ebert, Morten Schlager, and Adam Wolisz
  - *IEEE Personal Communications*, Vol. 5, Issue 3, pp. 40-48, Jun. 1998.
- ❑ Minimizing Energy for Wireless Web Access Using Bounded Slowdown
  - Ronny Krashinsky and Hari Balakrishnan
  - *MobiCom*, 2002.
- ❑ An Energy Efficient MAC Protocol for Wireless LANs
  - E. Jung and N. Vaidya
  - *IEEE Infocom*, 2002.

23

c.yu91@csuohio.edu

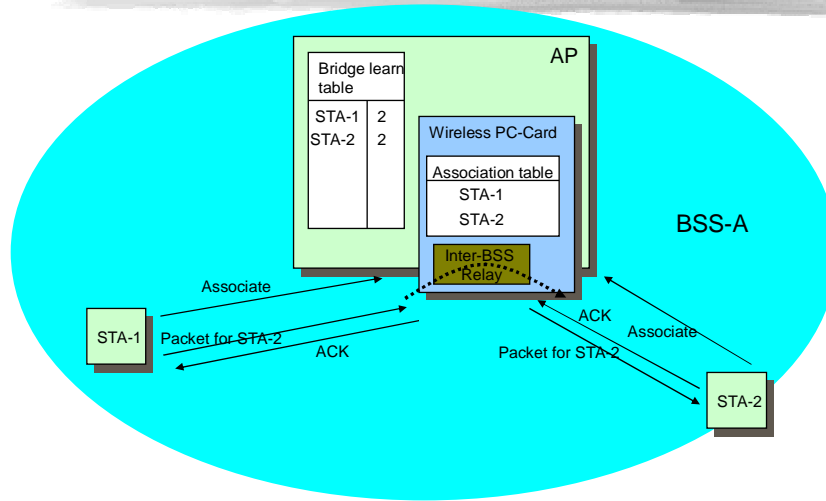
## (3) 802.11 MAC Management: Association/Reassociation (Roaming/Scanning)

- ❑ Each station is associated with a particular AP
  - Association: Establishes initial association between station and AP
- ❑ Mobile stations may move...
  - Beyond the coverage area of their AP
  - But within range of another AP
- ❑ Reassociation allows station to continue operation
  - Reassociation: Enables transfer of association from one AP to another, allowing station to move from one BSS to another
- ❑ Disassociation
  - Association termination notice from station or AP

24

c.yu91@csuohio.edu

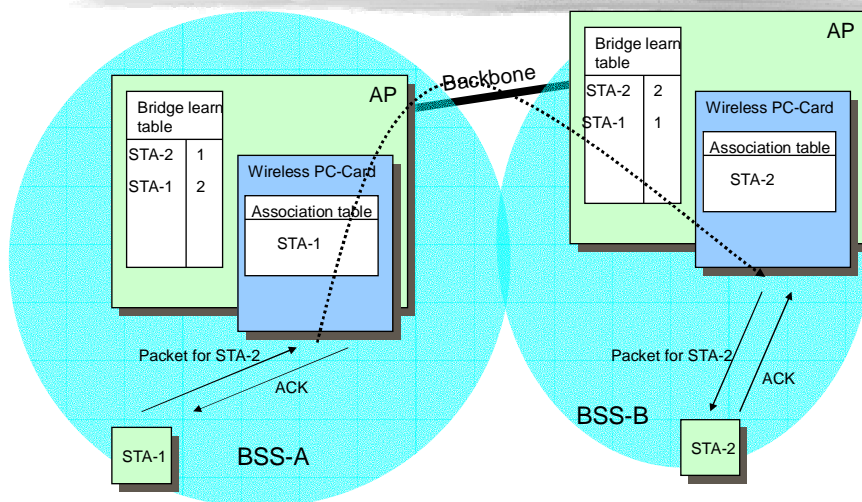
## Operational processes Traffic flow in a BSS



25

c.yu91@csuohio.edu

## Operational processes Traffic flow in an ESS



26

c.yu91@csuohio.edu

## Association/ Reassociation

- ❑ How does a station associate with an AP?
  - AP periodically (typically, 100ms) transmits beacon.
  - Beacon contains information such as BSSID, timestamp, TIM, power management, and roaming.
  - When a station receives a beacon with a reasonable signal strength, it “associates” with the AP.
  - AP grants permission to the station via an “association response” frame.

27

*c.yu91@csuohio.edu*

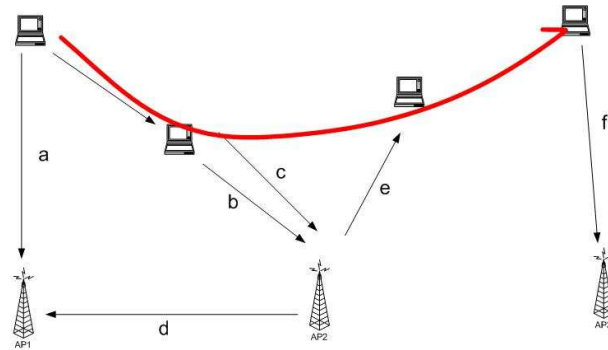
## Association/ Reassociation

- ❑ How to support mobility?
  - When a station receives a beacon from another AP in the same ESS (called BSS transition), the station “re-associates” with the new AP.
  - When a station receives a beacon from another AP in another ESS (called ESS transition), automatic handoff is not made (i.e., upper layer connection breaks. Mobile IP supports handoff of this kind.)

28

*c.yu91@csuohio.edu*

Ex.



- (a) ---- The station finds AP1, it will authenticate and associate.
- (b) ---- As the station moves, it may pre-authenticate with AP2.
- (c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.
- (d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.
- (e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.
- (f) ---- The station find another access point and authenticate and associate.

## Reassociation, Roaming/Scanning

- ❑ When is the time for a station to handoff?
  - Station measures signal strength of the current AP's beacon
  - If it becomes poor, it can simply listens to another AP's beacon (passive)
  - Or, perform scanning to find another AP (active) by sending "reassociation request" to one or several AP(s)
  - A new AP answers by sending "reassociation response"
- ❑ Reassociation request contains
  - Information about the station as well as the old AP
- ❑ Reassociation response contains
  - Information about the supported bit rates, station ID, and so on
- ❑ Question: what the old AP to do?
  - It does not know whereabouts of the station : Why does it have to know?
  - No standard for communication among AP's
  - IAPP (inter-access point protocol) emerges

# Scanning & Joining

## ❑ Scanning

- Passive Scanning : only listens for Beacon and get info of the BSS. Power is saved.
- Active Scanning: transmit and elicit response from APs. If IBSS, last station that transmitted beacon responds. Time is saved.

## ❑ Joining a BSS

- Synchronization in TSF and frequency : Adopt PHY parameters : The BSSID : WEP : Beacon Period : DTIM

Table 14.3 Valid Type and Subtype Combinations

## 802.11 MAC Data Type

| Type Value | Type Description | Subtype Value | 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       | 1000          | Beacon                                  |
| 00         | Management       | 1001          | Announcement traffic indication message |
| 00         | Management       | 1010          | Dissociation                            |
| 00         | Management       | 1011          | Authentication                          |
| 00         | Management       | 1100          | Deauthentication                        |
| 01         | Control          | 1010          | Power save - poll                       |
| 01         | Control          | 1011          | Request to send                         |
| 01         | Control          | 1100          | Clear to send                           |
| 01         | Control          | 1101          | Acknowledgment                          |
| 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)              |