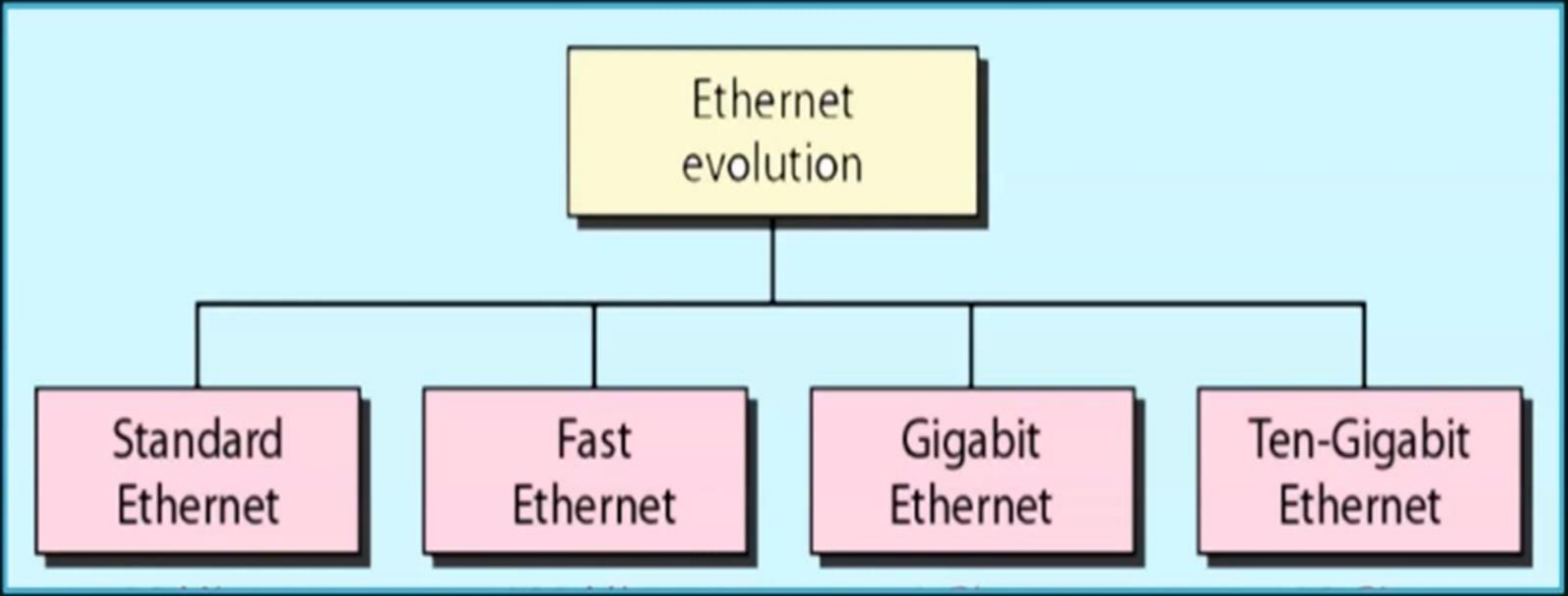
ETHERNET

- ★ One of the most widely used Wired LAN technologies.
- ★ Operates in the data link layer and the physical layer.
- ★ Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.
- ★ Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps).

Ethernet Standards

- ★ Define Layer 2 protocols and Layer 1 technologies
- ★ Two separate sublayers of the data link layer to operate – Logical link control (LLC) and the MAC sublayers.

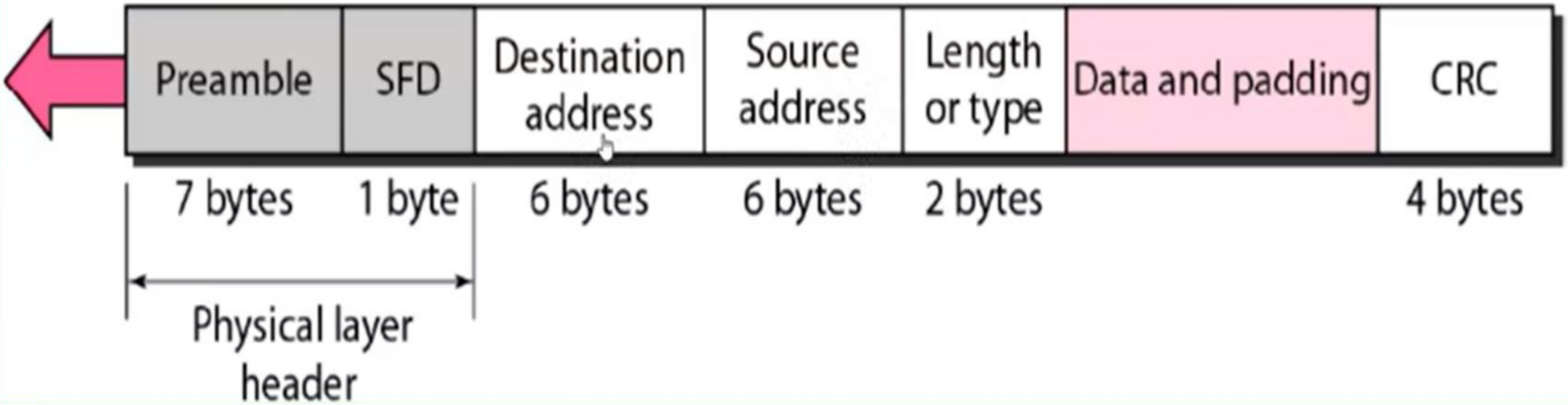


10 Mbps | 100 Mbps | 1 Gbps | 10 Gbps

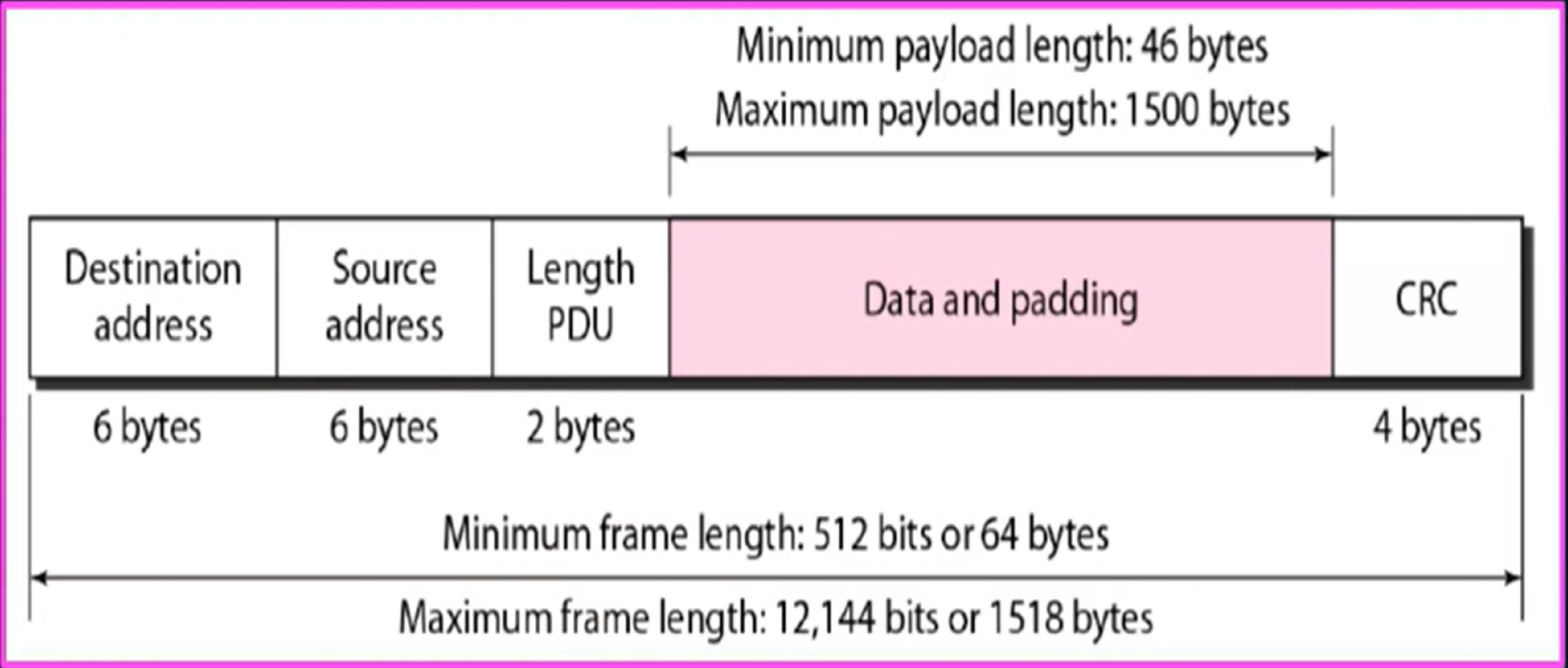
Ethernet frame format

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Ethernet frame – Min and Max Length



Ethernet address

Example – 06:01:02:01:2C:4B

06:01:02:01:2C:4B <=> 6 bytes <=> 12 hex digits <=>48 bits

The least significant bit of the first byte defines the type of address.

If the bit is 0, the address is unicast; otherwise, it is multicast.

If all bits are 1, then it is broadcast address

Access Protocol for Ethernet

The algorithm is commonly called Ethernet's Media Access Control (MAC) which is implemented in Hardware on the network adaptor.

Access Method of Ethernet: CSMA/CD

Encoding method: Manchester Encoding Technique for converting data bits into signals.

Ethernet Transmitter Algorithm

- When the adaptor has a frame to send and the line is idle, it transmits the frame immediately.
- The upper bound of 1500 bytes in the message means that the adaptor can occupy the line for a fixed length of time.
- When the adaptor has a frame to send and the line is busy, it waits for the line to go idle and then transmits immediately.
- The Ethernet is said to be CSMA 1-persistent protocol because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.

