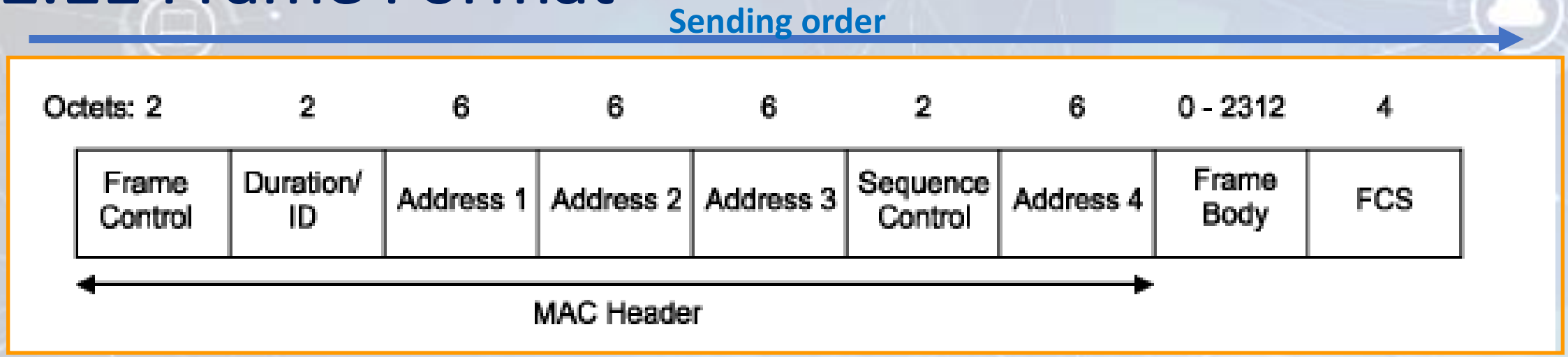
Cairo University
Faculty of Engineering
Computer Engineering Department


# Wireless Networks

Dr. Sandra Wahid

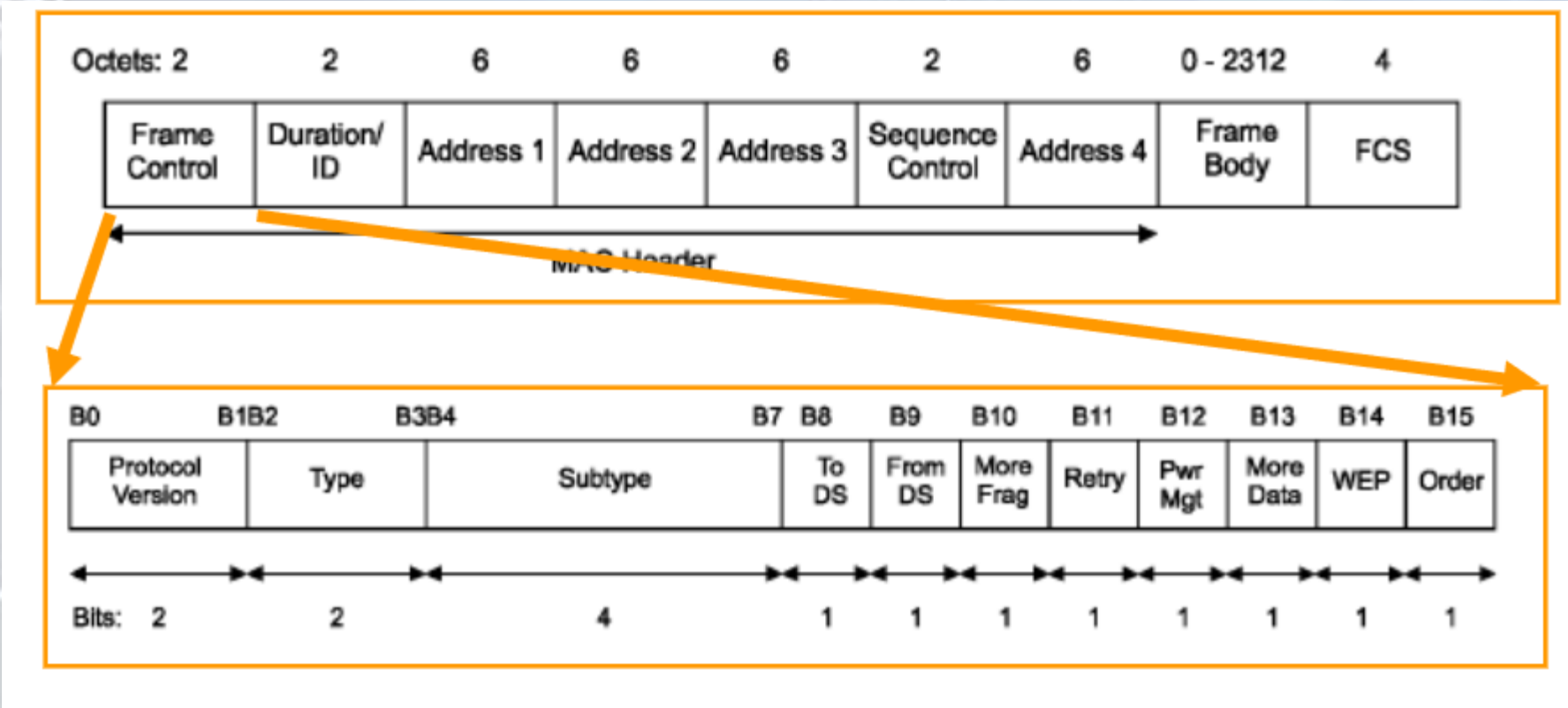
# 802.11 Frame Format




The MAC frame consists of:

- **MAC Header**
  - Frame Control
  - Duration/ID
  - Address → not all 4 are always used
  - Sequence Control information
- **Frame Body**
- **Frame Check Sequence (FCS)**

# Frame Control




- **Protocol version:** is currently 0 and all other values are reserved for future use.
- **3 Frame Types:** control, data, and management.
- Each type has several defined **subtypes**.

# Frame Control: Type and Subtype

B2 is sent first then B3

| 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 | ATIM |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101–1111 | Reserved |

- Stations send association requests to access points (APs) requesting to join the BSS.
- The AP responds to the station using an association response frame that includes an association ID (AID).
  - Each station within the BSS has a unique AID.

- The primary difference between reassociation and association requests is that the station will indicate the current AP it is connected to in reassociation requests.

- Stations send probe requests to search for wireless networks.
- AP's respond with probe response.

# Frame Control: Type and Subtype

| 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 | ATIM |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101–1111 | Reserved |

- Beacon frames are transmitted by the AP containing information about the network. Beacon frames are transmitted periodically to announce the presence of a wireless LAN and to synchronize the members of BSS.

- Announcement Traffic Indication Message (ATIM) to notify peers of an upcoming data transfer. The ATIM message is transmitted between wireless stations and prevents stations from entering power-save mode. The transmission takes place in the ATIM window at the beginning of the beacon period.

# Frame Control: Type and Subtype

| 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 | ATIM |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101–1111 | Reserved |

- Can be sent from either the station or the AP. Disassociation frames are used to terminate the station's association; it is a notification and does not expect a response. Clients may disassociate prior to powering off. APs may disassociate clients for various reasons including failure to properly authenticate, for load balancing or timeout reasons, entering a state of maintenance, etc.

- Authentication frames are used in joining the BSS to verify that the station attempting to join the BSS has the capabilities to do so. The station sends an authentication request and the AP sends an authentication response.

# Frame Control: Type and Subtype

| 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 | ATIM |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101–1111 | Reserved |

- When a station is disassociated it still maintains its authentication. This makes it easier for the client to associate again in the future. Deauthentication frames are used to reset the state machine for an associated client. If a station is deauthenticated, it is also disassociated.