ETHERNET TRANSMITTER ALGORITHM

- ★ Since there is no centralized control it is possible for two (or more) adaptors to begin transmitting at the same time, either because both found the line to be idle, or, both had been waiting for a busy line to become idle.
- ★ When this happens, the two (or more) frames are said to be collide on the network.

Ethernet Transmitter Algorithm

- ★ Since Ethernet supports collision detection, each sender is able to determine that a collision is in progress.
- ★ At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a 32-bit jamming sequence and then stops transmission.

Runt Frames

- A runt frame is an Ethernet frame that is less than the IEEE 802.3's minimum length of 64 bytes.
- Runt frames are most commonly caused by collisions.
- Other possible causes are a malfunctioning network card, buffer underrun, duplex mismatch or software issues.

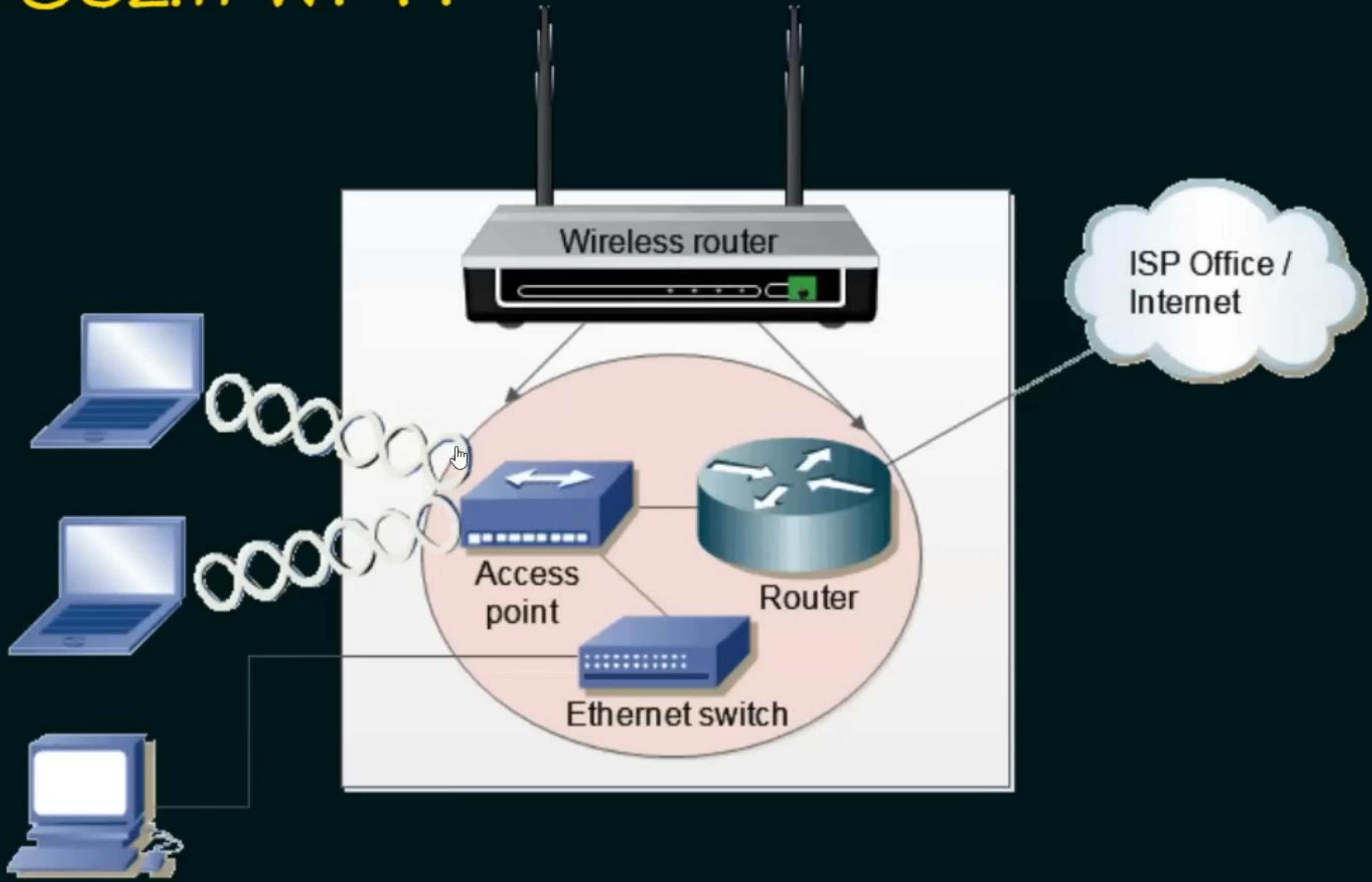
Exponential Backoff

- Once an adaptor has detected a collision, and stopped its transmission, it waits a certain amount of time and tries again.
- Each time the adaptor tries to transmit but fails, it doubles the amount of time it waits before trying again.
- This strategy of doubling the delay interval between each retransmission attempt is known as Exponential Backoff.

IEEE 802.11

- ★ Also known as Wireless Fidelity (Wi-Fi).
- ★ Like its Ethernet and token ring siblings, 802.11 is designed fo
  limited geographical area (homes, office buildings, campuse
- ★ Primary challenge is to mediate access to a shared commun
  medium - in this case, signals propagating through space.

IEEE 802.11 Wi-Fi



Wi-Fi Adaptor

Different Wi-Fi protocols

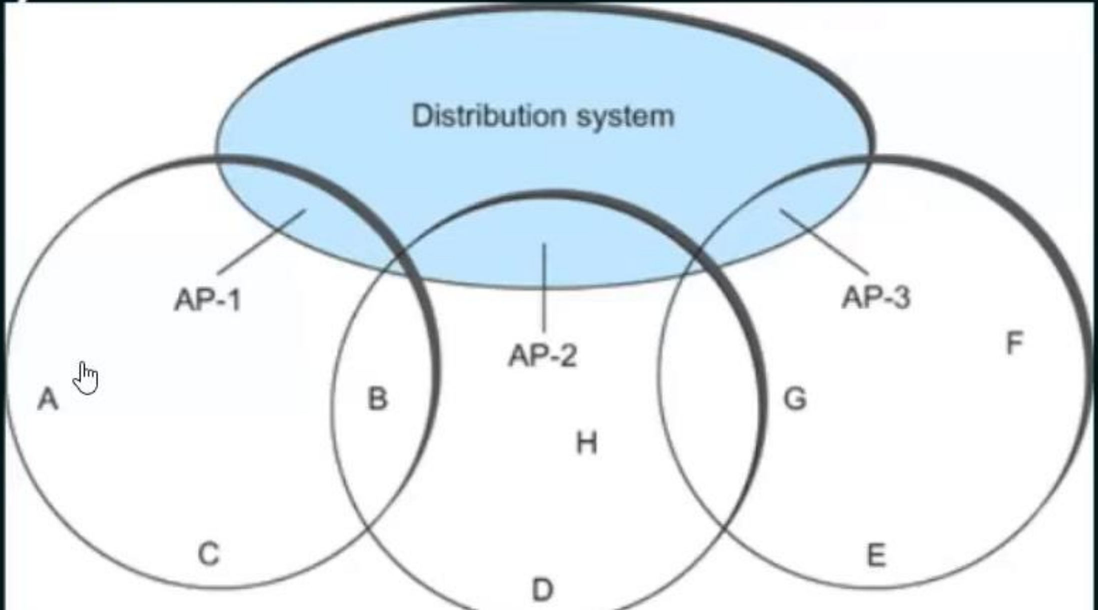
Protocol	Frequency	Channel Width	Maximum data rate (theoretical)
802.11 ax	2.4 or 5GHz	20, 40, 80, 160MHz	2.4 Gbps
802.11 ac wave2	5 GHz	20, 40, 80, 160MHz	1.73 Gbps
802.11 ac wave1	5 GHz	20, 40, 80MHz	866.7 Mbps
802.11n	2.4 or 5 GHz	20, 40MHz	450 Mbps
802.11g	2.4 GHz	20 MHz	54 Mbps
802.11a	5 GHz	20 MHz	54 Mbps
802.11b	2.4 GHz	20 MHz	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	2 Mbps

IEEE 802.11 Distribution System

- 802.11 is suitable for an ad-hoc configuration of nodes that may or may not be able to communicate with all other nodes.
- Nodes are free to move around.
- The set of directly reachable nodes may change over time.
- To deal with this mobility and partial connectivity,
  - 802.11 defines additional structures on a set of nodes
  - Instead of all nodes being created equal,
    - some nodes are allowed to roam and some are connected to a wired network infrastructure, they are called Access Points (AP) and they are connected to each other by a so-called distribution

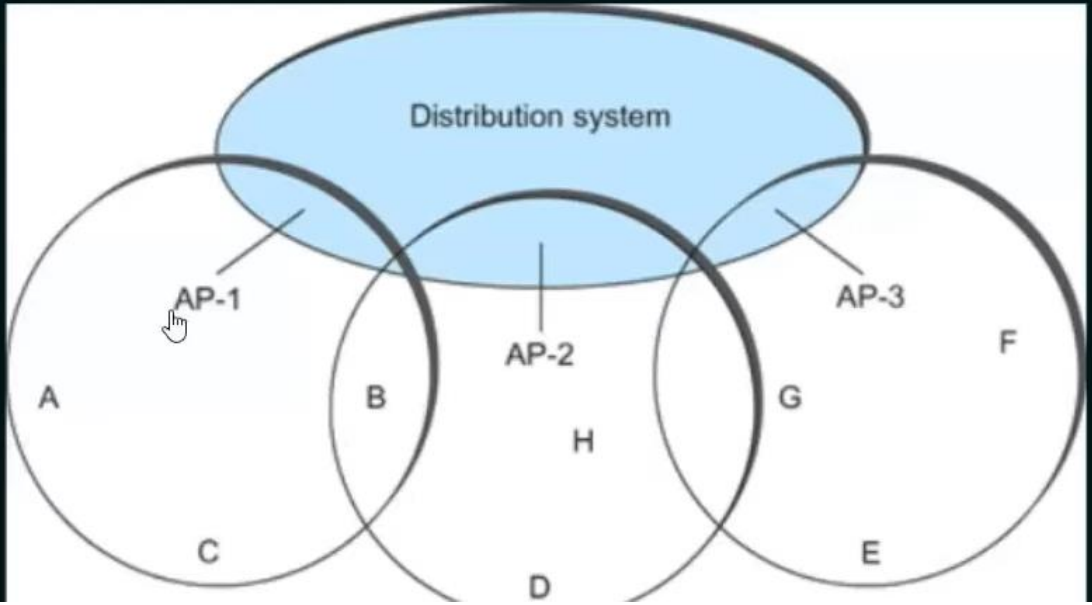
Access points connected to a Distribution network

- Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is
  - Each nodes associates itself with one access point.
  - For node A to communicate with node E, A first sends a frame to its AP–1 which forwards the frame across the distribution system to AP–3, which finally transmits the frame to E.