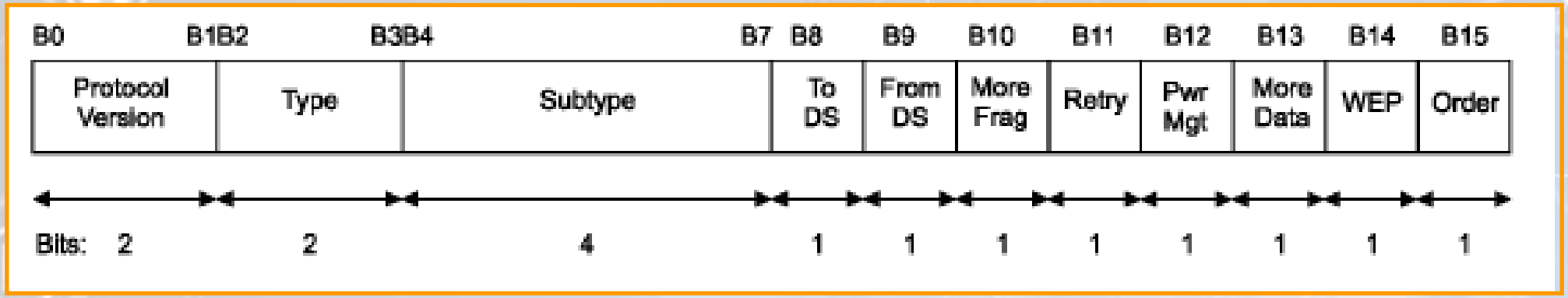
# Frame Control: Type and Subtype

| | | | |
|---|---|---|---|
| 01 | Control | 1010 | PS-Poll |
| 01 | Control | 1011 | RTS |
| 01 | Control | 1100 | CTS |
| 01 | Control | 1101 | ACK |
| 01 | Control | 1110 | 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 |

# Frame Control: To DS & From DS Bits

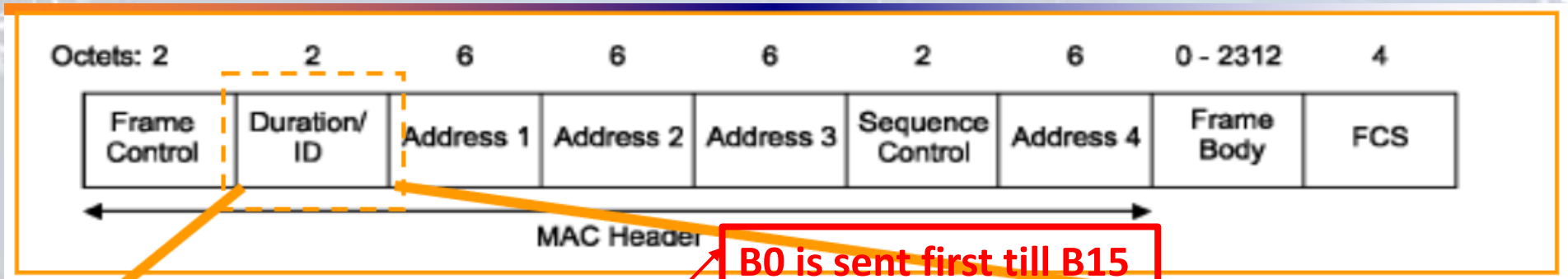
| To/From DS values | Meaning |
|---|---|
| To DS = 0<br>From DS = 0 | A data frame direct from one STA to another STA within the same IBSS, as well as all management and control type frames. |
| To DS = 1<br>From DS = 0 | Data frame destined for the DS. **From station to AP** |
| To DS = 0<br>From DS = 1 | Data frame exiting the DS. **From AP to station** |
| To DS = 1<br>From DS = 1 | Wireless distribution system (WDS) frame being distributed from one AP to another AP. |

# Frame Control: Other Bits




- **More Frag:** indicates whether there is another fragment to follow (1) or not (0).
- **Retry:** indicates whether this is a first (0) or retransmission (1).
- **Pwr Mgt:** indicate Power Saving (PS) mode after successful completion of current transmission: 0 (active) 1 (PS).
- **More Data:** AP indicates to PS STA that more frames are buffered for this STA.
- **WEP:** (1) indicates that the standard security mechanism of 802.11 is applied.
- **Order:** Frames and fragments can be transmitted in order at the cost of additional processing by both the sending and receiving MACs. When the "strict ordering" delivery is employed, this bit is set to 1.