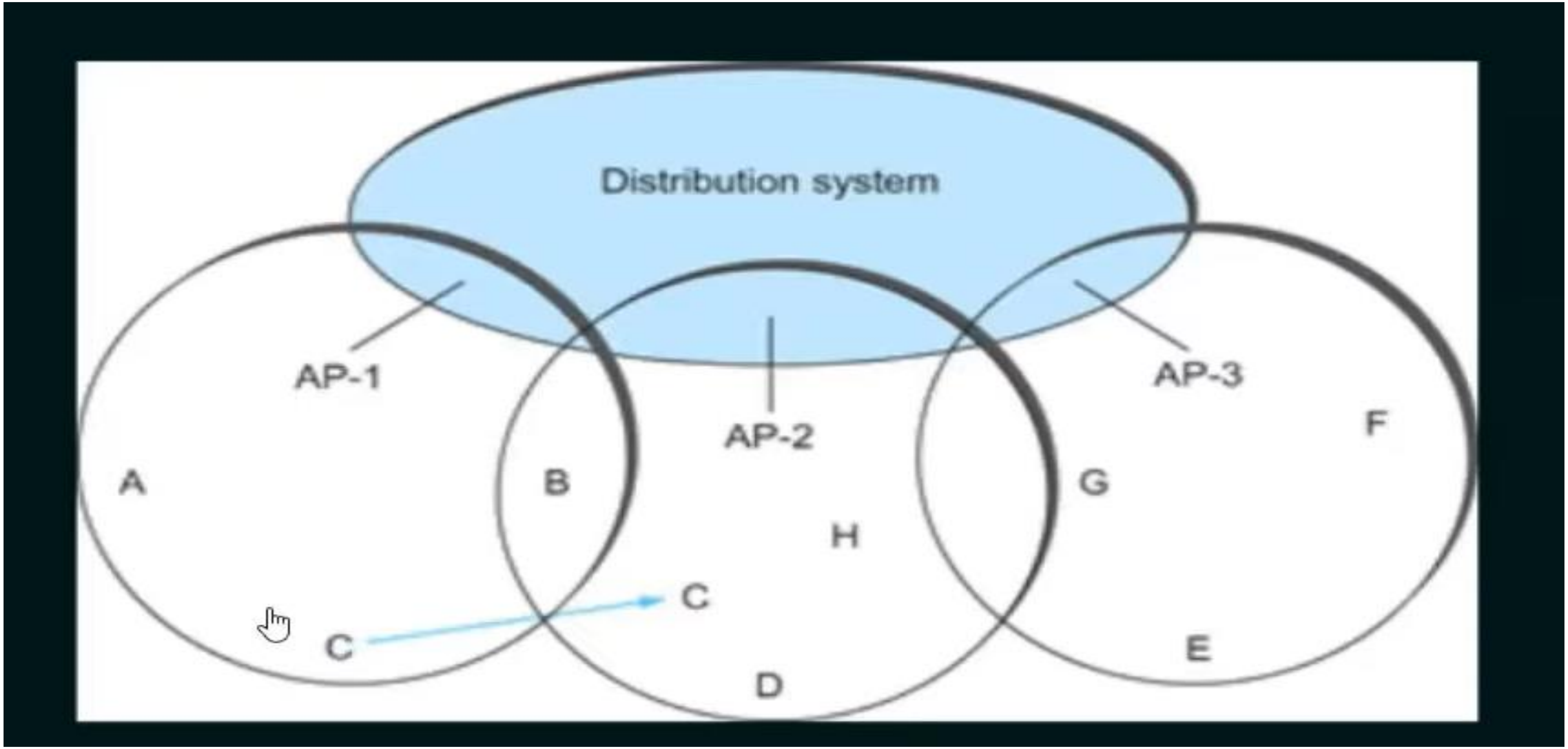
HOW DOES THE NODES SELECT THEIR AP?

- The technique for selecting an AP is called scanning.
  - The node sends a Probe frame.
  - All APs within reach reply with a Probe Response frame.
  - The node selects one of the access points and sends that AP an Association Request frame.
  - The AP replies with an Association Response frame.



How does the nodes select their AP?

- ★ A node engages this protocol whenever it joins the network, as well as
- ★ When it becomes unhappy with its current AP?
  - This might happen, for example, because the signal from its current AP has weakened due to the node moving away from it.
  - Whenever a node acquires a new AP, the new AP notifies the old AP of the change via the distribution system.


Distribution system
AP-1
AP-2
AP-3
A
B
C
C
D
E
F
G
H

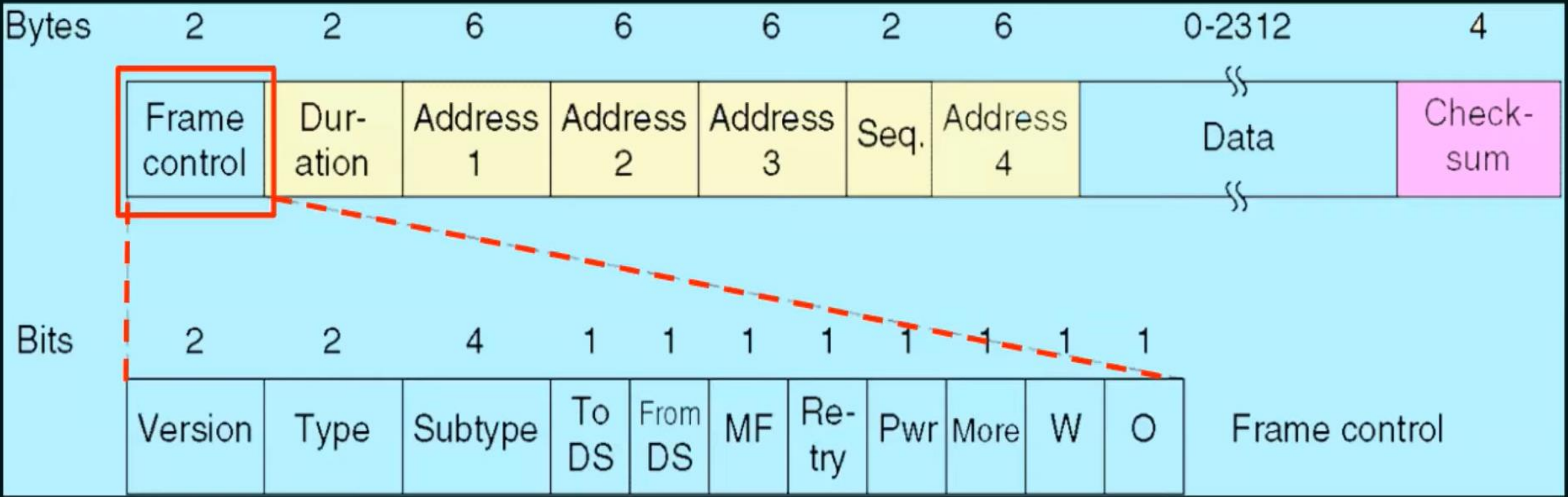
Node mobility

- ★ Consider the situation shown in the following figure when node C moves from the cell serviced by AP–1 to the cell serviced by AP–2.
- ★ As it moves, it sends Probe frames, which eventually result in Probe Responses from AP–2.
- ★ At some point, C prefers AP–2 over AP–1 , and so it associates itself with that access point. This is called active scanning since the node is actively searching for an access point.

Passive scanning

- ★ APs also periodically send a Beacon frame that advertises the capabilities of the access point; these include the transmission rate supported by the AP
  - This is called passive scanning.
  - A node can change to this AP based on the Beacon frame simply by sending it an Association Request frame back to the access point.

IEEE 802.11 Wi-Fi Frame Format

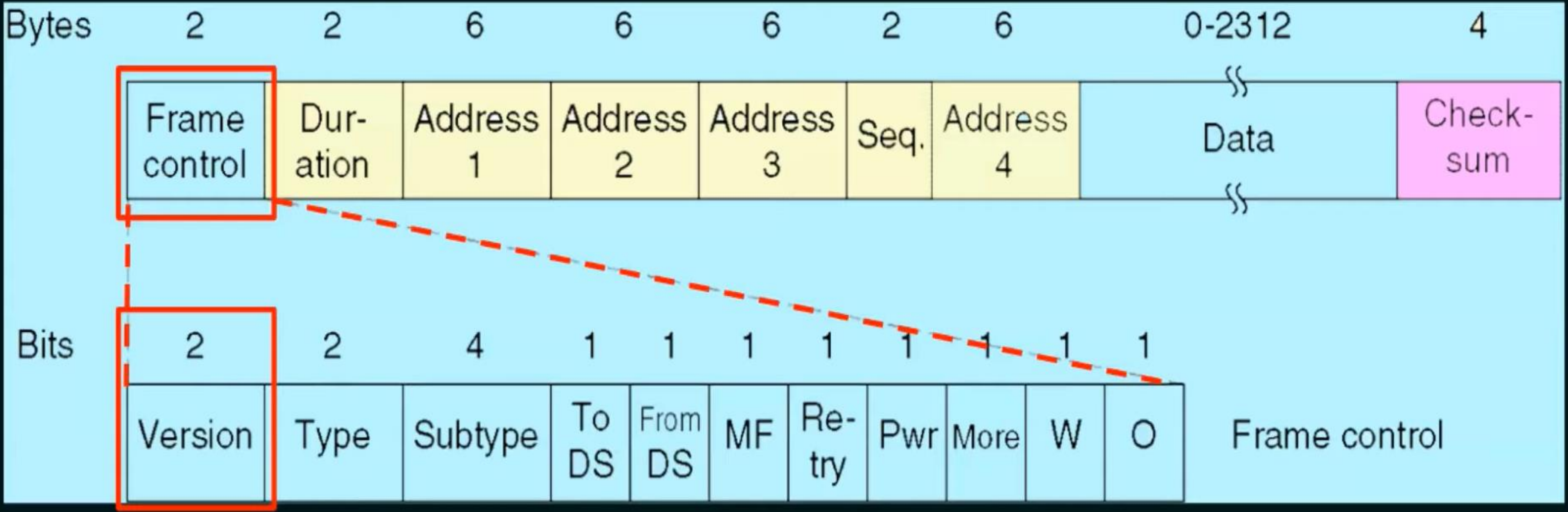


Frame Control:

★ It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.

★ It has 11 subfields

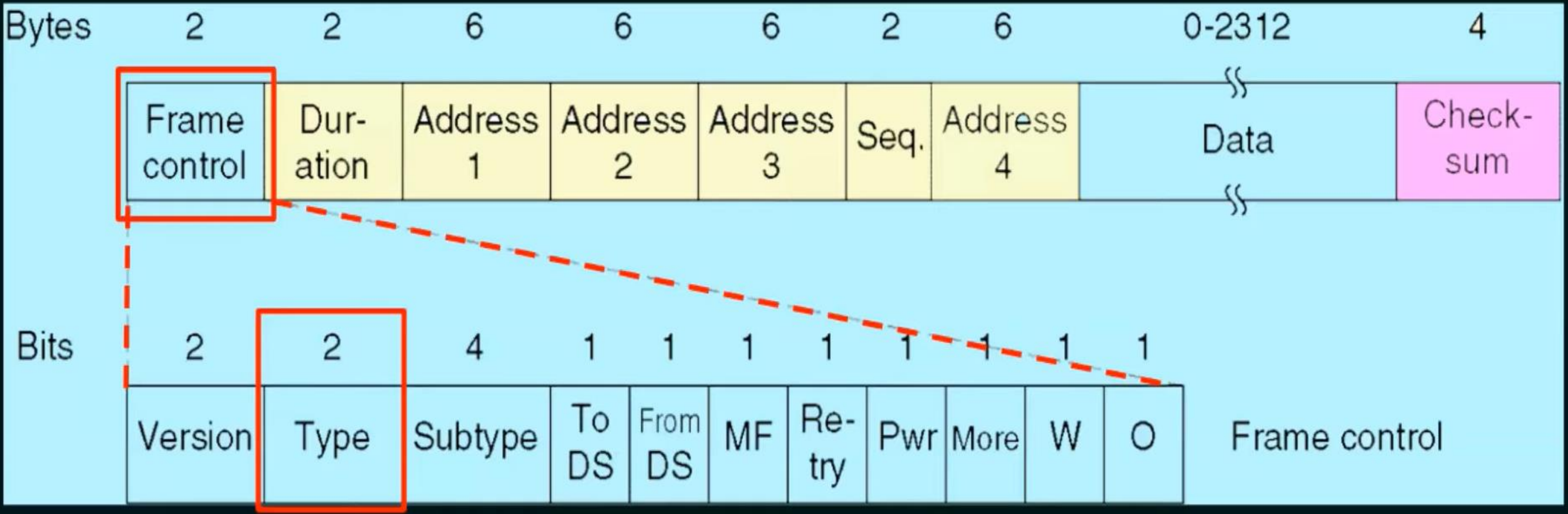
IEEE 802.11 Wi-Fi Frame Format



Protocol Version:

★ The first sub-field is a two – bit field set to 00. It has been included to allow future versions of IEEE 802.11 to operate simultaneously.

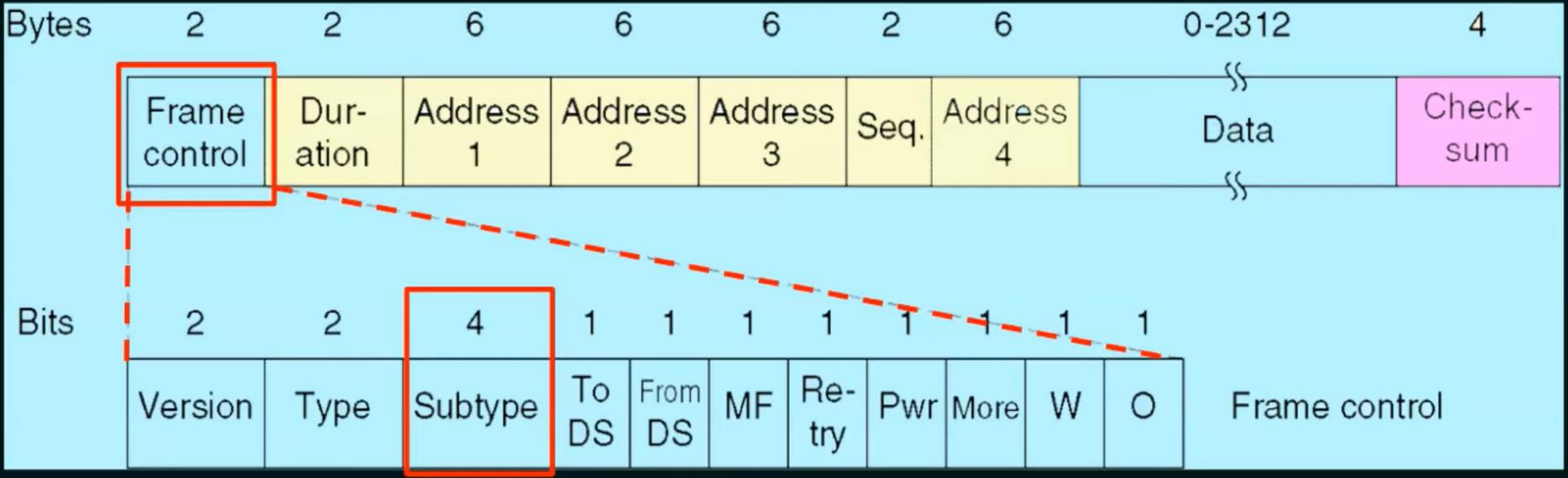
IEEE 802.11 Wi-Fi Frame Format



Type:

★ It is a two-bit subfield that specifies whether the frame is a data frame, control frame or a management frame.

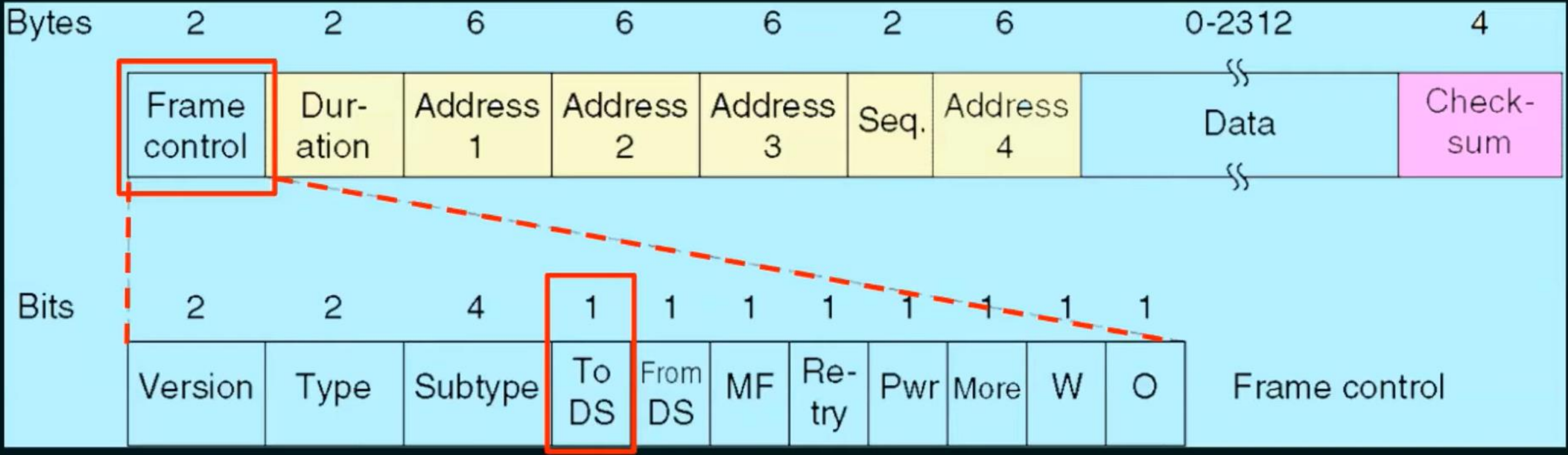
IEEE 802.11 Wi-Fi Frame Format



Subtype:

★ It is a four – bit subfield states whether the field is a Request to Send (RTS) or a Clear to Send (CTS) control frame. For a regular data frame, the value is set to 0000.