# Duration/ID




B0 is sent first till B15

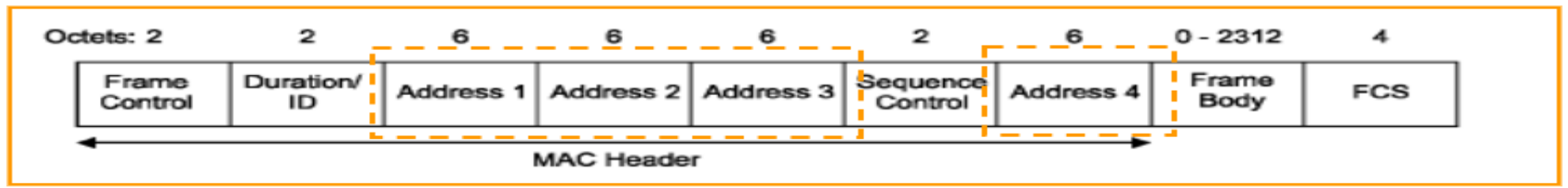
| Bit 15 | Bit 14 | Bits 13–0 | Usage |
|---|---|---|---|
| 0 | 0–32 767 | | Duration |
| 1 | 0 | 0 | Fixed value within frames transmitted during the CFP |
| 1 | 0 | 1–16 383 | Reserved |
| 1 | 1 | 0 | Reserved |
| 1 | 1 | 1–2 007 | AID in PS-Poll frames |
| 1 | 1 | 2 008–16 383 | Reserved |

NAV

Fixed value=32768

- AID : AP assigns it to STA during Association
- Duration: the period of time in which the medium is occupied (in microseconds).