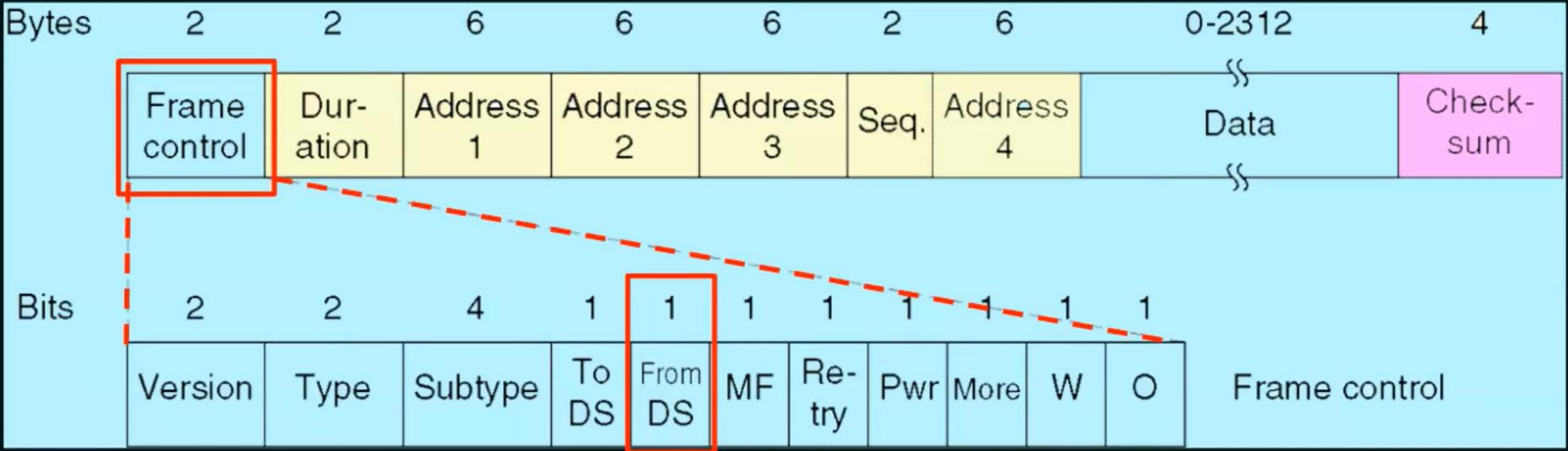
IEEE 802.11 Wi-Fi Frame Format



To DS:

★ A single bit subfield indicating whether the frame is going to the access point (AC), which coordinates the communications in centralised wireless systems.

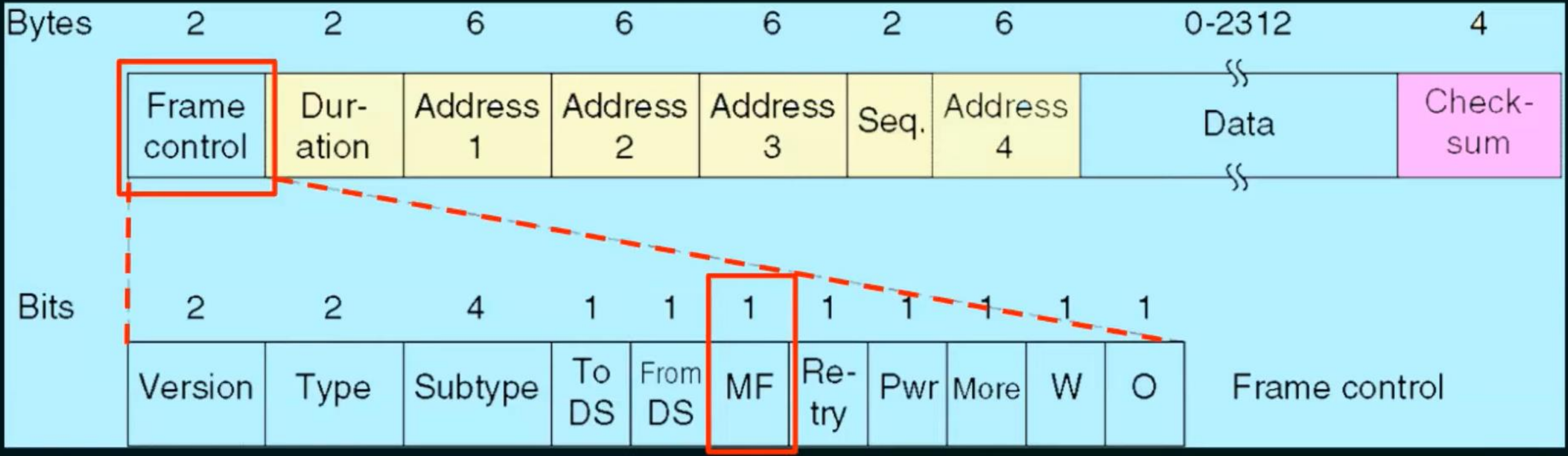
IEEE 802.11 Wi-Fi Frame Format



From DS:

★ A single bit subfield indicating whether the frame is coming from the Access point.

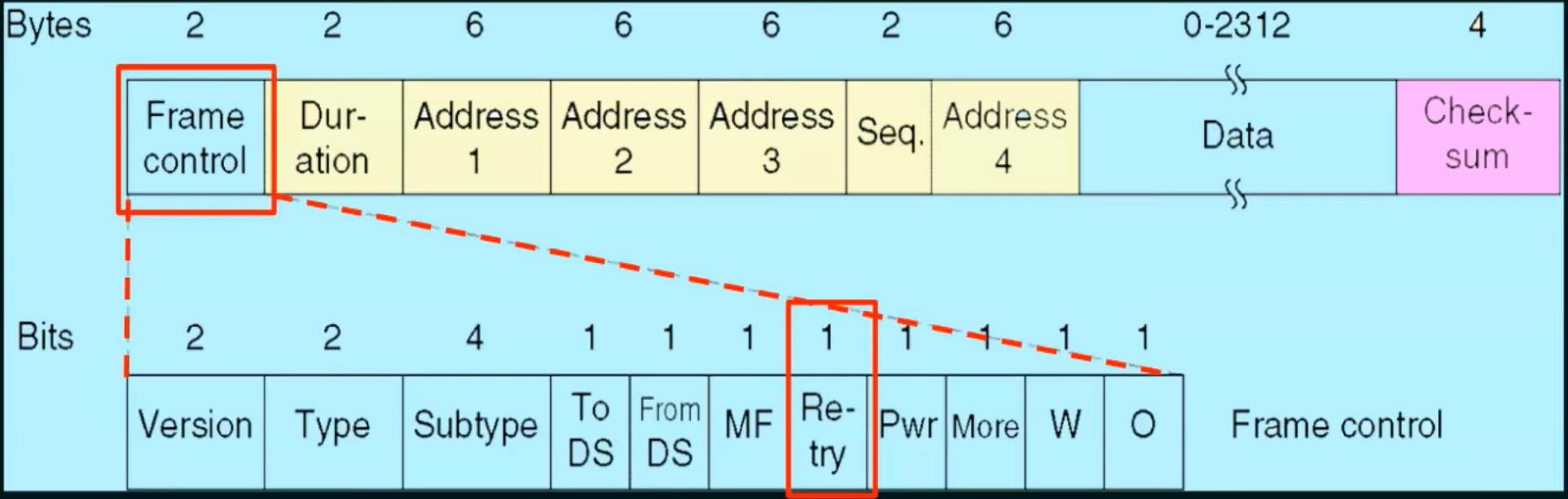
IEEE 802.11 Wi-Fi Frame Format



More Fragments:

★ A single bit subfield which when set to 1 indicates that more fragments would follow.

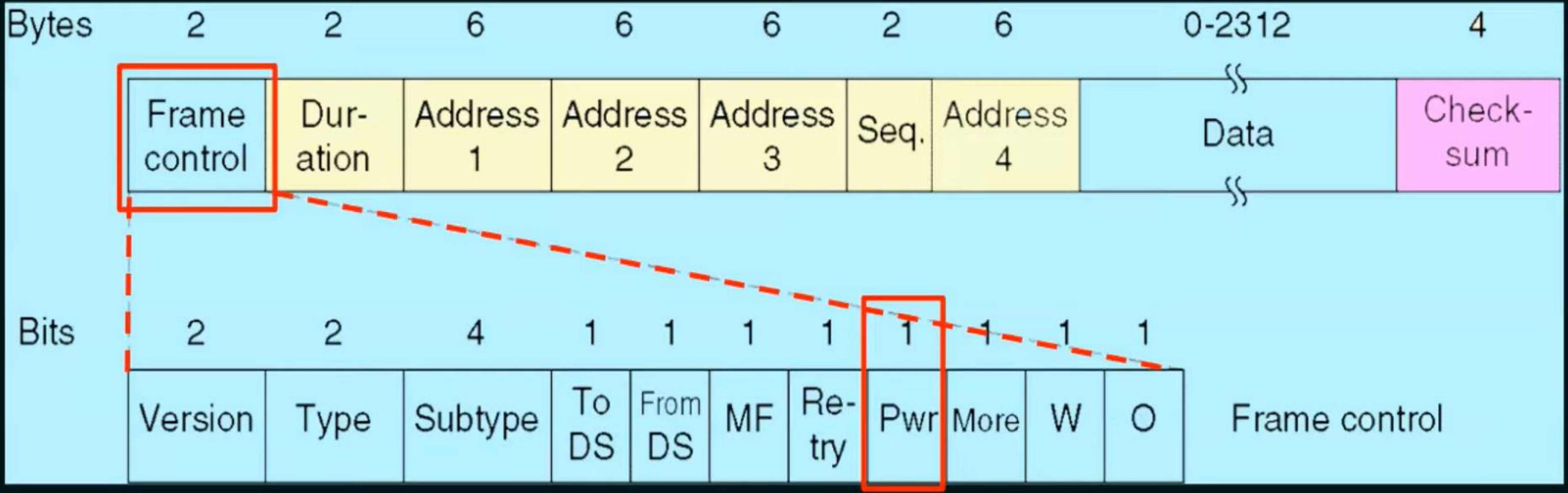
IEEE 802.11 Wi-Fi Frame Format



Retry:

- ★ A single bit subfield which when set to 1 specifies a retransmission of a previous frame.

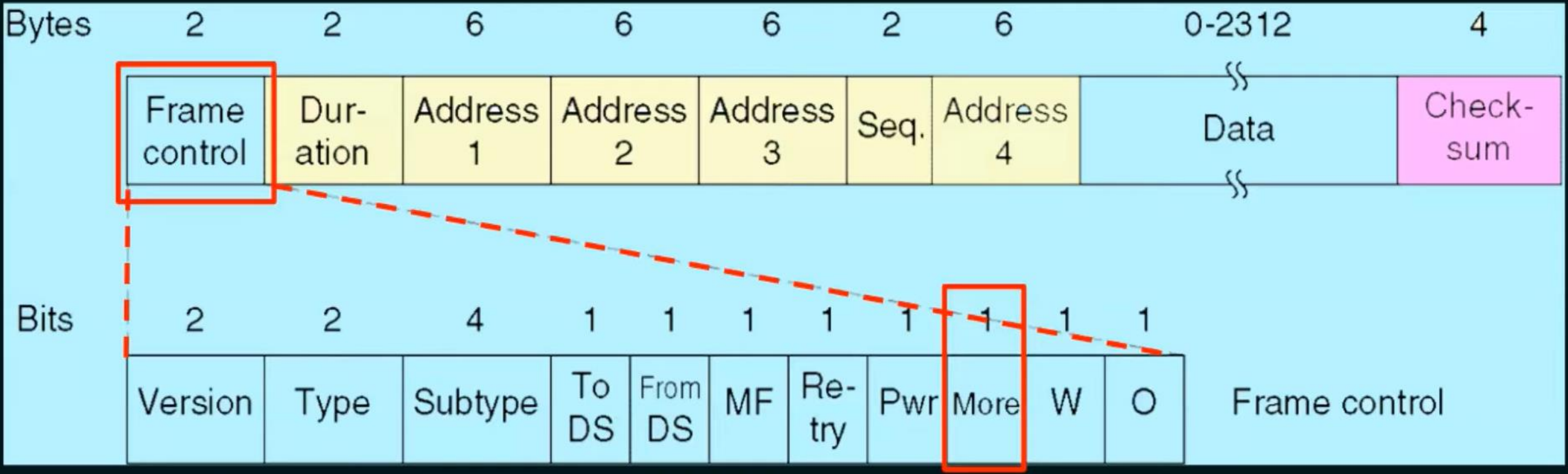
IEEE 802.11 Wi-Fi Frame Format



Power Management:

- ★ A single bit subfield indicating that the sender is adopting power-save mode.

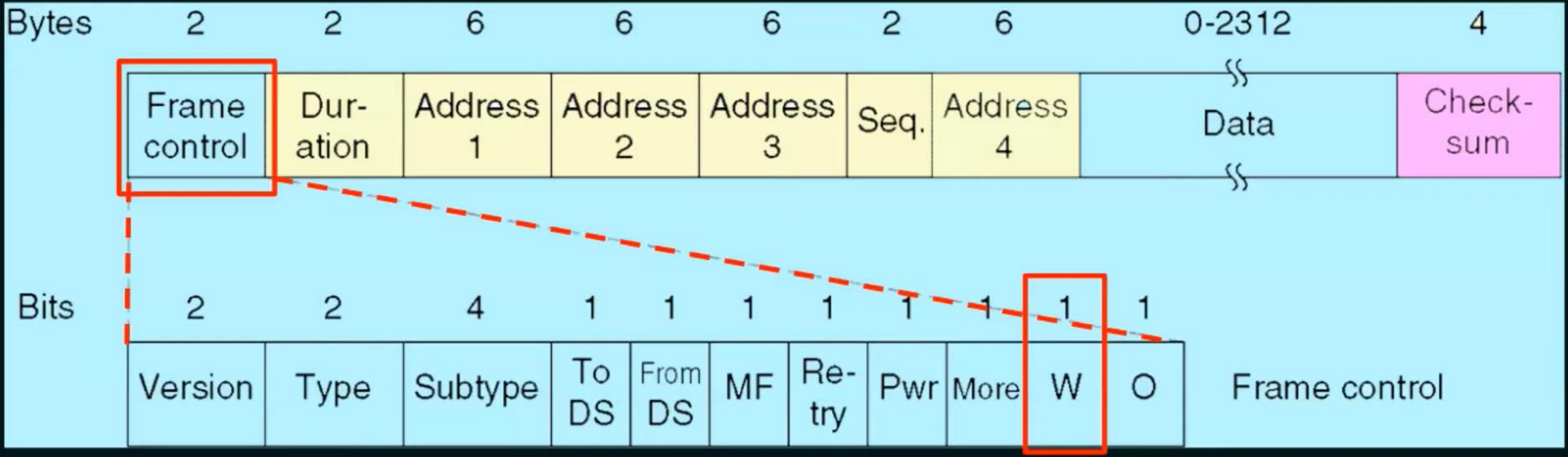
IEEE 802.11 Wi-Fi Frame Format



More Data:

★ A single bit subfield showing that sender has further data frames for the receiver.

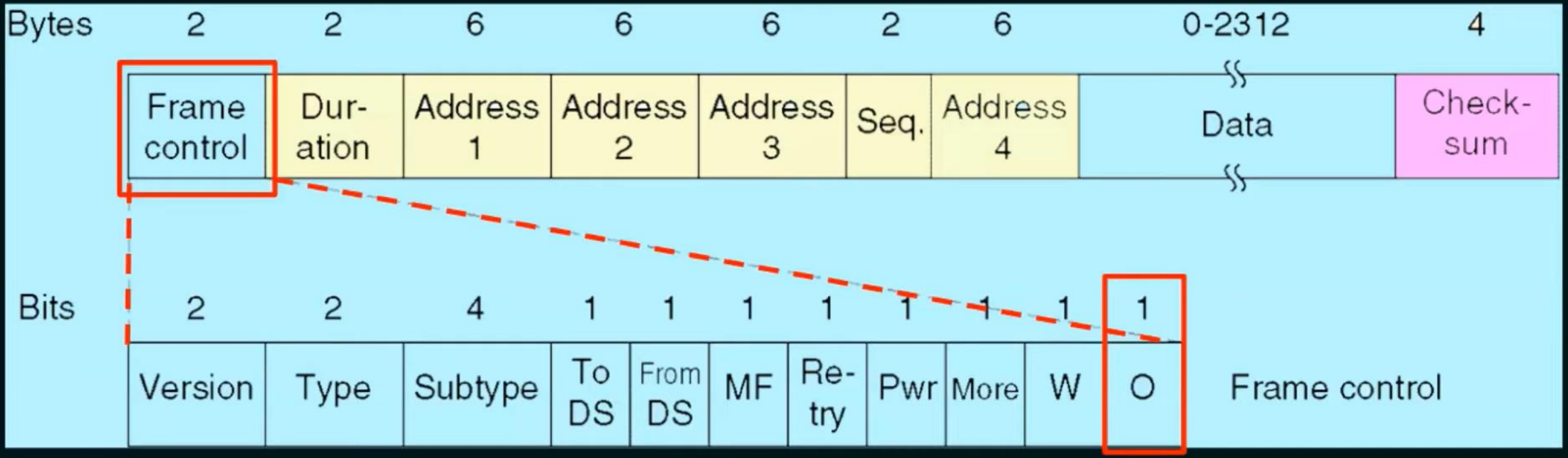
IEEE 802.11 Wi-Fi Frame Format



WEP:

★ A single bit subfield indicating that this is an encrypted frame.

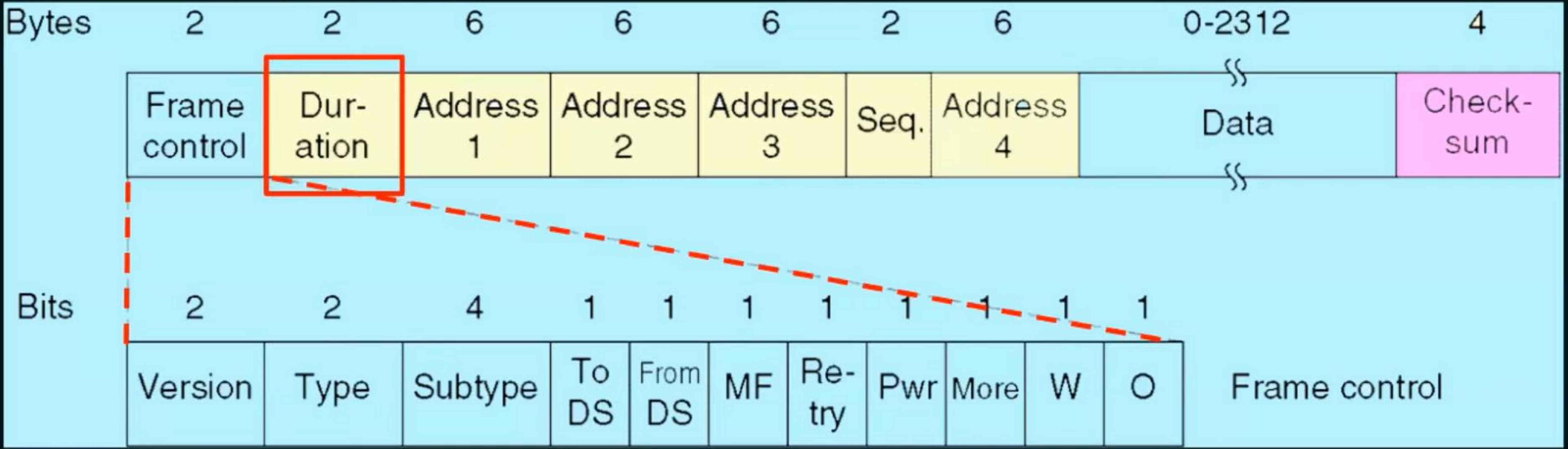
IEEE 802.11 Wi-Fi Frame Format



Order:

★ The last subfield, of one – bit, informs the receiver that to the higher layers the frames should be in an ordered sequence.