# Address Fields



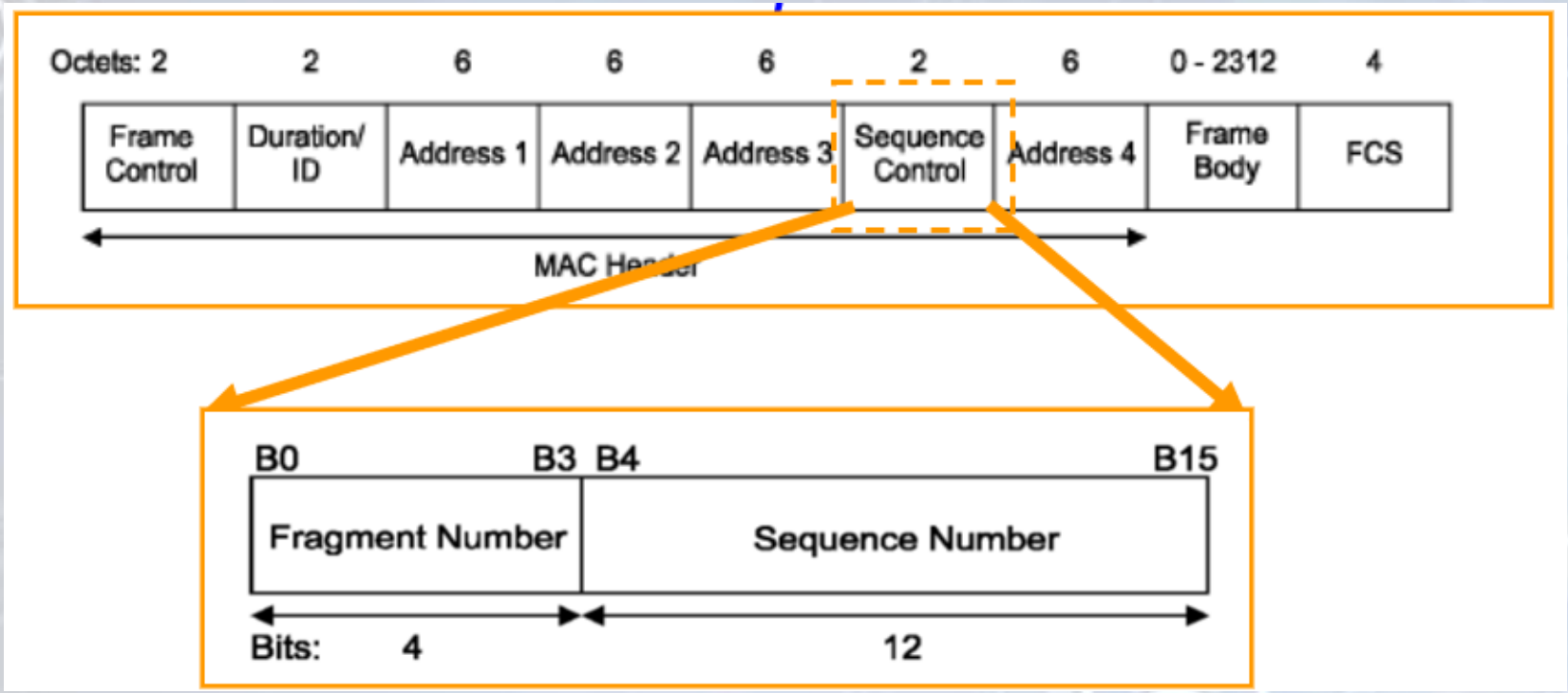

- 6*8=48 bits long MAC Address
- If the first bit (0)→Unicast, (1)→Mulitcast, All bits are 1s→ Broadcast
- Which addresses used depend on the “toDS and “fromDS” bits.
- Types of addresses:
  - DA: the final recipient **(destination)**→(might be a multicast/broadcast address)
  - SA: identifies the source of the transmission (Only one station) **(source)**
  - RA: immediate recipient **(receiver)**
  - TA: immediate transmitter **(transmitter)**
  - BSSID:
    - In case of Ad Hoc (IBSS), no access points are used. The transmitter is the source, and the receiver is the destination. All frames carry the BSSID so that stations may check broadcasts and multicasts; only stations that belong to the same BSS will process broadcasts and multicasts.
    - In an infrastructure BSS, the BSSID is the MAC address of the wireless interface in the access point creating the BSS.

# Address Fields

| 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 |

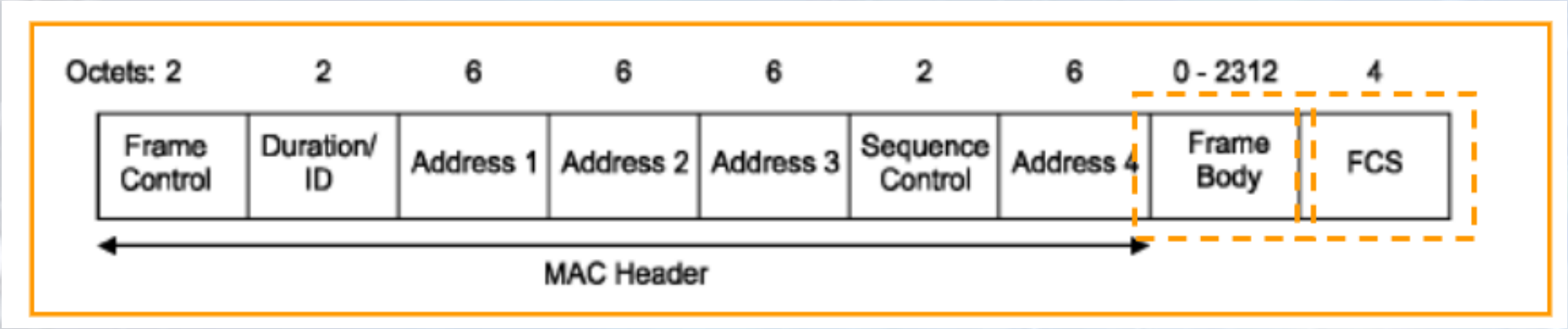
- Most frames use only three addresses: source, destination, and BSSID (which is the MAC address of the intermediate recipient)
  - That is why the first 3 addresses are contiguous.

# Sequence Control




- Higher-level frames are each given a SN as they are passed to the MAC for transmission.
- All fragments will have the same SN.
- Retransmitted frames have the same SN.
- The first fragment is given a fragment number of 0. Each successive fragment increments the fragment number by one.

# Frame Body and FCS




- **Frame body:**
  - Max payload: 2,304 bytes of higher-level data.
  - WEP overhead: 8 octets

- **FCS:**
  - 32-bit CRC in the trailer
  - All fields in the MAC header and the body of the frame are included in the FCS.


Thank You