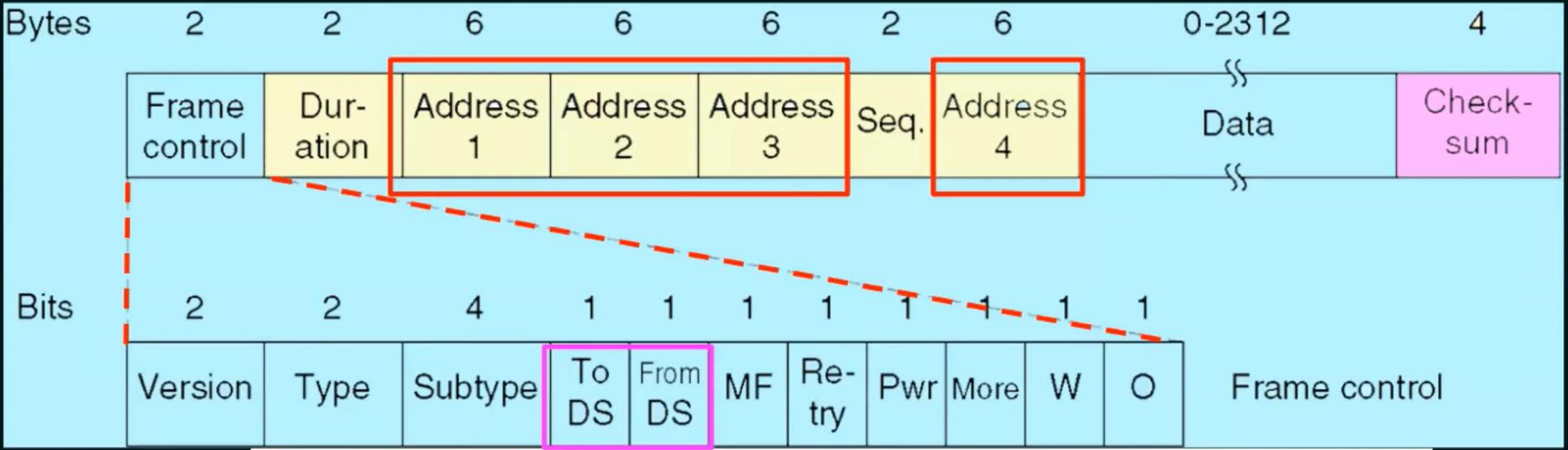
IEEE 802.11 Wi-Fi Frame Format



Duration:

★ It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.

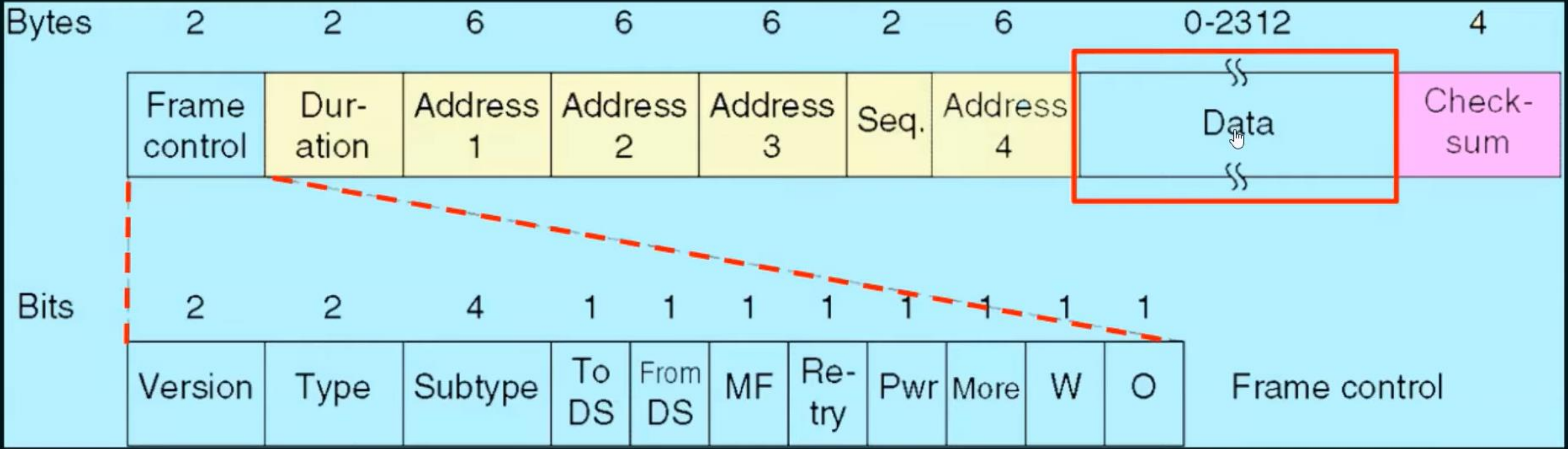
IEEE 802.11 Wi-Fi Frame Format



To DS	*From* DS	*Address* 1	*Address* 2	*Address* 3	*Address* 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	SendingAP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	SendingAP	Destination	Source

[redacted]

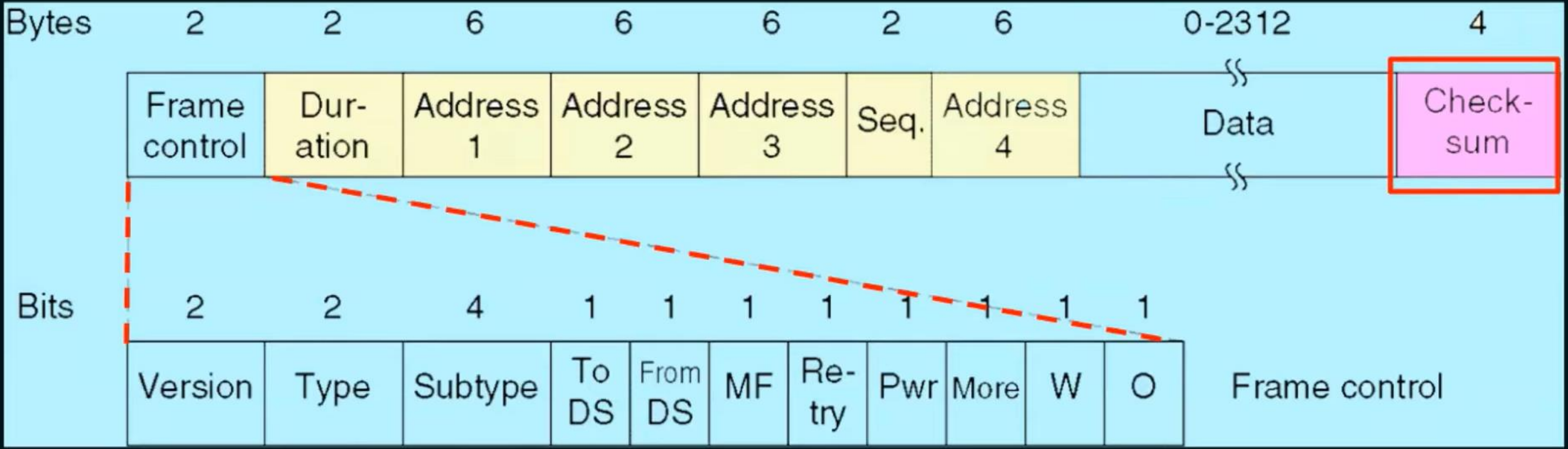
IEEE 802.11 Wi-Fi Frame Format



Data:

★ This is a variable sized field that carries the payload from the upper layers. The maximum size of data field is 2312 bytes.

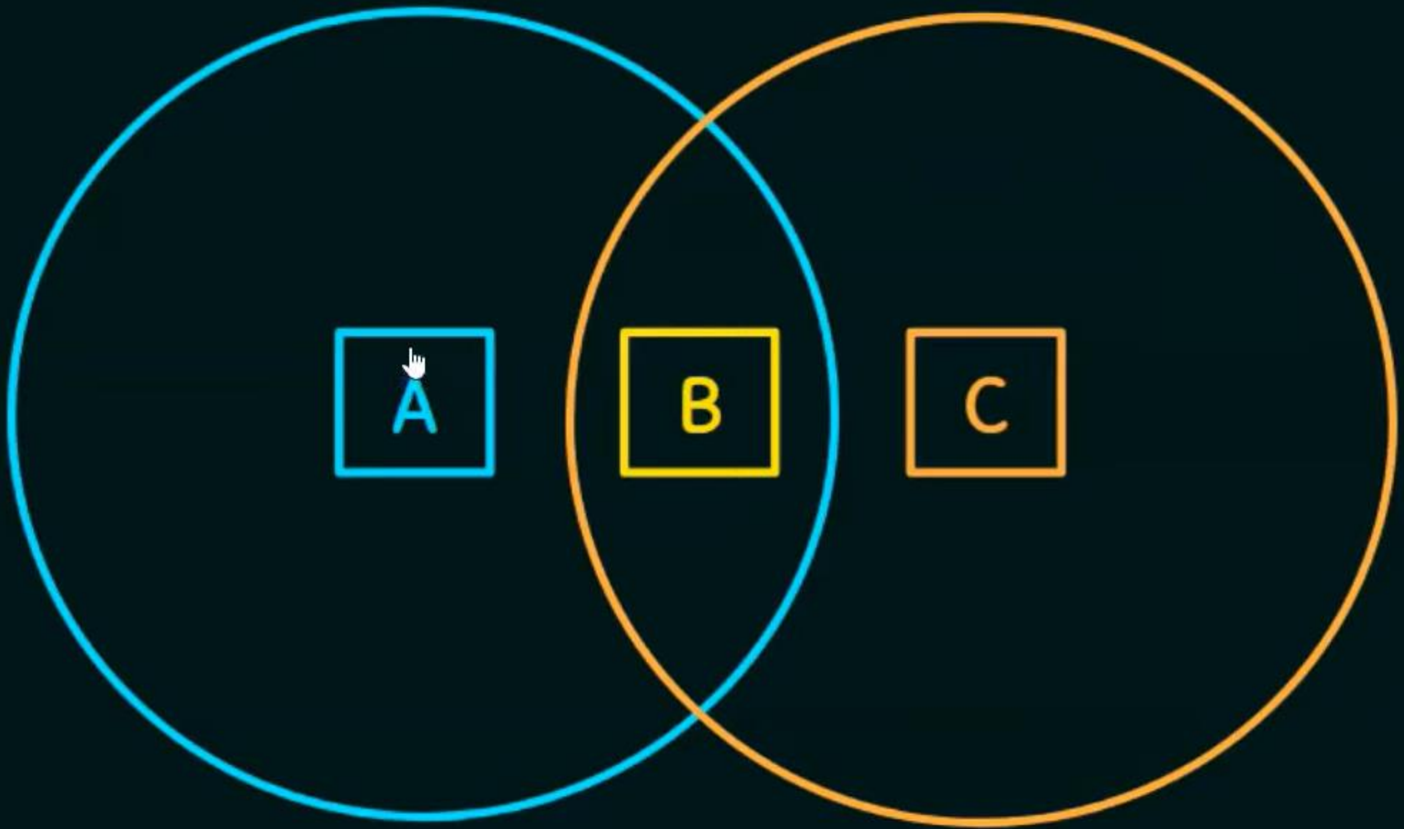
IEEE 802.11 Wi-Fi Frame Format



Checksum:

★ It is a 4-byte field for error detection purpose.

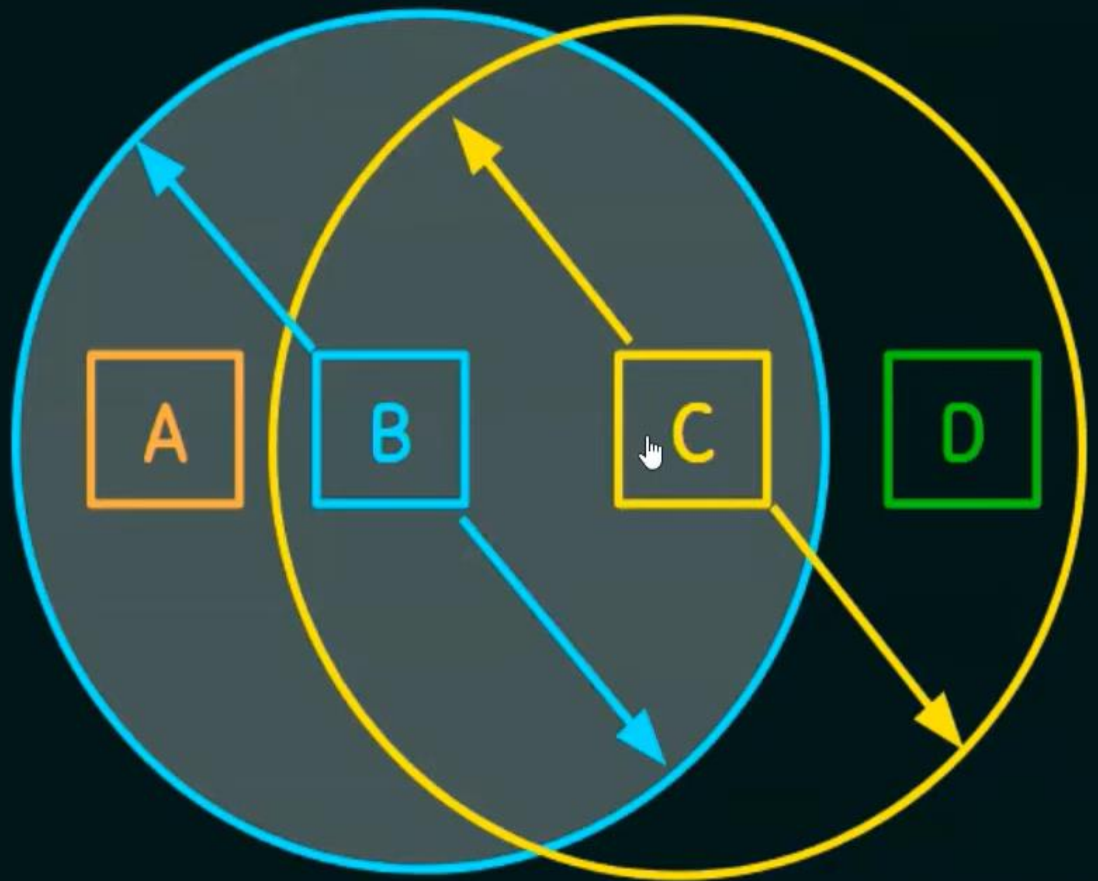
Hidden Terminal Problem



Suppose both A and C want to communicate with B and so they each send it a frame.

- ★ A and C are unaware of each other since their signals do not carry that far.
- ★ These two frames collide with each other at B (But unlike an Ethernet, neither A nor C is aware of this collision).
- ★ A and C are said to hidden nodes with respect to each other.

Exposed Terminal Problem



Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.

- ★ It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
- ★ Suppose C wants to transmit to node D.

IEEE 802.11 – Collision Avoidance

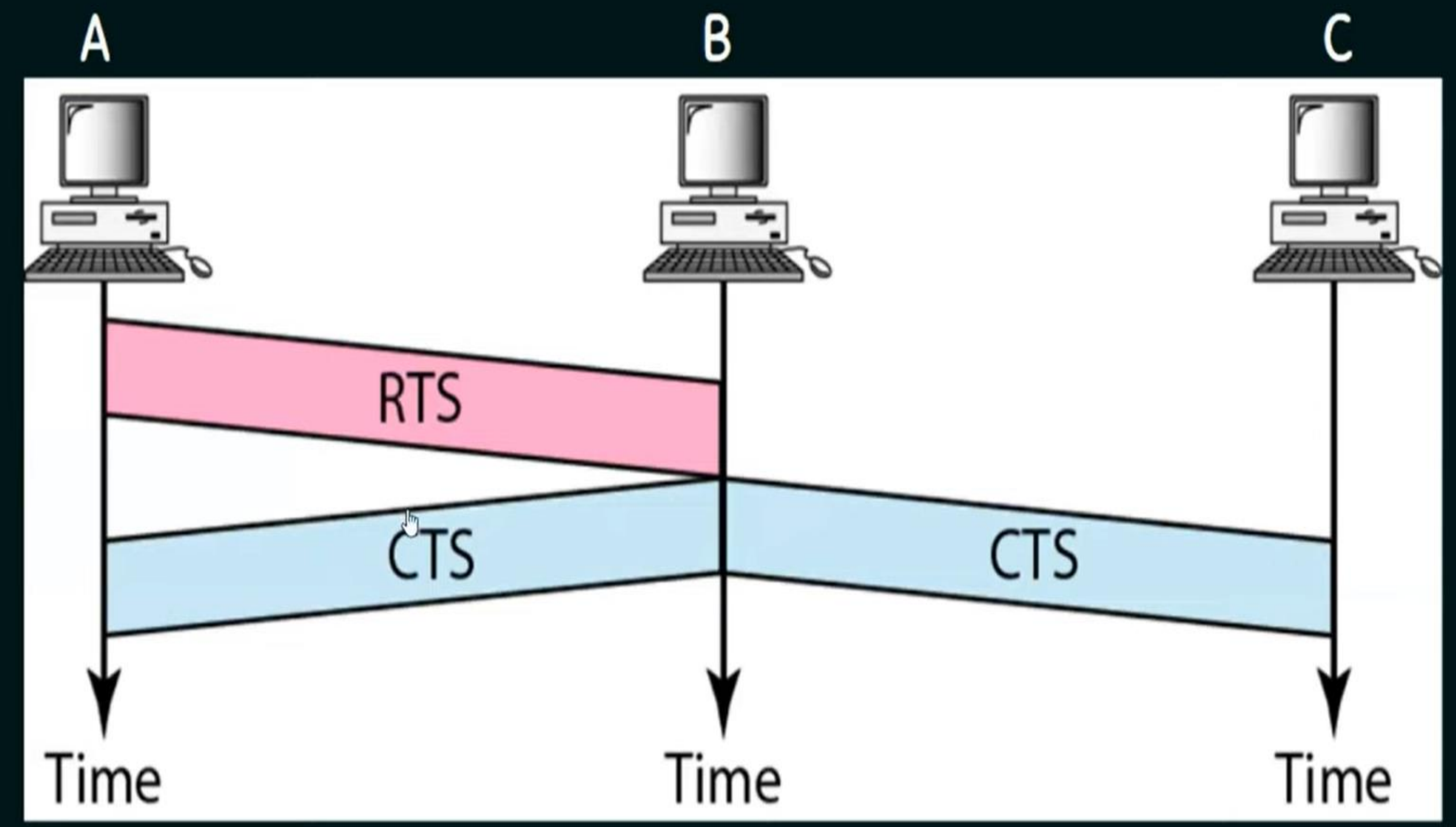
- ★ 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).

Key Idea

- ★ Sender and receiver exchange control frames with each other before the sender actually transmits any data.
- ★ This exchange informs all nearby nodes that a transmission is about to begin.
- ★ Sender transmits a Request to Send (RTS) frame to the receiver.
    - ○ The RTS frame includes a field that indicates how long the sender wants to hold the medium. Length of the data frame to be transmitted.
- ★ Receiver replies with a Clear to Send (CTS) frame
    - ○ This frame echoes this length field back to the sender

IEEE 802.11 – Collision Avoidance

- Any node that sees the CTS frame knows that
  - it is close to the receiver, therefore
  - cannot transmit for the period of time it takes to send a frame of the specified length
- Any node that sees the RTS frame but not the CTS frame
  - is not close enough to the receiver to interfere with it, and
  - so is free to transmit


A
B
C
RTS
CTS
CTS
Time
Time
Time

Consider a 512×10^3 bits/second satellite communication link with one way propagation delay of 150 milliseconds. GO Back-N protocol is used on this link to send data with a frame size of 1 kilobyte. Acknowledgement size is 64 byte, and frame processing time is 5 ms. Then what should be the minimum window size-------